Red Hat Enterprise Linux 6

6.4 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 6.4

Edition 4

Last Updated: 2017-10-20

Red Hat Enterprise Linux 6 6.4 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 6.4
Edition 4

Red Hat Customer Content Services

Legal Notice

Abstract

The Red Hat Enterprise Linux 6.4 Technical Notes list and document the changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications between Red Hat Enterprise Linux 6.3 and minor release Red Hat Enterprise Linux 6.4.

Table of Contents

PREFACE

The *Red Hat Enterprise Linux 6.4 Technical Notes* list and document the changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications between minor release Red Hat Enterprise Linux 6.3 and minor release Red Hat Enterprise Linux 6.4.

For system administrators and others planning Red Hat Enterprise Linux 6.4 upgrades and deployments, the Technical Notes provide a single, organized record of the bugs fixed in, features added to, and Technology Previews included with this new release of Red Hat Enterprise Linux.

For auditors and compliance officers, the *Red Hat Enterprise Linux 6.4 Technical Notes* provide a single, organized source for change tracking and compliance testing.

For every user, the *Red Hat Enterprise Linux 6.4 Technical Notes* provide details of what has changed in this new release.

NOTE

The Package Manifest is available as a separate document.

CHAPTER 1. IMPORTANT CHANGES TO EXTERNAL KERNEL PARAMETERS

This chapter provides system administrators with a summary of significant changes in the kernel shipped with Red Hat Enterprise Linux 6.4. These changes include added or updated **`procfs`** entries, **`sysfs`** default values, boot parameters, kernel configuration options, or any noticeable behavior changes.

`intel_idle.max_cstate`

A new kernel parameter, ***`intel_idle.max_cstate`***, has been added to specify the maximum depth of a C-state, or to disable **`intel_idle`** and fall back to **`acpi_idle`**. For more information, refer to the **`/usr/share/doc/kernel-doc-<version>/Documentation/kernel-parameters.txt`** file.

`nobar`

The new ***`nobar`*** kernel parameter, specific to the AMD64 / Intel 64 architecture, can be used to not assign address space to the Base Address Registers (BARs) that were not assigned by the BIOS.

`noari`

The new ***`noari`*** kernel parameter can disable the use of PCIe Alternative Routing ID Interpretation (ARI).

MD `state` file

The **`state`** file of an MD array component device (found in the **`/sys/block/md<md_number>/md/dev-<device_name>`** directory) can now contain additional device states. For more information, refer to the **`/usr/share/doc/kernel-doc-<version>/Documentation/md.txt`** file.

`route_localnet`

The ***`route_localnet`*** kernel parameter can be used to enable the use of 127/8 for local routing purposes. For more information, refer to the **`/usr/share/doc/kernel-doc-<version>/Documentation/networking/ip-sysctl.txt`** file.

`pf_retrans`

The ***`pf_retrans`*** kernel parameter specifies the number of re-transmissions that will be attempted on a given path before traffic is redirected to an alternate transport (should one exist). For more information, refer to the **`/usr/share/doc/kernel-doc-<version>/Documentation/networking/ip-sysctl.txt`** file.

`traceevent`

The new **`traceevent`** library, used by **perf**, uses the following sysfs control files:

```
/sys/kernel/debug/tracing/events/header_page
/sys/kernel/debug/tracing/events/.../.../format
/sys/bus/event_source/devices/<dev>/format
/sys/bus/event_source/devices/<dev>/events
/sys/bus/event_source/devices/<dev>/type
```

`/sys/kernel/fadump_*`

On 64-bit IBM POWER machines, the following control files have been added to be used by the firmware-assisted dump feature:

```
/sys/kernel/fadump_enabled
/sys/kernel/fadump_registered
/sys/kernel/fadump_release_mem
```

For more information about these files, refer to **`/usr/share/doc/kernel-doc-<`*`version`*`>/Documentation/powerpc/firmware-assisted-dump.txt`**.

Transparent Hugepages

The **`/sys/kernel/mm/transparent_hugepage symbolic`** link, which points to **`/sys/kernel/mm/redhat_transparent_hugepage`**, has been added for consistency purposes.

Documentation for transparent hugepages has been added to the following file:

```
/usr/share/doc/kernel-doc-<version>/Documentation/vm/transhuge.txt
```

vmbus_show_device_attr

The ***`vmbus_show_device_attr`*** attribute of the Hyper-V **`vmbus`** driver shows the device attribute in sysfs. This is invoked when the **`/sys/bus/vmbus/devices/<`*`busdevice`*`>/<`*`attr_name`*`>`** file is read.

BNA debugfs Interface

The BNA debugfs interface can be accessed through the **`bna/pci_dev:<`*`pci_name`*`>`** hierarchy (note that the debugfs file system must be mounted). The following debugging services are available for each **`pci_dev>`**:

- **`fwtrc`** — used to collect current firmware trace.
- **`fwsave`** — used to collect last-saved firmware trace as a result of firmware crash.
- **`regwr`** — used to write one word to the chip register.
- **`regrd`** — used to read one or more words from the chip register.

`iwlegacy` ***`debug_level`***

The **`iwlegacy`** driver includes a new sysfs control file, ***`/sys/bus/pci/drivers/iwl/debug_level`***, to control per-device level of debugging. The **`CONFIG_IWLEGACY_DEBUG`** option enables this feature.

`iwlwifi` ***`debug_level`***

The **`iwlwifi`** driver includes a new sysfs control file, ***`/sys/class/net/wlan0/device/debug_level`***, to control per-device level of debugging. The **`CONFIG_IWLWIFI_DEBUG`** option enables this feature.

`ie6xx_wdt`

If debugfs is mounted, the new **`/sys/kernel/debug/ie6xx_wdt`** file contains a value that determines whether the system was rebooted by watchdog.

`supported_krb5_enctypes`

The new **`/proc/fs/nfsd/supported_krb5_enctypes`** proc file lists the encryption types supported by the kernel's **`gss_krb5`** code.

`usbmixer`

The **`/proc/asound/card<card_number>/usbmixer`** proc file has been added. It contains a mapping between the ALSA control API and the USB mixer control units. This file can be used debugging and problem diagnostics.

`codec#<number>`

The **`/proc/asound/card<card_number>/codec#<number>`** proc files now contain information about the D3cold power state, the deepest power-saving state for a PCIe device. The **`codec#<number>`** files now also contain additional power state information, specifically: **`reset status`**, **`clock stop ok`**, and **`power states error`**. The following is an example output:

```
Power: setting=D0, actual=D0, Error, Clock-stop-OK, Setting-reset
```

`cgroup.procs`

The **`cgroup.procs`** file is now writable. Writing a TGID into the cgroup.procs file of a cgroup moves that thread group into that cgroup.

`sysfs_dirent`

The last **`sysfs_dirent`**, which represents a single sysfs node, is now cached to improve scalability of the **`readdir`** function.

`iov`

The **`iov`** sysfs directory was added under the **`ib`** device. This directory is used to manage and examine the port P_Key and guid paravirtualization.

FDMI attributes

Fabric Device Management Interface (FDMI) attributes can now be exposed to the **`fcoe`** driver via the **`fc_host`** class object.

`ltm_capable`

The **`/sys/bus/usb/devices/<device>/ltm_capable`** file has been added to show whether a device supports Latency Tolerance Messaging (LTM). This file is present for both USB 2.0 and USB 3.0 devices.

`fwdump_state`

The **`/sys/class/net/eth<number>/device/fwdump_state`** file has been added to determine whether the firmware dump feature is enabled or disabled.

`flags`, **`registers`**

The **`Commands in Q`** item was added to the **`/sys/block/rssd<number>/registers`** file. This file's output was also re-formatted. Also, a new **`/sys/block/rssd<number>/flags`** file has been added. This read-only file dumps the flags in a port and driver data structure.

duplex

The **/sys/class/net/eth*<number>*/duplex** file now reports **unknown** when the NIC duplex state is **DUPLEX_UNKNOWN**.

Mountpoint Interface

A sysfs mountpoint interface was added to the **perf** tool.

TCP_USER_TIMEOUT

TCP_USER_TIMEOUT is a TCP level socket option that specifies the maximum amount of time (in milliseconds) that transmitted data may remain unacknowledged before TCP will forcefully close the corresponding connection and return ETIMEDOUT to the application. If the value **0** is specified, TCP will continue to use the system default.

IPPROTO_ICMP

The **IPPROTO_ICMP** socket option makes it possible to send **ICMP_ECHO** messages and receive the corresponding **ICMP_ECHOREPLY** messages without any special privileges.

Increased Default in ST_MAX_TAPES

In Red Hat Enterprise Linux 6.4, the number of supported tape drives has increased from 128 to 512.

Increased Number of Supported IOMMUs

The number of supported input/output memory management units (IOMMUs) has been increased to be the same as the number of I/O Advanced Programmable Interrupt Controllers (APICs; defined in ***MAX_IO_APICS***).

New Module Parameters

The following list summarizes new command line arguments passed to various kernel modules. For more information about the majority of these module parameters, refer to the output of the **modinfo *<module>*** command, for example, **modinfo bna**.

- New **kvm** module parameter:

  ```
  module_param(min_timer_period_us, uint, S_IRUGO | S_IWUSR);
  ```

  - ***min_timer_period_us*** — Do not allow the guest to program periodic timers with small interval, since the hrtimers are not throttled by the host scheduler, and allow tuning the interval with this parameter. The default value is **500us**.

- New **kvm-intel** module parameter:

  ```
  module_param_named(eptad, enable_ept_ad_bits, bool, S_IRUGO);
  ```

  - ***enable_ept_ad_bits*** — Parameter to control enabling/disabling A/D bits, if supported by CPU. The default value is **enabled**.

- New **ata_piix** module parameter:

  ```
  module_param(prefer_ms_hyperv, int, 0);
  ```

  - ***prefer_ms_hyperv*** — On Hyper-V Hypervisors, the disks are exposed on both the emulated SATA controller and on the paravirtualized drivers. The CD/DVD devices are only exposed on the emulated controller. Request to ignore ATA devices on this host. The default value is **enabled**.

- New **drm** module parameters:

  ```
  module_param_named(edid_fixup, edid_fixup, int, 0400);
  module_param_string(edid_firmware, edid_firmware,
  sizeof(edid_firmware), 0644);
  ```

  - ***edid_fixup*** — Minimum number of valid EDID header bytes (0-8). The default value is **6**.

  - ***edid_firmware*** — Do not probe monitor, use specified EDID blob from built-in data or **/lib/firmware** instead.

- New **i915** module parameters:

  ```
  module_param_named(lvds_channel_mode, i915_lvds_channel_mode, int,
  0600);
  module_param_named(i915_enable_ppgtt, i915_enable_ppgtt, int,
  0600);
  module_param_named(invert_brightness,
  i915_panel_invert_brightness, int, 0600);
  ```

- New **nouveau** module parameter:

  ```
  module_param_named(vram_type, nouveau_vram_type, charp, 0400);
  ```

- New **radeon** module parameter:

  ```
  module_param_named(lockup_timeout, radeon_lockup_timeout, int,
  0444);
  ```

- New **i2c-ismt** module parameters:

  ```
  module_param(stop_on_error, uint, S_IRUGO);
  module_param(fair, uint, S_IRUGO);
  ```

- New **iw-cxgb4** module parameters:

  ```
  module_param(db_delay_usecs, int, 0644);
  module_param(db_fc_threshold, int, 0644);
  ```

- New **mlx4_ib** module parameter:

  ```
  module_param_named(sm_guid_assign, mlx4_ib_sm_guid_assign, int,
  0444);
  ```

- New **ib_qib** module parameter:

```
module_param_named(cc_table_size, qib_cc_table_size, uint,
S_IRUGO);
```

- New **bna** module parameter:

```
module_param(bna_debugfs_enable, uint, S_IRUGO | S_IWUSR);
```

- New **cxgb4** module parameters:

```
module_param(dbfifo_int_thresh, int, 0644);
module_param(dbfifo_drain_delay, int, 0644);
```

- New **e1000e** module parameter:

```
module_param(debug, int, 0);
```

- New **igb** module parameter:

```
module_param(debug, int, 0);
```

- New **igbvf** module parameter:

```
module_param(debug, int, 0);
```

- New **ixgbe** module parameter:

```
module_param(debug, int, 0);
```

- New **ixgbevf** module parameter:

```
module_param(debug, int, 0);
```

- New **hv_netvsc** module parameter:

```
module_param(ring_size, int, S_IRUGO);
```

- New **mlx4_core** module parameter:

```
module_param(enable_64b_cqe_eqe, bool, 0444);
```

  - ***enable_64b_cqe_eqe*** — Enable 64 byte CQEs/EQEs when the firmware supports this.

- New **sfc** module parameters:

```
module_param(vf_max_tx_channels, uint, 0444);
module_param(max_vfs, int, 0444);
```

- New **ath5k** module parameter:

```
module_param_named(no_hw_rfkill_switch,
ath5k_modparam_no_hw_rfkill_switch, bool, S_IRUGO);
```

- New **iwlegacy** module parameters:

```
module_param(led_mode, int, S_IRUGO);
module_param(bt_coex_active, bool, S_IRUGO);
```

- New **wlcore** module parameter:

```
module_param(no_recovery, bool, S_IRUSR | S_IWUSR);
```

- New s390 **scm_block** module parameters:

```
module_param(nr_requests, uint, S_IRUGO);
module_param(write_cluster_size, uint, S_IRUGO)
```

- New s390 **zfcp** module parameters:

```
module_param_named(no_auto_port_rescan, no_auto_port_rescan, bool,
0600);
module_param_named(datarouter, enable_multibuffer, bool, 0400);
module_param_named(dif, enable_dif, bool, 0400);
```

- New **aacraid** module parameters:

```
module_param(aac_sync_mode, int, S_IRUGO|S_IWUSR);
module_param(aac_convert_sgl, int, S_IRUGO|S_IWUSR);
```

- New **be2iscsi** module parameter:

```
module_param(beiscsi_##_name, uint, S_IRUGO);
```

- New **lpfc** module parameter:

```
module_param(lpfc_req_fw_upgrade, int, S_IRUGO|S_IWUSR);
```

- New **megaraid_sas** module parameters:

```
module_param(msix_vectors, int, S_IRUGO);
module_param(throttlequeuedepth, int, S_IRUGO);
module_param(resetwaittime, int, S_IRUGO);
```

- New **qla4xxx** module parameters:

```
module_param(ql4xqfulltracking, int, S_IRUGO | S_IWUSR);
module_param(ql4xmdcapmask, int, S_IRUGO);
module_param(ql4xenablemd, int, S_IRUGO | S_IWUSR);
```

- New **hv_storvsc** module parameter:

```
module_param(storvsc_ringbuffer_size, int, S_IRUGO);
```

- New **`ehci-hcd`** driver parameter:

  ```
  module_param(io_watchdog_force, uint, S_IRUGO);
  ```

  - ***`io_watchdog_force`*** — Force I/O watchdog to be ON for all devices.

- New **`ie6xx_wdt`** module parameters:

  ```
  module_param(timeout, uint, 0);
  module_param(nowayout, bool, 0);
  module_param(resetmode, byte, 0);
  ```

- New **`snd-ua101`** module parameter:

  ```
  module_param(queue_length, uint, 0644);
  ```

CHAPTER 2. DEVICE DRIVERS

This chapter provides a comprehensive listing of all device drivers which were updated in Red Hat Enterprise Linux 6.4.

Storage Drivers

- The Direct Access Storage Devices (**DASD**) device driver has been updated to detect path configuration errors that cannot be detected by hardware or microcode. Upon successful detection, the device driver does not use such paths. With this feature, for example, the DASD device driver detects paths that are assigned to a specific subchannel but lead to different storage servers.

- The **zfcp** device driver has been updated to add data structures and error handling to support the enhanced mode of the System z Fibre Channel Protocol (FCP) adapter card. In this mode, the adapter passes data directly from memory to the SAN (data routing) when memory on the adapter card is blocked by large and slow I/O requests.

- The **mtip32xx** driver has been updated to add support for the latest PCIe SSD drives.

- The **lpfc** driver for Emulex Fibre Channel Host Bus Adapters has been updated to version 8.3.5.86.1p.

- The **qla2xxx** driver for QLogic Fibre Channel HBAs has been updated to version 8.04.00.04.06.4-k, which adds support for QLogic's 83XX Converged Network Adapter (CNA), 16 GBps FC support for QLogic adapters, and new Form Factor CNA for HP ProLiant servers.

- The **qla4xxxx** driver has been updated to version v5.03.00.00.06.04-k0, which adds ***change_queue_depth*** API support, fixes a number of bugs, and introduces various enhancements.

- The **ql2400-firmware** firmware for QLogic 4Gbps fibre channel HBA has been updated to version 5.08.00.

- The **ql2500-firmware** firmware for QLogic 4Gbps fibre channel HBA has been updated to version 5.08.00.

- The **ipr** driver for IBM Power Linux RAID SCSI HBAs has been updated to version 2.5.4, which adds support for the Power7 6Gb SAS adapters and enables SAS VRAID capability on these adapters.

- The **hpsa** driver has been updated to version 2.0.2-4-RH1 to add PCI-IDs for the HP Smart Array Generation 8 family of controllers.

- The **bnx2i** driver for Broadcom NetXtreme II iSCSI has been updated to version 2.7.2.2 with general hardware support enablements. iSCSI and FCoE boot support on Broadcom devices is now fully supported in Red Hat Enterprise Linux 6.4. These two features are provided by the bnx2i and bnx2fc Broadcom drivers.

- The **bnx2fc** driver for the Broadcom Netxtreme II 57712 chip has been updated to version 1.0.12.

  iSCSI and FCoE boot support on Broadcom devices is now fully supported in Red Hat Enterprise Linux 6.4. These two features are provided by the bnx2i and bnx2fc Broadcom drivers.

- The **mpt2sas** driver has been updated to version 13.101.00.00, which adds multi-segment mode support for the Linux BSG Driver.

- The Brocade **bfa** Fibre Channel and FCoE driver has been updated to version 3.0.23.0 which includes Brocade 1860 16Gbps Fibre Channel Adapter support, new hardware support in Dell PowerEdge 12th Generation servers, and **issue_lip** support. The **bfa** firmware was updated to version 3.0.3.1.

- The **be2iscsi** driver for ServerEngines BladeEngine 2 Open iSCSI devices has been updated to version 4.4.58.0r to add iSCSI netlink VLAN support.

- The **qib** driver for TrueScale HCAs has been updated to the latest version with the following enhancements:

  - Enhanced NUMA awareness

  - Congestion Control Agent (CCA) for Performance Scale Messaging (PSM) fabrics

  - Dual Rail for PSM fabrics

  - Performance enhancements and bug fixes

- The following drivers have been updated to include latest upstream features and bug fixes: **ahci**, **md**/**bitmap**, **raid0**, **raid1**, **raid10**, and **raid456**.

Network Drivers

- The **netxen_nic** driver for NetXen Multi port (1/10) Gigabit Network has been updated to version 4.0.80, which adds miniDIMM support. The **netxen_nic** firmware has been updated to version 4.0.588.

- The **bnx2x** driver has been updated to the version 1.72.51-0 to include support for Broadcom 57800/57810/57811/57840 chips as well as general bug fixes and updated firmware for Broadcom 57710/57711/57712 chips. This update also includes the following enhancements:

  - Support for iSCSI offload and Data Center Bridging/Fibre Channel over Ethernet (DCB/FCOE) on Broadcom 57712/578xx chips. The Broadcom 57840 chip is supported in a 4x10G configuration only and does not support iSCSI offload and FCoE. Future releases will support additional configurations and iSCSI offload and FCoE.

  - Additional physical layer support, including Energy Efficient Ethernet (EEE).

  - iSCSI offload enhancements

  - OEM-specific features

- The **be2net** driver for Emulex OneConnect 10GbE Network Adapters has been updated to version 4.4.31.0r. The SR-IOV functionality of the Emulex **be2net** driver is now fully supported in Red Hat Enterprise Linux 6.4. SR-IOV runs on all Emulex-branded and OEM variants of BE3-based hardware (with minimum firmware version 4.2.324.30), which all require the **be2net** driver software.

- The **ixgbevf** driver has been updated to version 2.6.0-k to include the latest hardware support, enhancements, and bug fixes.

- The **cxgb4** driver for Chelsio Terminator4 10G Unified Wire Network Controllers has been updated to add support for Chelsio's T480-CR and T440-LP-CR adapters.
- The **cxgb3** driver for the Chelsio T3 Family of network devices has been updated to version 1.1.5-ko.
- The **ixgbe** driver for Intel 10 Gigabit PCI Express network devices has been updated to version 3.9.15-k to include support for SR-IOV with Data Center Bridging (DCB) or Receive-Side Scaling (RSS), PTP support as a Technology Preview, latest hardware support, enhancements, and bug fixes.
- The **iw_cxgb3** driver has been updated.
- The **iw_cxgb4** driver has been updated.
- The **e1000e** driver for Intel PRO/1000 network devices has been updated to add the latest hardware support, features, and provide a number of bug fixes.
- The **enic** driver for Cisco 10G Ethernet devices has been updated to version 2.1.1.39.
- The **igbvf** driver (Intel Gigabit Virtual Function Network driver) has been updated to the latest upstream version.
- The **igb** driver for Intel Gigabit Ethernet Adapters has been updated to version 4.0.1 to add the latest hardware support. Also, PTP support has been added to the **igb** driver as a Technology Preview.
- The **tg3** driver for Broadcom Tigon3 Ethernet devices has been updated to version 3.124 to add new hardware support. Also, PTP support has been added to the **tg3** driver as a Technology Preview.
- The **qlcnic** driver for the HP NC-Series QLogic 10 Gigabit Server Adapters has been updated to version 5.0.29.
- The Brocade **bna** driver for Brocade 10Gb PCIe Ethernet Controllers driver has been updated to version 3.0.23.0 to add new hardware support for Dell PowerEdge 12th Generation servers, and enable the use of non-Brocade Twinax Copper cables. The **bna** firmware was updated to version 3.0.3.1.
- The Broadcom NetXtreme II **cnic** driver has been updated to version 2.5.13 to include new features, bug fixes, and support for new OEM platforms.
- The wireless drivers have been updated to upstream version 3.5, including the **iwlwifi** driver for Intel wireless LAN adapters and the **ath9k** driver for PCI/PCI-Express adapters with Atheros wireless LAN chipsets. Additionally, the **rt2800pci** and **rt2800usb** drivers have been added to support various USB and PCI/PCI-Express adapters with Ralink wireless LAN chipsets.

Miscellaneous Drivers

- The **intel_idle** cpuidle driver for Intel processors has been updated to add support for Intel's Xeon E5-XXX V2 series of processors.
- The **wacom** driver has been updated to add support for the CTL-460 Wacom Bamboo Pen, the Wacom Intuos5 Tablet, and the Wacom Cintiq 22HD Pen Display.

- The ALSA HDA audio driver has been updated to enable or improve support for new hardware and fix a number of bugs.
- The **`mlx4_en`** driver has been updated to the latest upstream version.
- The **`mlx4_ib`** driver has been updated to the latest upstream version.
- The **`mlx4_core`** driver has been updated to the latest upstream version.
- The **`z90crypt`** device driver has been updated to support the new Crypto Express 4 (CEX4) adapter card.

CHAPTER 3. DEPRECATED FUNCTIONALITY

`systemtap` component

The systemtap-grapher package has been removed from Red Hat Enterprise Linux 6. For more information, see https://access.redhat.com/solutions/757983.

`matahari` component

The **Matahari** agent framework (matahari-*) packages have been removed from Red Hat Enterprise Linux 6. Focus for remote systems management has shifted towards the use of the CIM infrastructure. This infrastructure relies on an already existing standard which provides a greater degree of interoperability for all users.

`distribution` component

The following packages have been deprecated and are subjected to removal in a future release of Red Hat Enterprise Linux 6. These packages will not be updated in the Red Hat Enterprise Linux 6 repositories and customers who do not use the MRG-Messaging product are advised to uninstall them from their system.

- mingw-gcc
- mingw-boost
- mingw32-qpid-cpp
- python-qmf
- python-qpid
- qpid-cpp
- qpid-qmf
- qpid-tests
- qpid-tools
- ruby-qpid
- saslwrapper

Red Hat MRG-Messaging customers will continue to receive updated functionality as part of their regular updates to the product.

`fence-virt` component

The **libvirt-qpid** is no longer part of the fence-virt package.

openscap component

The openscap-perl subpackage has been removed from openscap.

CHAPTER 4. TECHNOLOGY PREVIEWS

This chapter provides a list of all available Technology Previews in Red Hat Enterprise Linux 6.4.

Technology Preview features are currently not supported under Red Hat Enterprise Linux subscription services, may not be functionally complete, and are generally not suitable for production use. However, these features are included as a customer convenience and to provide the feature with wider exposure.

Customers may find these features useful in a non-production environment. Customers are also free to provide feedback and functionality suggestions for a Technology Preview feature before it becomes fully supported. Errata will be provided for high-severity security issues.

During the development of a Technology Preview feature, additional components may become available to the public for testing. It is the intention of Red Hat clustering to fully support Technology Preview features in a future release.

4.1. STORAGE AND FILE SYSTEMS

Cross Realm Kerberos Trust Functionality for samba4 Libraries

The Cross Realm Kerberos Trust functionality provided by Identity Management, which relies on the capabilities of the samba4 client library, is included as a Technology Preview starting with Red Hat Enterprise Linux 6.4. This functionality uses the libndr-nbt library to prepare Connection-less Lightweight Directory Access Protocol (CLDAP) messages.

Package: samba-3.6.9-151

Open multicast ping (Omping), BZ#657370

Open Multicast Ping (Omping) is a tool to test the IP multicast functionality, primarily in the local network. This utility allows users to test IP multicast functionality and assists in the diagnosing if an issues is in the network configuration or elsewhere (that is, a bug). In Red Hat Enterprise Linux 6 Omping is provided as a Technology Preview.

Package: omping-0.0.4-1

System Information Gatherer and Reporter (SIGAR)

The System Information Gatherer and Reporter (SIGAR) is a library and command-line tool for accessing operating system and hardware level information across multiple platforms and programming languages. In Red Hat Enterprise Linux 6.4, SIGAR is considered a Technology Preview package.

Package: sigar-1.6.5-0.4.git58097d9

fsfreeze

Red Hat Enterprise Linux 6 includes **fsfreeze** as a Technology Preview. **fsfreeze** is a new command that halts access to a file system on a disk. **fsfreeze** is designed to be used with hardware RAID devices, assisting in the creation of volume snapshots. For more details on the **fsfreeze** utility, refer to the `fsfreeze(8)` man page.

Package: util-linux-ng-2.17.2-12.9

DIF/DIX support

DIF/DIX, is a new addition to the SCSI Standard and a Technology Preview in Red Hat Enterprise Linux 6. DIF/DIX increases the size of the commonly used 512-byte disk block from 512 to 520 bytes, adding the Data Integrity Field (DIF). The DIF stores a checksum value for the data block that is calculated by the Host Bus Adapter (HBA) when a write occurs. The storage device then confirms the checksum on receive, and stores both the data and the checksum. Conversely, when a read occurs, the checksum can be checked by the storage device, and by the receiving HBA.

The DIF/DIX hardware checksum feature must only be used with applications that exclusively issue ***O_DIRECT*** I/O. These applications may use the raw block device, or the XFS file system in ***O_DIRECT*** mode. (XFS is the only file system that does not fall back to buffered I/O when doing certain allocation operations.) Only applications designed for use with ***O_DIRECT*** I/O and DIF/DIX hardware should enable this feature.

For more information, refer to section *Block Devices with DIF/DIX Enabled* in the Storage Administration Guide.

Package: kernel-2.6.32-358

Filesystem in user space

Filesystem in Userspace (FUSE) allows for custom file systems to be developed and run in user space.

Package: fuse-2.8.3-4

Btrfs, BZ#614121

Btrfs is under development as a file system capable of addressing and managing more files, larger files, and larger volumes than the ext2, ext3, and ext4 file systems. Btrfs is designed to make the file system tolerant of errors, and to facilitate the detection and repair of errors when they occur. It uses checksums to ensure the validity of data and metadata, and maintains snapshots of the file system that can be used for backup or repair. The Btrfs Technology Preview is only available on AMD64 and Intel 64 architectures.

> **WARNING**
>
> Red Hat Enterprise Linux 6 includes Btrfs as a technology preview to allow you to experiment with this file system. You should not choose Btrfs for partitions that will contain valuable data or that are essential for the operation of important systems.

Package: btrfs-progs-0.20-0.2.git91d9eec

LVM Application Programming Interface (API)

Red Hat Enterprise Linux 6 features the new LVM application programming interface (API) as a Technology Preview. This API is used to query and control certain aspects of LVM.

Package: lvm2-2.02.98-9

FS-Cache

FS-Cache in Red Hat Enterprise Linux 6 enables networked file systems (for example, NFS) to have a persistent cache of data on the client machine.

Package: cachefilesd-0.10.2-1

eCryptfs File System

eCryptfs is a stacked, cryptographic file system. It is transparent to the underlying file system and provides per-file granularity. eCryptfs is provided as a Technology Preview in Red Hat Enterprise Linux 6.

Package: ecryptfs-utils-82-6

4.2. NETWORKING

linuxptp

The linuxptp package, included in Red Hat Enterprise Linux 6.4 as a Technology Preview, is an implementation of the Precision Time Protocol (PTP) according to IEEE standard 1588 for Linux. The dual design goals are to provide a robust implementation of the standard and to use the most relevant and modern Application Programming Interfaces (API) offered by the Linux kernel. Supporting legacy APIs and other platforms is not a goal.

Package: linuxptp-0-0.6.20121114gite6bbbb

PTP support in kernel drivers

PTP support has been added as a technology preview to the ixgbe, igb, and tg3 kernel drivers.

Packages: kernel-2.6.32-335

QFQ queuing discipline

In Red Hat Enterprise Linux 6, the **tc** utility has been updated to work with the Quick Fair Scheduler (QFQ) kernel features. Users can now take advantage of the new QFQ traffic queuing discipline from userspace. This feature is considered a Technology Preview.

Package: kernel-2.6.32-358

vios-proxy, BZ#721119

vios-proxy is a stream-socket proxy for providing connectivity between a client on a virtual guest and a server on a Hypervisor host. Communication occurs over virtio-serial links.

Package: vios-proxy-0.1-1

IPv6 support in IPVS

The IPv6 support in IPVS (IP Virtual Server) is considered a Technology Preview.

Package: kernel-2.6.32-358

4.3. CLUSTERING AND HIGH AVAILABILITY

pcs

The pcs package has been added to Red Hat Enterprise Linux 6 as a Technology Preview. This package provides a command-line tool configure and manage the **corosync** and **pacemaker** utilities.

Package: pcs-0.9.26-10

luci support for fence_sanlock

The **luci** tool now supports the Sanlock fence agent as a Technology Preview, which is available in the luci's list of agents.

Package: luci-0.26.0-37

Recovering a node via a hardware watchdog device

New fence_sanlock agent and checkquorum.wdmd, included in Red Hat Enterprise Linux 6.4 as a Technology Preview, provide new mechanisms to trigger the recovery of a node via a hardware watchdog device. Tutorials on how to enable this Technology Preview will be available at https://fedorahosted.org/cluster/wiki/HomePage

Note that SELinux in enforcing mode is currently not supported.

Package: cluster-3.0.12.1-49

keepalived

Red Hat Enterprise Linux 6.4 includes the keepalived package as a Technology Preview. The keepalived package provides simple and robust facilities for load-balancing and high-availability. The load-balancing framework relies on the well-know and widely used Linux Virtual Server kernel module providing Layer4 network load-balancing. The keepalived daemon implements a set of health checkers to load-balanced server pools according to their state. The keepalived daemon also implements the Virtual Router Redundancy Protocol (VRRP), allowing router or director failover to achieve high availability.

Package: keepalived-1.2.7-3

HAProxy

HAProxy is a stand-alone, layer-7, high-performance network load balancer for TCP and HTTP-based applications which can perform various types of scheduling based on the content of the HTTP requests. Red Hat Enterprise Linux 6.4 introduces the haproxy package as a Technology Preview.

Package: haproxy-1.4.22-3

libqb package

The libqb package provides a library with the primary purpose of providing high performance client server reusable features, such as high performance logging, tracing, inter-process communication, and polling. This package is introduced as a dependency of the pacemaker package, and is considered a Technology Preview.

Package: libqb-0.14.2-3

pacemaker, BZ#456895

Pacemaker, a scalable high-availability cluster resource manager, is included in Red Hat Enterprise Linux 6 as a Technology Preview. Pacemaker is not fully integrated with the Red Hat cluster stack.

Package: pacemaker-1.1.8-7

4.4. AUTHENTICATION

Simultaneous maintaining of TGTs for multiple KDCs

Kerberos version 1.10 added a new cache storage type, DIR:, which allows Kerberos to maintain Ticket Granting Tickets (TGTs) for multiple Key Distribution Centers (KDCs) simultaneously and auto-select between them when negotiating with Kerberized resources. In Red Hat Enterprise Linux 6.4, SSSD has been enhanced to allow you to select the DIR: cache for users that are logging in via SSSD. This feature is introduced as a Technology Preview.

Package: sssd-1.9.2-82

4.5. SECURITY

TPM

TPM (Trusted Platform Module) hardware can create, store and use RSA keys securely (without ever being exposed in memory), verify a platform's software state using cryptographic hashes and more. The trousers and tpm-tools packages are considered a Technology Preview.

Packages: trousers-0.3.4-4, tpm-tools-1.3.4-2

4.6. DEVICES

mpt2sas lockless mode

The **`mpt2sas`** driver is fully supported. However, when used in the lockless mode, the driver is a Technology Preview.

Package: kernel-2.6.32-358

4.7. KERNEL

Thin-provisioning and scalable snapshot capabilities

The **`dm-thinp`** targets, **`thin`** and **`thin-pool`**, provide a device mapper device with thin-provisioning and scalable snapshot capabilities. This feature is available as a Technology Preview.

Package: kernel-2.6.32-358

Kernel Media support

The following features are presented as Technology Previews:

- The latest upstream video4linux
- Digital video broadcasting
- Primarily infrared remote control device support
- Various webcam support fixes and improvements

Package: kernel-2.6.32-358

Remote audit logging

The audit package contains the user space utilities for storing and searching the audit records generated by the **`audit`** subsystem in the Linux 2.6 kernel. Within the audispd-plugins sub-package is a utility that allows for the transmission of audit events to a remote aggregating machine. This remote audit logging application, **audisp-remote**, is considered a Technology Preview in Red Hat Enterprise Linux 6.

Package: audispd-plugins-2.2-2

Linux (NameSpace) Container [LXC]

Linux containers provide a flexible approach to application runtime containment on bare-metal systems without the need to fully virtualize the workload. Red Hat Enterprise Linux 6 provides application level containers to separate and control the application resource usage policies via cgroups and namespaces. This release includes basic management of container life-cycle by allowing creation, editing and deletion of containers via the **libvirt** API and the **virt-manager** GUI. Linux Containers are a Technology Preview.

Packages: libvirt-0.9.10-21, virt-manager-0.9.0-14

Diagnostic pulse for the fence_ipmilan agent, BZ#655764

A diagnostic pulse can now be issued on the IPMI interface using the **`fence_ipmilan`** agent. This new Technology Preview is used to force a kernel dump of a host if the host is configured to do so. Note that this feature is not a substitute for the **`off`** operation in a production cluster.

Package: fence-agents-3.1.5-25

4.8. VIRTUALIZATION

Performance monitoring in KVM guests, BZ#645365

KVM can now virtualize a performance monitoring unit (vPMU) to allow virtual machines to use performance monitoring. Note that the **`-cpu`** flag must be set when using this feature.

With this feature, Red Hat virtualization customers running Red Hat Enterprise Linux 6 guests can use the CPU's PMU counter while using the performance tool for profiling. The virtual performance monitoring unit feature allows virtual machine users to identify sources of performance problems in their guests, thereby improving the ability to profile a KVM guest from the host.

This feature is a Technology Preview in Red Hat Enterprise Linux 6.4.

Package: kernel-2.6.32-358

Dynamic virtual CPU allocation

KVM now supports dynamic virtual CPU allocation, also called vCPU hot plug, to dynamically manage capacity and react to unexpected load increases on their platforms during off-peak hours.

The virtual CPU hot-plugging feature gives system administrators the ability to dynamically adjust CPU resources in a guest. Because a guest no longer has to be taken offline to adjust the CPU resources, the availability of the guest is increased.

This feature is a Technology Preview in Red Hat Enterprise Linux 6.4. Currently, only the vCPU hot-add functionality works. The vCPU hot-unplug feature is not yet implemented.

Package: qemu-kvm-0.12.1.2-2.355

System monitoring via SNMP, BZ#642556

This feature provides KVM support for stable technology that is already used in data center with bare metal systems. SNMP is the standard for monitoring and is extremely well understood as well as computationally efficient. System monitoring via SNMP in Red Hat Enterprise Linux 6 allows the KVM hosts to send SNMP traps on events so that hypervisor events can be communicated to the user via standard SNMP protocol. This feature is provided through the addition of a new package: libvirt-snmp. This feature is a Technology Preview.

Package: libvirt-snmp-0.0.2-3

Wire speed requirement in KVM network drivers

Virtualization and cloud products that run networking work loads need to run wire speeds. Up until Red Hat Enterprise Linux 6.1, the only way to reach wire speed on a 10 GB Ethernet NIC with a lower CPU utilization was to use PCI device assignment (passthrough), which limits other features like memory overcommit and guest migration

The **macvtap**/**vhost** zero-copy capabilities allow the user to use those features when high performance is required. This feature improves performance for any Red Hat Enterprise Linux 6.x guest in the VEPA use case. This feature is introduced as a Technology Preview.

Package: qemu-kvm-0.12.1.2-2.355

CHAPTER 5. KNOWN ISSUES

5.1. INSTALLATION

anaconda component, BZ#895982

Physical-extents size less than 32MB on top of an MD physical volume leads to problems with calculating the capacity of a volume group. To work around this problem, use a physical-extent size of 32MB or leave space double the physical-extent size free when allocating logical volumes. Another option is to change the default 4MB size of a physical extent to 32MB.

anaconda component, BZ#875644

After upgrading the system using kickstart, IBM System z machines halt instead of rebooting, despite the instruction to reboot. To work around this problem, boot the system manually.

anaconda component

Setting the qla4xxx parameter ***ql4xdisablesysfsboot*** to **1** may cause boot from SAN failures.

anaconda component

To automatically create an appropriate partition table on disks that are uninitialized or contain unrecognized formatting, use the **zerombr** kickstart command. The **--initlabel** option of the **clearpart** command is not intended to serve this purpose.

anaconda component, BZ#676025

Users performing an upgrade using the Anaconda's text mode interface who do not have a boot loader already installed on the system, or who have a non-GRUB boot loader, need to select **Skip Boot Loader Configuration** during the installation process. Boot loader configuration will need to be completed manually after installation. This problem does not affect users running Anaconda in the graphical mode (graphical mode also includes VNC connectivity mode).

anaconda component

On s390x systems, you cannot use automatic partitioning and encryption. If you want to use storage encryption, you must perform custom partitioning. Do not place the **/boot** volume on an encrypted volume.

anaconda component

The order of device names assigned to USB attached storage devices is not guaranteed. Certain USB attached storage devices may take longer to initialize than others, which can result in the device receiving a different name than you expect (for example, **sdc** instead of **sda**).

During installation, verify the storage device size, name, and type when configuring partitions and file systems.

kernel component

Recent Red Hat Enterprise Linux 6 releases use a new naming scheme for network interfaces on some machines. As a result, the installer may use different names during an upgrade in certain scenarios (typically **em1** is used instead of **eth0** on new Dell machines). However, the previously used network interface names are preserved on the system and the upgraded system will still use the previously used interfaces. This is not the case for Yum upgrades.

anaconda component

The **`kdump default on`** feature currently depends on Anaconda to insert the ***`crashkernel=`*** parameter to the kernel parameter list in the boot loader's configuration file.

`firstaidkit` component

The firstaidkit-plugin-grub package has been removed from Red Hat Enterprise Linux 6.2. As a consequence, in rare cases, the system upgrade operation may fail with unresolved dependencies if the plug-in has been installed in a previous version of Red Hat Enterprise Linux. To avoid this problem, the firstaidkit-plugin-grub package should be removed before upgrading the system. However, in most cases, the system upgrade completes as expected.

anaconda component, BZ#623261

In some circumstances, disks that contain a whole disk format (for example, an LVM Physical Volume populating a whole disk) are not cleared correctly using the **`clearpart --initlabel`** kickstart command. Adding the **`--all`** switch—as in **`clearpart --initlabel --all`**—ensures disks are cleared correctly.

anaconda component

When installing on the IBM System z architecture, if the installation is being performed over SSH, avoid resizing the terminal window containing the SSH session. If the terminal window is resized during the installation, the installer will exit and the installation will terminate.

`yaboot` component, BZ#613929

The kernel image provided on the CD/DVD is too large for Open Firmware. Consequently, on the POWER architecture, directly booting the kernel image over a network from the CD/DVD is not possible. Instead, use **yaboot** to boot from a network.

anaconda component

The Anaconda partition editing interface includes a button labeled **`Resize`**. This feature is intended for users wishing to shrink an existing file system and an underlying volume to make room for an installation of a new system. Users performing manual partitioning cannot use the **`Resize`** button to change sizes of partitions as they create them. If you determine a partition needs to be larger than you initially created it, you must delete the first one in the partitioning editor and create a new one with the larger size.

`system-config-kickstart` component

Channel IDs (read, write, data) for network devices are required for defining and configuring network devices on IBM S/390 systems. However, **system-config-kickstart**—the graphical user interface for generating a kickstart configuration—cannot define channel IDs for a network device. To work around this issue, manually edit the kickstart configuration that **system-config-kickstart** generates to include the desired network devices.

5.2. ENTITLEMENT

`subscription-manager` component

When **firstboot** is running in text mode, the user can only register via Red Hat Network Register, not with **subscription-manager**. Both are available in GUI mode.

`subscription-manager` component

If multiple repositories are enabled, **subscription-manager** installs product certificates from all repositories instead of installing the product certificate only from the repository from which the RPM package was installed.

`subscription-manager` component

firstboot fails to provide Red Hat Network registration to a virtual machine in a NAT-based network; for example, in the **libvirt** environment. Note that this problem only occurs during the first boot after installation. If you run **firstboot** manually later, the registration finishes successfully.

5.3. DEPLOYMENT

`389-ds-base` component, BZ#878111

The **ns-slapd** utility terminates unexpectedly if it cannot rename the **`dirsrv-<instance>`** log files in the **`/var/log/`** directory due to incorrect permissions on the directory.

`cpuspeed` component, BZ#626893

Some HP Proliant servers may report incorrect CPU frequency values in **`/proc/cpuinfo`** or **`/sys/device/system/cpu/*/cpufreq`**. This is due to the firmware manipulating the CPU frequency without providing any notification to the operating system. To avoid this ensure that the **`HP Power Regulator`** option in the BIOS is set to ***`OS Control`***. An alternative available on more recent systems is to set **`Collaborative Power Control`** to ***`Enabled`***.

`releng` component, BZ#644778

Some packages in the Optional repositories on RHN have multilib file conflicts. Consequently, these packages cannot have both the primary architecture (for example, x86_64) and secondary architecture (for example, i686) copies of the package installed on the same machine simultaneously. To work around this issue, install only one copy of the conflicting package.

`grub` component, BZ#695951

On certain UEFI-based systems, you may need to type **`BOOTX64`** rather than **`bootx64`** to boot the installer due to case sensitivity issues.

`grub` component, BZ#698708

When rebuilding the grub package on the x86_64 architecture, the glibc-static.i686 package must be used. Using the glibc-static.x86_64 package will not meet the build requirements.

5.4. VIRTUALIZATION

`qemu-kvm` component, BZ#1159613

If a **`virtio`** device is created where the number of vectors is set to a value higher than 32, the device behaves as if it was set to a zero value on Red Hat Enterprise Linux 6, but not on Enterprise Linux 7. The resulting vector setting mismatch causes a migration error if the number of vectors on any **`virtio`** device on either platform is set to 33 or higher. It is, therefore, not recommended to set the **`vector`** value to be greater than 32.

`kernel` component

In Red Hat Enterprise Linux 6.4, if Large Receive Offload (LRO) is enabled with the **`macvtap`** driver, a kernel panic can occur on the host machine. This problem was observed on machines using Broadcom, QLogic and Intel cards. To work around the problem, disable LRO by running **`ethtool -K large-receive-offload off`**.

`kernel` component

There is a known issue with the Microsoft Hyper-V host. If a legacy network interface controller (NIC) is used on a multiple-CPU virtual machine, there is an interrupt problem in the emulated hardware when the IRQ balancing daemon is running. Call trace information is logged in the **`/var/log/messages`** file.

`libvirt` component, BZ#888635

Under certain circumstances, virtual machines try to boot from an incorrect device after a network boot failure. For more information, please refer to this article on Customer Portal.

`qemu-kvm` component, BZ#894277

"Fast startup" used in Microsoft Windows 8 is not fully compatible with **qemu-kvm** in Red Hat Enterprise Linux 6. Windows 8 can therefore fail to boot the second time after its shutdown. To ensure successful boot of Windows 8 inside **qemu-kvm**, disable Windows 8 "fast startup" in **System Settings**.

numad component, BZ#872524

If **numad** is run on a system with a task that has very large resident memory (>= 50% total system memory), then the numad-initiated NUMA page migrations for that task can cause swapping. The swapping can then induce long latencies for the system. An example is running a 256GB Microsoft Windows KVM Virtual Machine on a 512GB host. The Windows guest will fault in all pages on boot in order to zero them. On a four node system, **numad** will detect that a 256GB task can fit in a subset of two or three nodes, and then attempt to migrate it to that subset. Swapping can then occur and lead to latencies. These latencies may then cause the Windows guest to hang, as timing requirements are no longer met. Therefore, on a system with only one or two very large Windows machines, it is recommended to disable **numad**.

Note that this problem is specific to Windows 2012 guests that use more memory than exists in a single node. Windows 2012 guests appear to allocate memory more gradually than other Windows guest types, which triggers the issue. Other varieties of Windows guests do not seem to experience this problem. You can work around this problem by:

- limiting Windows 2012 guests to less memory than exists in a given node -- so on a typical 4 node system with even memory distribution, the guest would need to be less than the total amount of system memory divided by 4; or

- allowing the Windows 2012 guests to finish allocating all of its memory before allowing **numad** to run. **numad** will handle extremely huge Windows 2012 guests correctly after allowing a few minutes for the guest to finish allocating all of its memory.

`grubby` component, BZ#893390

When a Red Hat Enterprise Linux 6.4 guest updates the kernel and then the guest is turned of through Microsoft Hyper-V Manager, the guest fails to boot due to incomplete grub information. This is because the data is not synced properly to disk when the machine is turned off through Hyper-V Manager. To work around this problem, execute the **`sync`** command before turning the guest off.

`kernel` component

Using the mouse scroll wheel does not work on Red Hat Enterprise Linux 6.4 guests that run under Microsoft Hyper-V Manager installed on a physical machine. However, the scroll wheel works as expected when the **vncviewer** utility is used.

`kernel` component, BZ#874406

Microsoft Windows Server 2012 guests using the e1000 driver can become unresponsive consuming 100% CPU during reboot.

`kernel` component

When a kernel panic is triggered on a Microsoft Hyper-V guest, the **kdump** utility does not capture the kernel error information; an error is only displayed on the command line.

`kernel` component

Due to a bug in Microsoft Hyper-V Server 2008 R2, attempting to remove and then reload the hv_utils module on a Hyper-V guest running Red Hat Enterprise Linux 6.4 will cause a shutdown and the heartbeat service to not work. To work around this issue, upgrade the host system to Microsoft Hyper-V Server 2012.

`quemu-kvm` component, BZ#871265

AMD Opteron G1, G2 or G3 CPU models on **qemu-kvm** use the family and models values as follows: family=15 and model=6. If these values are larger than 20, the **`lahfm_lm`** CPU feature is ignored by Linux guests, even when the feature is enabled. To work around this problem, use a different CPU model, for example AMD Opteron G4.

`qemu-kvm` component, BZ#860929

KVM guests must not be allowed to update the host CPU microcode. KVM does not allows this and instead always returns the same microcode revision or patch level value to the guest. If the guest tries to update the CPU microcode, it will fail and show an error message similar to:

```
CPU0: update failed (for patch_level=0x6000624)
```

To work around this, configure the guest to not install CPU microcode updates; for example, uninstall the microcode_ctl package Red Hat Enterprise Linux of Fedora guests.

`virt-p2v` component, BZ#816930

Converting a physical server running either Red Hat Enterprise Linux 4 or Red Hat Enterprise Linux 5 which has its file system root on an MD device is not supported. Converting such a guest results in a guest which fails to boot. Note that conversion of a Red Hat Enterprise Linux 6 server which has its root on an MD device is supported.

`virt-p2v` component, BZ#808820

When converting a physical host with a multipath storage, Virt-P2V presents all available paths for conversion. Only a single path must be selected. This must be a currently active path.

`virtio-win` component, BZ#615928

The balloon service on Windows 7 guests can only be started by the Administrator user.

`libvirt` component, BZ#622649

libvirt uses transient **iptables** rules for managing NAT or bridging to virtual machine guests. Any external command that reloads the **iptables** state (such as running **system-config-firewall**) will overwrite the entries needed by **libvirt**. Consequently, after running any command or tool that changes the state of **iptables**, guests may lose access to the network. To work around this issue, use the **`service libvirt reload`** command to restore **libvirt**'s additional **iptables** rules.

`virtio-win` component, BZ#612801

A Windows virtual machine must be restarted after the installation of the kernel Windows driver framework. If the virtual machine is not restarted, it may crash when a memory balloon operation is performed.

`qemu-kvm` component, BZ#720597

Installation of Windows 7 Ultimate x86 (32-bit) Service Pack 1 on a guest with more than 4GB of RAM and more than one CPU from a DVD medium often crashes during the final steps of the installation process due to a system hang. To work around this issue, use the Windows Update utility to install the Service Pack.

`qemu-kvm` component, BZ#612788

A dual function Intel 82576 Gigabit Ethernet Controller interface (codename: Kawela, PCI Vendor/Device ID: 8086:10c9) cannot have both physical functions (PF's) device-assigned to a Windows 2008 guest. Either physical function can be device assigned to a Windows 2008 guest (PCI function 0 or function 1), but not both.

`virt-v2v` component, BZ#618091

The **virt-v2v** utility is able to convert guests running on an ESX server. However, if an ESX guest has a disk with a snapshot, the snapshot must be on the same datastore as the underlying disk storage. If the snapshot and the underlying storage are on different datastores, **virt-v2v** will report a 404 error while trying to retrieve the storage.

`virt-v2v` component, BZ#678232

The VMware Tools application on Microsoft Windows is unable to disable itself when it detects that it is no longer running on a VMware platform. Consequently, converting a Microsoft Windows guest from VMware ESX, which has VMware Tools installed, will result in errors. These errors usually manifest as error messages on start-up, and a "Stop Error" (also known as a BSOD) when shutting down the guest. To work around this issue, uninstall VMware Tools on Microsoft Windows guests prior to conversion.

5.5. STORAGE AND FILE SYSTEMS

anaconda component

In UEFI mode, when creating a partition for software RAID, **anaconda** can be unable to allocate the **`/boot/efi`** mount point to the software RAID partition and fails with the "have not created /boot/efi" message in such a scenario.

`Driver Update Disk` component, BZ#904945

The hpsa driver installed from the AMD64 and Intel 64 Driver Update Program ISO might not be loaded properly on Red Hat Enterprise Linux 6.3. Consequently, the system can become unresponsive. To work around this problem, use the **`pci=nomsi`** kernel parameter before installing the driver from the ISO.

kernel component, BZ#918647

Thin provisioning uses reference counts to indicate that data is shared between a thin volume and snapshots of the thin volume. There is a known issue with the way reference counts are managed in the case when a discard is issued to a thin volume that has snapshots. Creating snapshots of a thin volume and then issuing discards to the thin volume can therefore result in data loss in the snapshot volumes. Users are strongly encouraged to disable discard support on the thin-pool for the time being. To do so using lvm2 while the pool is offline, use the **lvchange --discard ignore <pool>** command. Any discards that might be issued to thin volumes will be ignored.

kernel component

Storage that reports a discard_granularity that is not a power of two will cause the kernel to improperly issue discard requests to the underlying storage. This results in I/O errors associated with the failed discard requests. To work around the problem, if possible, do not upgrade to newer vendor storage firmware that reports discard_granularity that is not a power of two.

parted component

Users might be unable to access a partition created by **parted**. To work around this problem, reboot the machine.

lvm2 component, BZ#852812

When filling a thin pool to 100% by writing to thin volume device, access to all thin volumes using this thin pool can be blocked. To prevent this, try not to overfill the pool. If the pool is overfilled and this error occurs, extend the thin pool with new space to continue using the pool.

dracut component

The Qlogic QLA2xxx driver can miss some paths after booting from Storage Area Network (SAN). To workaround this problem, run the following commands:

```
echo "options qla2xxx ql2xasynclogin=0" > /etc/modprobe.d/qla2xxx.conf
mkinitrd  /boot/initramfs-`uname -r`.img `uname -r` --force
```

lvm2 component, BZ#903411

Activating a logical volume can fail if the **--thinpool** and **--discards** options are specified on logical-volume creation. To work around this problem, manually deactivate all thin volumes related to the changed thin pool prior to running the **lvchange** command.

kernel component

Unloading the **nfs** module can cause the system to terminate unexpectedly if the **fsx** utility was ran with NFSv4.1 before.

kernel component

Due to a bug in the CIFS mount code, it is not possible to mount Distributed File System (DFS) shares in Red Hat Enterprise Linux 6.4.

device-mapper-multipath component

When the **multipathd** service is not running, failed devices will not be restored. However, the multipath command gives no indication that multipathd is not running. Users can unknowingly set up multipath devices without starting the **multipathd** service, keeping failed paths from automatically getting restored. Make sure to start multipathing by

- either running:

  ```
  ~]# mpathconf --enable
  ~]# service multipathd start
  ```

- or:

  ```
  ~]# chkconfig multipathd on
  ~]# service multipathd start
  ```

multipathd will automatically start on boot, and multipath devices will automatically restore failed paths.

lvm2 component, BZ#837603

When the administrator disables use of the **lvmetad** daemon in the **lvm.conf** file, but the daemon is still running, the cached metadata are remembered until the daemon is restarted. However, if the **use_lvmetad** parameter in **lvm.conf** is reset to **1** without an intervening **lvmetad** restart, the cached metadata can be incorrect. Consequently, VG metadata can be overwritten with previous versions. To work around this problem, stop the **lvmedat** daemon manually when disabling **use_lvmetad** in **lvm.conf**. The daemon can only be restarted after **use_lvmetad** has been set to 1. To recover from an out-of-sync **lvmetad** cache, execute the **pvscan --cache** command or restart **lvmetad**. To restore metadata to correct versions, use **vgcfrestore** with a corresponding file in **/etc/lvm/archive**.

lvm2 component, BZ#563927

Due to the limitations of the LVM 'mirror' segment type, it is possible to encounter a deadlock situation when snapshots are created of mirrors. The deadlock can occur if snapshot changes (e.g. creation, resizing or removing) happen at the same time as a mirror device failure. In this case, the mirror blocks I/O until LVM can respond to the failure, but the snapshot is holding the LVM lock while trying to read the mirror.

If the user wishes to use mirroring and take snapshots of those mirrors, then it is recommended to use the 'raid1' segment type for the mirrored logical volume instead. This can be done by adding the additional arguments '--type raid1' to the command that creates the mirrored logical volume, as follows:

```
~]$ lvcreate --type raid1 -m 1 -L 1G -n my_mirror my_vg
```

kernel component, BZ#606260

The NFSv4 server in Red Hat Enterprise Linux 6 currently allows clients to mount using UDP and advertises NFSv4 over UDP with **rpcbind**. However, this configuration is not supported by Red Hat and violates the RFC 3530 standard.

lvm2 component

The **pvmove** command cannot currently be used to move mirror devices. However, it is possible to move mirror devices by issuing a sequence of two commands. For mirror images, add a new image on the destination PV and then remove the mirror image on the source PV:

```
~]$ lvconvert -m +1 <vg/lv> <new PV>
~]$ lvconvert -m -1 <vg/lv> <old PV>
```

Mirror logs can be handled in a similar fashion:

```
~]$ lvconvert --mirrorlog core <vg/lv>
~]$ lvconvert --mirrorlog disk <vg/lv> <new PV>
```

or

```
~]$ lvconvert --mirrorlog mirrored <vg/lv> <new PV>
~]$ lvconvert --mirrorlog disk <vg/lv> <old PV>
```

5.6. NETWORKING

samba4 component, BZ#878168

If configured, the Active Directory (AD) DNS server returns IPv4 and IPv6 addresses of an AD server. If the FreeIPA server cannot connect to the AD server with an IPv6 address, running the **ipa trust-add** command will fail even if it would be possible to use IPv4. To work around this problem, add the IPv4 address of the AD server to the **/etc/hosts** file. In this case, the FreeIPA server will use only the IPv4 address and executing **ipa trust-add** will be successful.

kernel component

Destroying the root port before any NPIV ports can cause unexpected system behavior, including a full system crash. Note that one instance where the root port is destroyed before the NPIV ports is when the system is shut down. To work around this problem, destroy NPIV ports before destroying the root port that the NPIV ports were created on. This means that for each created NPIV port, the user should write to the **sysfs vport_delete** interface to delete that NPIV port. This should be done before the root port is destroyed. Users are advised to script the NPIV port deletion and configure the system such that the script is executed before the **fcoe** service is stopped, in the shutdown sequence.

kernel component

A Linux LIO FCoE target causes the **bfa** driver to reset all FCoE targets which might lead to data corruption on LUN. To avoid these problems, do not use the **bfa** driver with a Linux FCoE target.

NetworkManager component, BZ#896198

A **GATEWAY** setting in the **/etc/sysconfig/network** file causes **NetworkManager** to assign that gateway to all interfaces with static IP addresses, even if their configuration did not specify a gateway or specified a different gateway. Interfaces have the incorrect gateway information and the wrong interface may have the default route. Instead of using **GATEWAY** in **/etc/sysconfig/network** to specify which interface receives the default route, set **DEFROUTE=no** in each **ifcfg** file that should *not* have the default route. Any interface connected using configuration from an **ifcfg** file containing **DEFROUTE=no** will never receive the default route.

kernel component

Typically, on platforms with no Intelligent Platform Management Interface (IPMI) hardware the user can see the following message the on the boot console and in **dmesg** log:

```
Could not set up I/O space
```

This message can be safely ignored, unless the system really does have IPMI hardware. In that case, the message indicates that the IPMI hardware could not be initialized. In order to support Advanced Configuration and Power Interface (ACPI) opregion access to IPMI functionality early in the boot, the IPMI driver has been statically linked with the kernel image. This means that the IPMI driver is "loaded" whether or not there is any hardware. The IPMI driver will try to initialize the IPMI hardware, but if there is no IPMI hardware present on the booting platform, the driver will print error messages on the console and in the **dmesg** log. Some of these error messages do not identify themselves as having been issued by the IPMI driver, so they can appear to be serious, when they are harmless.

`kernel` component

Shutting down the **`fcoe-target`** service while the Fibre Channel over Ethernet (FCoE) can lead to a kernel crash. Please minimize FCoE traffic before stopping or restarting this service.

`fcoe-utils` component

After an ixgbe Fibre Channel over Ethernet (FCoE) session is created, server reboot can cause some or all of the FCoE sessions to not be created automatically. To work around this problem, follow the following steps (assuming that *eth0* is the missing NIC for the FCoE session):

```
ifconfig eth0 down
ifconfig eth0 up
sleep 5
dcbtool sc eth0 dcb on
sleep 5
dcbtool sc eth0 pfc e:1 a:1 w:1
dcbtool sc eth0 app:fcoe e:1 a:1 w:1
service fcoe restart
```

`fcoe-target-utils` component

Using **`targetcli`** to configure the FCoE Target will fail with the message **`Could not create RTSRoot in configFS`**. To prevent this, ensure that the **`fcoe-target`** service is running by executing **`service fcoe-target start`**.

`libibverbs` component

The InfiniBand UD transport test utility could become unresponsive when the **`ibv_ud_pingpong`** command was used with a packet size of 2048 or greater. UD is limited to no more than the smallest MTU of any point in the path between point A and B, which is between 0 and 4096 given that the largest MTU supported (but not the smallest nor required) is 4096. If the underlying Ethernet is jumbo frame capable, and with a 4096 IB MTU on an RoCE device, the max packet size that can be used with UD is 4012 bytes.

`bind-dyndb-ldap` component

IPA creates a new DNS zone in two separate steps. When the new zone is created, it is invalid for a short period of time. **`A/AAAA`** records for the name server belonging to the new zone are created after this delay. Sometimes, **BIND** attempts to load this invalid zone and fails. In such a case, reload **BIND** by running either **`rndc reload`** or **`service named restart`**.

`selinux-policy` component

SELinux can prevent the **`nmbd`** service from writing into the **`/var/`**, which breaks NetBIOS name resolution and leads to SELinux AVC denials.

`kernel` component

If multiple DHCP6 servers are configured on multiple VLANs, for example two DHCP6 servers on VLAN1 and VLAN3, the bna driver NIC does not set up a VLAN interface but can get the VLAN3 IPv6 address.

`kernel` component

The latest version of the sfc NIC driver causes lower UDP and TX performance with large amounts of fragmented UDP packets. This problem can be avoided by setting a constant interrupt moderation period (not adaptive moderation) on both sides, sending and receiving.

`kernel` component

When IPv6 is administratively disabled via **`disable=1`** module parameter, all of the IPv6 protocol handlers are disabled. This includes any offload handlers that support TSO/GSO. The lack of handlers results in the host dropping any TSO/GSO IPv6 packets it may receive from the guest. This can cause problems with retransmission on the guest and throughput. If you want to disable IPV6 support on the host administratively while enabling and providing IPv6 support to the guest without incurring a performance penalty:

- set the **`disable_ipv6`** module to 1
- or use the following **sysctl** entries:
  - net.ipv6.conf.all.disable_ipv6 = 1
  - net.ipv6.conf.default.disable_ipv6 = 1

`kernel` component

Some network interface cards (NICs) may not get an IPv4 address assigned after the system is rebooted. To work around this issue, add the following line to the **`/etc/sysconfig/network-scripts/ifcfg-<`*`interface`*`>`** file:

```
LINKDELAY=10
```

`NetworkManager` component, BZ#758076

If a Certificate Authority (CA) certificate is not selected when configuring an 802.1x or WPA-Enterprise connection, a dialog appears indicating that a missing CA certificate is a security risk. This dialog presents two options: ignore the missing CA certificate and proceed with the insecure connection, or choose a CA certificate. If the user elects to choose a CA certificate, this dialog disappears and the user may select the CA certificate in the original configuration dialog.

`samba` component

Current Samba versions shipped with Red Hat Enterprise Linux 6.4 are not able to fully control the user and group database when using the **`ldapsam_compat`** back end. This back end was never designed to run a production LDAP and Samba environment for a long period of time. The **`ldapsam_compat`** back end was created as a tool to ease migration from historical Samba releases (version 2.2.x) to Samba version 3 and greater using the new **`ldapsam`** back end and the new LDAP schema. The **`ldapsam_compat`** back end lack various important LDAP attributes and object classes in order to fully provide full user and group management. In particular, it cannot allocate user and group IDs. In the Red Hat Enterprise Linux Reference Guide, it is pointed out that this back end is likely to be deprecated in future releases. Refer to Samba's documentation for instructions on how to migrate existing setups to the new LDAP schema.

When you are not able to upgrade to the new LDAP schema (though upgrading is strongly recommended and is the preferred solution), you may work around this issue by keeping a dedicated machine running an older version of Samba (v2.2.x) for the purpose of user account management. Alternatively, you can create user accounts with standard LDIF files. The important part is the assignment of user and group IDs. In that case, the old Samba 2.2 algorithmic mapping from Windows RIDs to Unix IDs is the following: *user RID = UID * 2 + 1000*, while for groups it is: *group RID = GID * 2 + 1001*. With these workarounds, users can continue using the **`ldapsam_compat`** back end with their existing LDAP setup even when all the above restrictions apply.

`kernel` component

Because Red Hat Enterprise Linux 6.4 defaults to using Strict Reverse Path filtering, packets are dropped by default when the route for outbound traffic differs from the route of incoming traffic. This is in line with current recommended practice in RFC3704. For more information about this issue please refer to **`/usr/share/doc/kernel-doc-<version>/Documentation/networking/ip-sysctl.txt`** and https://access.redhat.com/site/solutions/53031.

5.7. CLUSTERING

`corosync` component

The redundant ring feature of corosync is not fully supported in combination with InfiniBand or Distributed Lock Manager (DLM). A double ring failure can cause both rings to break at the same time on different nodes. In addition, DLM is not functional if ring0 is down.

`selinux-policy` component

The fence-sanlock agent does not support SELinux in Enforcing mode at the moment.

`lvm2` component, BZ#814779

Clustered environment is not supported by **`lvmetad`** at the moment. If global/use_lvmetad=1 is used together with global/locking_type=3 configuration setting (clustered locking), the use_lvmetad setting is automatically overriden to **`0`** and **`lvmetad`** is not used in this case at all. Also, the following warning message is displayed:

```
WARNING: configuration setting use_lvmetad overriden to 0 due to
locking_type 3. Clustered environment not supported by lvmetad yet.
```

`luci` component, BZ#615898

`luci` will not function with Red Hat Enterprise Linux 5 clusters unless each cluster node has **`ricci`** version 0.12.2-14.

5.8. AUTHENTICATION

`ipa` component, BZ#894388

The Identity Management installer configures all integrated services to listen on all interfaces. The administrator has no means to instruct the Identity Management installer to listen only on chosen interfaces even though the installer requires a valid interface IP address as one installation parameter. To work around this problem, change service configuration after Identity Management installation.

`ipa` component, BZ#894378

Identity Management LDAP permission manipulation plugin validates subtree and filter permission specifiers as mutually exclusive even though it is a valid combination in the underlying LDAP Access Control Instruction (ACI). Permissions with filter and subtree specifiers can be neither created nor modified. This affects for example the **`Add Automount Keys`** permission which cannot be modified.

`ipa` component, BZ#817080

In some cases the certificates tracked by **certmonger** are not cleared when running the **`ipa-server-install --uninstall`** command. This will cause a subsequent re-installation to fail with an unexpected error.

`sssd` component, BZ#892604

The **ssh_cache** utility sets the DEBUG level after it processes the command-line parameters. If the command-line parameters cannot be processed, the utility prints DEBUG lines that are not supposed to be printed by default. To avoid this, correct parameters must be used.

`sssd` component, BZ#891647

It is possible to specify the **`enumerate=true`** value in the **`sssd.conf`** file to access all users in the system. However, using **`enumerate=true`** is not recommended in large environments as this can lead to high CPU consumption. As a result, operations like login or logout can be slowed down.

`ipa` component, BZ#888579

The Identity Management server processes Kerberos Password Expiration Time field as a 32-bit integer. If Maximum Lifetime of a user password in Identity Management Password Policy is set to a value causing the resulting Kerberos Password Expiration Time timestamp to exceed 32 bits and to overflow, the passwords that are being changed are configured with an expiration time that lies in the past and are always rejected. To ensure that new user passwords are valid and can be changed properly, do not set password Maximum Lifetime in Identity Management Password Policy to values that would cause the Kerberos Password Expiration Time timestamp to exceed 32 bits; that is, passwords that would expire after 2038-01-19. At the moment, recommended values for the Maximum Lifetime field are numbers lower than 9000 days.

`sssd` component, BZ#785877

When reconnecting to an LDAP server, SSSD does not check it was re-initialized during the downtime. If the server was re-initialized during the downtime and was filled with completely different data, SSSD does not update its database. As a consequence, the user can get invalid information from SSSD. To work around this problem:

1. stop SSSD before reconnecting to the re-initialized server;
2. clear the SSSD caches manually before reconnecting;
3. start SSSD.

`krb5` component

In environments where entropy is scarce, the **kadmind** tool can take longer to initialize after startup than it did in previous releases as it attempts to read data from the **`/dev/random`** file and seed its internal random number generator (RNG). Clients which attempt to connect to the **`kadmin`** service can time out and fail with a GSS-API or Kerberos error. After the service completely finishes initializing itself, it will process messages received from now-disconnected clients and can log clock-skew or decrypt-integrity-check-failed errors for those connections. To work around this problem, use a service such as **`rngd`** to seed the system RNG using hardware sources of entropy.

ipa component, BZ#887193

The Identity Management server in Red Hat Enterprise Linux 6.3 introduced a technical preview of SELinux user mapping feature, which enabled a mapping of SELinux users to users managed by the Identity Management based on custom rules. However, the default configured SELinux user (**guest_u:s0**) used when no custom rule matches is too constraining. An Identity Management user authenticating to Red Hat Enterprise Linux 6.4 can be assigned the too constraining SELinux user in which case a login through graphical session would always fail. To work around this problem, change a too constraining default SELinux user in the Identity Management server from **guest_u:s0** to a more relaxed value **unconfined_u:s0-s0:c0.c1023**:

```
kinit admin
ipa config-mod --ipaselinuxusermapdefault=unconfined_u:s0-s0:c0.c1023
```

An unconfined SELinux user will be now assigned to the Identity Management user by default, which will allow the user to successfully authenticate through graphical interface.

ipa component, BZ#761574

When attempting to view a host in the web UI, the following message can appear:

```
Certificate operation cannot be completed: Unable to communicate with
CMS (Unauthorized)
```

Attempting to delete installed certificates through the web UI or command-line interface can fail with the same error message. To work around this problem, run the following command:

```
~]# yum downgrade ipa-server libipa_hbac libipa_hbac-python ipa-python
ipa-client ipa-admintools ipa-server-selinux
```

ipa component, BZ#877324

After upgrading to Red Hat Identity Manager 2.2, it is not possible to add SSH public keys in the web UI. However, SSH public keys can be added on the command line by running **ipa user-mod *<user>* --sshpubkey**.

sssd component, BZ#880150

Rules with **sudoUser** specified as **+netgroup** are always matched with the **sssd sudoers** plugin.

sssd component

When the **ldap_sasl_authid** is not configured in the **sssd.conf** file, SSSD terminates unexpectedly with a segmentation fault. To avoid this problem, ensure that the option is configured.

ipa component

When upgrading the ipa-server package using **anaconda**, the following error message is logged in the **upgrade.log** file:

```
/sbin/restorecon:  lstat(/var/lib/pki-ca/publish*) failed:  No such file
or directory
```

This problem does not occur when using **yum**.

sssd component

In the Identity Manager subdomain code, a User Principal Name (UPN) is by default built from the SAM Account Name and Active Directory trust users, that is **`user@DOMAIN`**. The UPN can be changed to differ from the UPN in Active Directory, however only the default format, **`user@DOMAIN`**, is supported.

`sssd` component, BZ#805921

Sometimes, group members may not be visible when running the **`getent group groupname`** command. This can be caused by an incorrect **`ldap_schema`** in the **`[domain/DOMAINNAME]`** section of the **`sssd.conf`** file. **SSSD** supports three LDAP schema types: RFC 2307, RFC 2307bis, and IPA. By default, **SSSD** uses the more common RFC 2307 schema. The difference between RFC 2307 and RFC 2307bis is the way which group membership is stored in the LDAP server. In an RFC 2307 server, group members are stored as the multi-valued memberuid attribute which contains the name of the users that are members. In an RFC2307bis server, group members are stored as the multi-valued attribute member (or sometimes uniqueMember) which contains the DN of the user or group that is a member of this group. RFC2307bis allows nested groups to be maintained as well.

When encountering this problem:

- add **`ldap_schema = rfc2307bis`** in the **`sssd.conf`** file,
- detele the **`/var/lib/sss/db/cache_DOMAINNAME.ldb`** file,
- and restart **SSSD**.

If the workaround does not work, add **`ldap_group_member = uniqueMember`** in the **`sssd.conf`** file, delete the cache file and restart SSSD.

Identity Management component, BZ#826973

When Identity Management is installed with its CA certificate signed by an external CA, the installation is processed in 2 stages. In the first stage, a CSR is generated to be signed by an external CA. The second stage of the installation then accepts a file with the new signed certificate for the Identity Management CA and a certificate of the external CA. During the second stage of the installation, a signed Identity Management CA certificate subject is validated. However, there is a bug in the certificate subject validation procedure and its default value (**`O=$REALM`**, where **`$REALM`** is the realm of the new Identity Management installation) is never pulled. Consequently, the second stage of the installation process always fails unless the **`--subject`** option is specified. To work around this issue, add the following option for the second stage of the installation: **`--subject "O=$REALM"`** where **`$REALM`** is the realm of the new Identity Management installation. If a custom subject was used for the first stage of the installation, use its value instead. Using this work around, the certificate subject validation procedure succeeds and the installation continues as expected.

Identity Management component, BZ#822350

When a user is migrated from a remote LDAP, the user's entry in the Directory Server does not contain Kerberos credentials needed for a Kerberos login. When the user visits the password migration page, Kerberos credentials are generated for the user and logging in via Kerberos authentication works as expected. However, Identity Management does not generate the credentials correctly when the migrated password does not follow the password policy set on the Identity Management server. Consequently, when the password migration is done and a user tries to log in via Kerberos authentication, the user is prompted to change the password as it does not follow the password policy, but the password change is never successful and the user is not able to use Kerberos authentication. To work around this issue, an administrator can reset the password of a migrated user with the **`ipa passwd`** command. When reset, user's Kerberos credentials in the Directory Server are properly generated and the user is able to log in using Kerberos authentication.

Identity Management component

In the Identity Management webUI, deleting a DNS record may, under come circumstances, leave it visible on the page showing DNS records. This is only a display issue and does not affect functionality of DNS records in any way.

Identity Management component, BZ#790513

The ipa-client package does not install the policycoreutils package as its dependency, which may cause install/uninstall issues when using the **`ipa-client-install`** setup script. To work around this issue, install the policycoreutils package manually:

```
~]# yum install policycoreutils
```

Identity Management component, BZ#813376

Updating the Identity Management LDAP configuration via the **`ipa-ldap-updater`** fails with a traceback error when executed by a non-root user due to the SASL EXTERNAL bind requiring root privileges. To work around this issue, run the aforementioned command as the root user.

Identity Management component, BZ#794882

With netgroups, when adding a host as a member that Identity Management does not have stored as a host already, that host is considered to be an external host. This host can be controlled with netgroups, but Identity Management has no knowledge of it. Currently, there is no way to use the **`netgroup-find`** option to search for external hosts.

Also, note that when a host is added to a netgroup as an external host, rather than being added in Identity Management as an external host, that host is not automatically converted within the netgroup rule.

Identity Management component, BZ#786629

Because a permission does not provide write access to an entry, delegation does not work as expected. The 389 Directory Server (**389-ds**) distinguishes access between entries and attributes. For example, an entry can be granted add or delete access, whereas an attribute can be granted read, search, and write access. To grant write access to an entry, the list of writable attributes needs to be provided. The **`filter`**, **`subtree`**, and other options are used to target those entries which are writable. Attributes define which part(s) of those entries are writable. As a result, the list of attributes will be writable to members of the permission.

`sssd` component, BZ#808063

The manpage entry for the **`ldap_disable_paging`** option in the **`sssd-ldap`** man page does not indicate that it accepts the boolean values True or False, and defaulting to False if it is not explicitly specified.

Identity Management component, BZ#812127

Identity Management relies on the LDAP schema to know what type of data to expect in a given attribute. If, in certain situations (such as replication), data that does not meet those expectations is inserted into an attribute, Identity Management will not be able to handle the entry, and LDAP tools have do be used to manually clean up that entry.

Identity Management component, BZ#812122

Identity Management **`sudo`** commands are not case sensitive. For example, executing the following commands will result in the latter one failing due to the case insensitivity:

```
~]$ ipa sudocmd-add /usr/bin/X
 ⋮
~]$ ipa sudocmd-add /usr/bin/x
ipa: ERROR: sudo command with name "/usr/bin/x" already exists
```

Identity Management component

When an Identity Management server is installed with a custom hostname that is not resolvable, the **`ipa-server-install`** command should add a record to the static hostname lookup table in **`/etc/hosts`** and enable further configuration of Identity Management integrated services. However, a record is not added to **`/etc/hosts`** when an IP address is passed as an CLI option and not interactively. Consequently, Identity Management installation fails because integrated services that are being configured expect the Identity Management server hostname to be resolvable. To work around this issue, complete one of the following:

- Run the **`ipa-server-install`** without the **`--ip-address`** option and pass the IP address interactively.

- Add a record to **`/etc/hosts`** before the installation is started. The record should contain the Identity Management server IP address and its full hostname (the **`hosts(5)`** man page specifies the record format).

As a result, the Identity Management server can be installed with a custom hostname that is not resolvable.

sssd component

Upgrading SSSD from the version provided in Red Hat Enterprise Linux 6.1 to the version shipped with Red Hat Enterprise Linux 6.2 may fail due to a bug in the dependent library **`libldb`**. This failure occurs when the SSSD cache contains internal entries whose distinguished name contains the **`\,`** character sequence. The most likely example of this is for an invalid ***`memberUID`*** entry to appear in an LDAP group of the form:

```
memberUID: user1,user2
```

`memberUID` is a multi-valued attribute and should not have multiple users in the same attribute.

If the upgrade issue occurs, identifiable by the following debug log message:

```
(Wed Nov  2 15:18:21 2011) [sssd] [ldb] (0): A transaction is still
active in
ldb context [0xaa0460] on /var/lib/sss/db/cache_<DOMAIN>.ldb
```

remove the **`/var/lib/sss/db/cache_<DOMAIN>.ldb`** file and restart SSSD.

WARNING

Removing the **`/var/lib/sss/db/cache_<DOMAIN>.ldb`** file purges the cache of all entries (including cached credentials).

sssd component, BZ#751314

When a group contains certain incorrect multi-valued ***memberUID*** values, SSSD fails to sanitize the values properly. The ***memberUID*** value should only contain one username. As a result, SSSD creates incorrect users, using the broken ***memberUID*** values as their usernames. This, for example, causes problems during cache indexing.

Identity Management component

Two Identity Management servers, both with a CA (Certificate Authority) installed, use two replication replication agreements. One is for user, group, host, and other related data. Another replication agreement is established between the CA instances installed on the servers. If the CA replication agreement is broken, the Identity Management data is still shared between the two servers, however, because there is no replication agreement between the two CAs, issuing a certificate on one server will cause the other server to not recognize that certificate, and vice versa.

Identity Management component

The Identity Management (ipa) package cannot be build with a **6ComputeNode** subscription.

sssd component, BZ#741264

Active Directory performs certain LDAP referral-chasing that is incompatible with the referral mechanism included in the **openldap** libraries. Notably, Active Directory sometimes attempts to return a referral on an LDAP bind attempt, which used to cause a hang, and is now denied by the **openldap** libraries. As a result, SSSD may suffer from performance issues and occasional failures resulting in missing information.

To work around this issue, disable referral-chasing by setting the following parameter in the **[domain/DOMAINNAME]** section of the **/etc/sssd/sssd.conf** file:

```
ldap_referrals = false
```

5.9. DEVICES

kernel component

A Linux LIO FCoE target causes the bnx2fc driver to perform sequence level error recovery when the target is down. As a consequence, the FCoE session cannot be resumed after the Ethernet link is bounced, the bnx2fc kernel module cannot be unloaded and the FCoE session cannot be removed when running the **fcoeadm -d eth0** command. To avoid these problems, do not use the bnx2fc driver with a Linux FCoE target.

kernel component

When using large block size (1MB), the tape driver sometimes returns an EBUSY error. To work around this problem, use a smaller block size, that is 256KB.

kernel component

On some of the older Broadcom tg3 devices, the default Maximum Read Request Size (MRRS) value of 512 byte is known to cause lower performance. It is because these devices perform direct memory access (DMA) requests serially. 1500-byte ethernet packet will be broken into 3 PCIE read requests using 512 byte MRRS. When using a higher MRRS value, the DMA transfer can be faster as fewer requests will be needed. However, the MRRS value is meant to be tuned by system software and not by the driver. PCIE Base spec 3.0 section 7.8.4 contains an implementation note that illustrates how system software might tune the MRRS for all devices in the system. As a result, Broadcom modified the tg3 driver to remove the code that sets the MRRS to 4K bytes so that any value selected by system software (BIOS) will be preserved.

`kernel` component

The Brocade BFA Fibre Channel and FCoE driver does not currently support dynamic recognition of Logical Unit addition or removal using the **sg3_utils** utilities (for example, the **`sg_scan`** command) or similar functionality. Please consult Brocade directly for a Brocade equivalent of this functionality.

`kernel` component

iSCSI and FCoE boot support on Broadcom devices is not included in Red Hat Enterprise Linux 6.4. These two features, which are provided by the **`bnx2i`** and **`bnx2fc`** Broadcom drivers, remain a Technology Preview until further notice.

`kexec-tools` component

Starting with Red Hat Enterprise Linux 6.0 and later, kexec kdump supports dumping core to the Brtfs file system. However, note that because the **findfs** utility in **busybox** does not support Btrfs yet, ***`UUID/LABEL`*** resolving is not functional. Avoid using the ***`UUID/LABEL`*** syntax when dumping core to Btrfs file systems.

`trace-cmd` component

The **`trace-cmd`** service does start on 64-bit PowerPC and IBM System z systems because the **`sys_enter`** and **`sys_exit`** events do not get enabled on the aforementioned systems.

`trace-cmd` component

trace-cmd's subcommand, **`report`**, does not work on IBM System z systems. This is due to the fact that the ***`CONFIG_FTRACE_SYSCALLS`*** parameter is not set on IBM System z systems.

`libfprint` component

Red Hat Enterprise Linux 6 only has support for the first revision of the UPEK Touchstrip fingerprint reader (USB ID 147e:2016). Attempting to use a second revision device may cause the fingerprint reader daemon to crash. The following command returns the version of the device being used in an individual machine:

```
~]$ lsusb -v -d 147e:2016 | grep bcdDevice
```

`kernel` component

The Emulex Fibre Channel/Fibre Channel-over-Ethernet (FCoE) driver in Red Hat Enterprise Linux 6 does not support DH-CHAP authentication. DH-CHAP authentication provides secure access between hosts and mass storage in Fibre-Channel and FCoE SANs in compliance with the FC-SP specification. Note, however that the Emulex driver (**`lpfc`**) does support DH-CHAP authentication on Red Hat Enterprise Linux 5, from version 5.4. Future Red Hat Enterprise Linux 6 releases may include DH-CHAP authentication.

`kernel` component

The recommended minimum HBA firmware revision for use with the **`mpt2sas`** driver is "Phase 5 firmware" (that is, with version number in the form **`05.xx.xx.xx`**). Note that following this recommendation is especially important on complex SAS configurations involving multiple SAS expanders.

5.10. KERNEL

`kernel` component

In Red Hat Enterprise Linux 6.4, irqbalance has been updated to upstream version 1.0.4. This version of irqbalance requires **`/sys/device/system/cpu/cpu?/node*`** to exist; however, kernel-2.6.32-358 or earlier does not include support for this sysfs node. To work around this problem, use the irqbalance-0.55-35.el6_3 package or earlier.

`kernel` component

Red Hat Enterprise Linux 6.4 changed the maximum read/write socket memory default value to be higher, allowing for better performance on some machines. It was observed that if the values of **`?mem_max`** are not symmetrical between two machines, the performance can be negatively affected. To work around this problem, adjust the value of **`?mem_max`** to be equal across all Red Hat Enterprise Linux systems in the network.

`kabi-whitelists` component

The vxfs module might not work properly on Red Hat Enterprise Linux 6.4 because of the broken **`radix_tree_gang_lookup_slot`** symbol. Consult Symantec should you require a workaround for this issue.

`kernel` component

Enabling TCP Segmentation Offload (TSO) on TAP interface may cause low throughput when the uplink is a high-speed interface. To improve throughput, turn off TSO on the tap interface of the virtual machine.

`kabi-whitelists` component, BZ#871580

A patch submitted in Red Hat Enterprise Linux 6.3 broke a kABI symbol. Consequently, the previously working Red Hat Enterprise Linux 6.2 Veritas **`vxfs`** module did not work on the 6.3 kernel; a newer compiled version of the Red Hat Enterprise Linux 6.3 Veritas **`vxfs`** module had to be used. In Red Hat Enterprise Linux 6.4, the kABI issue has been fixed, and the Red Hat Enterprise Linux 6.3 Veritas **`vxfs`** module works as expected. Refer to Table 5.1, “Functionality Matrix” for a summary of what versions of Red Hat Enterprise Linux 6 and **`vxfs`** function as expected.

Table 5.1. Functionality Matrix

		Red Hat Enterprise Linux Version (Kernel Version)		
		6.2 GA (2.6.32-220.el6)	6.3 GA (2.6.32-279.el6)	6.4 pre-alpha (2.6.32-330.el6)
`vxfs` Module Version	5.1.120.000-SP1PR2	works	fails	works
	5.1.133.000-SP1RP3	-	works	fail

`kernel` component

When using Chelsio's iSCSI HBAs for an iSCSI root partition, the first boot after install fails. This occurs because Chelsio's iSCSI HBA is not properly detected. To work around this issue, users must add the ***`iscsi_firmware`*** parameter to grub's kernel command line. This will signal to dracut to boot from the iSCSI HBA.

kernel component

The installation of Red Hat Enterprise Linux 6.4 i386 may occasionally fail. To work around this issue, add the following parameter to the kernel command line:

```
vmalloc=256MB
```

kernel component

If a device reports an error, while it is opened (via the **open(2)** system call), then the device is closed (via the **close(2)** system call), and the **/dev/disk/by-id** link for the device may be removed. When the problem on the device that caused the error is resolved, the **by-id** link is not re-created. To work around this issue, run the following command:

```
~]# echo 'change' > /sys/class/block/sdX/uevent
```

kernel component

When an HBA that uses the **mpt2sas** driver is connected to a storage using an SAS switch LSI SAS 6160, the driver may become unresponsive during Controller Fail Drive Fail (CFDF) testing. This is due to faulty firmware that is present on the switch. To fix this issue, use a newer version (14.00.00.00 or later) of firmware for the LSI SAS 6160 switch.

kernel component, BZ#745713

In some cases, Red Hat Enterprise Linux 6 guests running fully-virtualized under Red Hat Enterprise Linux 5 experience a time drift or fail to boot. In other cases, drifting may start after migration of the virtual machine to a host with different speed. This is due to limitations in the Red Hat Enterprise Linux 5 Xen hypervisor. To work around this, add the ***nohpet*** parameter or, alternatively, the ***clocksource=jiffies*** parameter to the kernel command line of the guest. Or, if running under Red Hat Enterprise Linux 5.7 or newer, locate the guest configuration file for the guest and add the ***hpet=0*** parameter in it.

kernel component

On some systems, Xen full-virt guests may print the following message when booting:

```
WARNING: BIOS bug: CPU MTRRs don't cover all of memory, losing
<number>MB of RAM
```

It is possible to avoid the memory trimming by using the **disable_mtrr_trim** kernel command line option.

kernel component

The **perf record** command becomes unresponsive when specifying a tracepoint event and a hardware event at the same time.

kernel component

On 64-bit PowerPC, the following command may cause kernel panic:

```
~]# ./perf record -agT -e sched:sched_switch -F 100 -- sleep 3
```

kernel component

Applications are increasingly using more than 1024 file descriptors. It is not recommended to increase the default soft limit of file descriptors because it may break applications that use the **select()** call. However, it is safe to increase the default hard limit; that way, applications requiring a large amount of file descriptors can increase their soft limit without needing root privileges and without any user intervention.

kernel component

In network only use of Brocade Converged Network Adapters (CNAs), switches that are not properly configured to work with Brocade FCoE functionality can cause a continuous linkup/linkdown condition. This causes continuous messages on the host console:

```
bfa xxxx:xx:xx.x: Base port (WWN = xx:xx:xx:xx:xx:xx:xx:xx) lost fabric
connectivity
```

To work around this issue, unload the Brocade **bfa** driver.

kernel component

In Red Hat Enterprise Linux 6, a legacy bug in the PowerEdge Expandable RAID Controller 5 (PERC5) which causes the kdump kernel to fail to scan for **scsi** devices. It is usually triggered when a large amounts of I/O operations are pending on the controller in the first kernel before performing a kdump.

kernel component, BZ#679262

In Red Hat Enterprise Linux 6.2 and later, due to security concerns, addresses in **/proc/kallsyms** and **/proc/modules** show all zeros when accessed by a non-root user.

kernel component

Superfluous information is displayed on the console due to a correctable machine check error occurring. This information can be safely ignored by the user. Machine check error reporting can be disabled by using the **nomce** kernel boot option, which disables machine check error reporting, or the **mce=ignore_ce** kernel boot option, which disables correctable machine check error reporting.

kernel component

The order in which PCI devices are scanned may change from one major Red Hat Enterprise Linux release to another. This may result in device names changing, for example, when upgrading from Red Hat Enterprise Linux 5 to 6. You must confirm that a device you refer to during installation, is the intended device.

One way to assure the correctness of device names is to, in some configurations, determine the mapping from the controller name to the controller's PCI address in the older release, and then compare this to the mapping in the newer release, to ensure that the device name is as expected.

The following is an example from /var/log/messages:

```
kernel: cciss0: <0x3230> at PCI 0000:1f:00.0 IRQ 71 using DAC
…
kernel: cciss1: <0x3230> at PCI 0000:02:00.0 IRQ 75 using DAC
```

If the device name is incorrect, add the ***pci=bfsort*** parameter to the kernel command line, and check again.

`kernel` component

The minimum firmware version for NIC adapters managed by **`netxen_nic`** is 4.0.550. This includes the boot firmware which is flashed in option ROM on the adapter itself.

`kernel` component

High stress on 64-bit IBM POWER series machines prevents kdump from successfully capturing the **`vmcore`**. As a result, the second kernel is not loaded, and the system becomes unresponsive.

`kernel` component

Triggering kdump to capture a **`vmcore`** through the network using the Intel 82575EB ethernet device in a 32 bit environment causes the networking driver to not function properly in the kdump kernel, and prevent the **`vmcore`** from being captured.

`kernel` component

Memory Type Range Register (MTRR) setup on some hyperthreaded machines may be incorrect following a suspend/resume cycle. This can cause graphics performance (specifically, scrolling) to slow considerably after a suspend/resume cycle.

To work around this issue, disable and then re-enable the hyperthreaded sibling CPUs around suspend/resume, for example:

```
#!/bin/sh
# Disable hyper-threading processor cores on suspend and hibernate, re-
enable
# on resume.
# This file goes into /etc/pm/sleep.d/

case $1 in
        hibernate|suspend)
                echo 0 > /sys/devices/system/cpu/cpu1/online
                echo 0 > /sys/devices/system/cpu/cpu3/online
                ;;

        thaw|resume)
                echo 1 > /sys/devices/system/cpu/cpu1/online
                echo 1 > /sys/devices/system/cpu/cpu3/online
                ;;
esac
```

`kernel` component

In Red Hat Enterprise Linux 6.2, **`nmi_watchdog`** registers with the **`perf`** subsystem. Consequently, during boot, the **`perf`** subsystem grabs control of the performance counter registers, blocking OProfile from working. To resolve this, either boot with the **`nmi_watchdog=0`** kernel parameter set, or run the following command to disable it at run time:

```
echo 0 > /proc/sys/kernel/nmi_watchdog
```

To re-enable **`nmi-watchdog`**, use the following command

```
echo 1 > /proc/sys/kernel/nmi_watchdog
```

`kernel` component, BZ#603911

Due to the way **ftrace** works when modifying the code during start-up, the NMI watchdog causes too much noise and **ftrace** can not find a quiet period to instrument the code. Consequently, machines with more than 512 CPUs will encounter issues with the NMI watchdog. Such issues will return error messages similar to **`BUG: NMI Watchdog detected LOCKUP`** and have either **`ftrace_modify_code`** or **`ipi_handler`** in the backtrace. To work around this issue, disable NMI watchdog by setting the **`nmi_watchdog=0`** kernel parameter, or using the following command at run time:

```
echo 0 > /proc/sys/kernel/nmi_watchdog
```

`kernel` component

On 64-bit POWER systems the EHEA NIC driver will fail when attempting to dump a **`vmcore`** via NFS. To work around this issue, utilize other kdump facilities, for example dumping to the local file system, or dumping over SSH.

`kernel` component, BZ#587909

A BIOS emulated floppy disk might cause the installation or kernel boot process to hang. To avoid this, disable emulated floppy disk support in the BIOS.

`kernel` component

The preferred method to enable nmi_watchdog on 32-bit x86 systems is to use either ***`nmi_watchdog=2`*** or ***`nmi_watchdog=lapic`*** parameters. The parameter ***`nmi_watchdog=1`*** is not supported.

`kernel` component

The kernel parameter, **`pci=noioapicquirk`**, is required when installing the 32-bit variant of Red Hat Enterprise Linux 6 on HP xw9300 workstations. Note that the parameter change is not required when installing the 64-bit variant.

5.11. DESKTOP

`firefox` package

In certain environments, storing personal Firefox configuration files (~/.mozilla/) on an NFS share, such as when your home directory is on a NFS share, led to Firefox functioning incorrectly, for example, navigation buttons not working as expected, and bookmarks not saving. This update adds a new configuration option, storage.nfs_filesystem, that can be used to resolve this issue. If you experience this issue:

1. Start **Firefox**.
2. Type **`about:config`** into the URL bar and press the Enter key.
3. If prompted with "This might void your warranty!", click the **`I'll be careful, I promise!`** button.
4. Right-click in the **Preference Name** list. In the menu that opens, select **New** → **Boolean**.
5. Type "storage.nfs_filesystem" (without quotes) for the preference name and then click the **`OK`** button.

6. Select **`true`** for the boolean value and then press the **`OK`** button.

`Red_Hat_Enterprise_Linux-Release_Notes-6` component

The link in the **`RELEASE-NOTES-si-LK.html`** file (provided by the Red_Hat_Enterprise_Linux-Release_Notes-6-si-LK package) incorrectly points at the Beta online version of the 6.4 Release Notes. Because the si-LK language is no longer supported, the link should correctly point to the en-US online 6.4 Release Notes located at: https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html-single/6.4_Release_Notes/index.html.

`libwacom` component

The Lenovo X220 Tablet Touchscreen is not supported in the kernel shipped with Red Hat Enterprise Linux 6.4.

`wacomcpl` package, BZ#769466

The wacomcpl package has been deprecated and has been removed from the package set. The wacomcpl package provided graphical configuration of Wacom tablet settings. This functionality is now integrated into the GNOME Control Center.

`acroread` component

Running a AMD64 system without the sssd-client.i686 package installed, which uses SSSD for getting information about users, causes **acroread** to fail to start. To work around this issue, manually install the sssd-client.i686 package.

`kernel` component, BZ#681257

With newer kernels, such as the kernel shipped in Red Hat Enterprise Linux 6.1, Nouveau has corrected the Transition Minimized Differential Signaling (TMDS) bandwidth limits for pre-G80 NVIDIA chipsets. Consequently, the resolution auto-detected by X for some monitors may differ from that used in Red Hat Enterprise Linux 6.0.

`fprintd` component

When enabled, fingerprint authentication is the default authentication method to unlock a workstation, even if the fingerprint reader device is not accessible. However, after a 30 second wait, password authentication will become available.

`evolution` component

Evolution's IMAP backend only refreshes folder contents under the following circumstances: when the user switches into or out of a folder, when the auto-refresh period expires, or when the user manually refreshes a folder (that is, using the menu item **Folder** → **Refresh**). Consequently, when replying to a message in the Sent folder, the new message does not immediately appear in the Sent folder. To see the message, force a refresh using one of the methods describe above.

`anaconda` component

The clock applet in the GNOME panel has a default location of Boston, USA. Additional locations are added via the applet's preferences dialog. Additionally, to change the default location, left-click the applet, hover over the desired location in the **`Locations`** section, and click the **`Set...`** button that appears.

`xorg-x11-server` component, BZ#623169

In some multi-monitor configurations (for example, dual monitors with both rotated), the cursor confinement code produces incorrect results. For example, the cursor may be permitted to disappear off the screen when it should not, or be prevented from entering some areas where it should be allowed to go. Currently, the only workaround for this issue is to disable monitor rotation.

5.12. TOOLS

`coolkey` component, BZ#906537

Personal Identity Verification (PIV) Endpoint Cards which support both CAC and PIV interfaces might not work with the latest **coolkey** update; some signature operations like PKINIT can fail. To work around this problem, downgrade **coolkey** to the version shipped with Red Hat Enterprise Linux 6.3.

`libreport` component

Even if the stored credentials are used , the **report-gtk** utility can report the following error message:

```
Wrong settings detected for Red Hat Customer Support [..]
```

To work around this problem, close the dialog window; the **`Login=<rhn-user>`** and **`Password=<rhn-password>`** credentials in the **`/etc/libreport/plugins/rhtsupport.conf`** will be used in the same way they are used by **report-rhtsupport**.

For more information, refer to this Knowledge Base article.

`vlock` component

When a user password is used to lock a console with **vlock**, the console can only be unlocked with the user password, not the root password. That is, even if the first inserted password is incorrect, and the user is prompted to provide the root password, entering the root password fails with an error message.

`libreoffice` component

Libreoffice contains a number of harmless files used for testing purposes. However, on Microsoft Windows system, these files can trigger false positive alerts on various anti-virus software, such as Microsoft Security Essentials. For example, the alerts can be triggered when scanning the Red Hat Enterprise Linux 6 ISO file.

`gnome-power-manager` component

When the computer runs on battery, custom brightness level is not remembered and restored if power saving features like "dim display when idle" or "reduce backlight brightness when idle" are enabled.

`rsyslog` component

rsyslog does not reload its configuration after a **`SIGHUP`** signal is issued. To reload the configuration, the **`rsyslog`** daemon needs to be restarted:

```
~]# service rsyslog restart
```

`parted` component

The **parted** utility in Red Hat Enterprise Linux 6 cannot handle Extended Address Volumes (EAV) Direct Access Storage Devices (DASD) that have more than 65535 cylinders. Consequently, EAV DASD drives cannot be partitioned using **parted**, and installation on EAV DASD drives will fail. To work around this issue, complete the installation on a non EAV DASD drive, then add the EAV device after the installation using the tools provided in the s390-utils package.

CHAPTER 6. NEW PACKAGES

6.1. RHEA-2013:0278 — NEW PACKAGES: DEV86 AND IASL

New dev86 and iasl packages are now available for Red Hat Enterprise Linux 6.

The dev86 and iasl packages are build dependencies of the qemu-kvm package.

This enhancement update adds the dev86 and iasl packages to the 32-bit x862 Optional channels of Red Hat Enterprise Linux 6. (BZ#901677, BZ#901678)

All users who require dev86 and iasl are advised to install these new packages.

6.2. RHEA-2013:0484 — NEW PACKAGES: HYPERVKVPD

New hypervkvpd packages are now available for Red Hat Enterprise Linux 6.

The hypervkvpd packages contain hypervkvpd, the guest Hyper-V Key-Value Pair (KVP) daemon. Using VMbus, hypervkvpd passes basic information to the host. The information includes guest IP address, fully qualified domain name, operating system name, and operating system release number. An IP injection functionality is also provided which allows you to change the IP address of a guest from the host via the hypervkvpd daemon.

This enhancement update adds the hypervkvpd packages to Red Hat Enterprise Linux 6. For more information about inclusion of, and guest installation support for, Microsoft Hyper-V drivers, refer to the Red Hat Enterprise Linux 6.4 Release Notes. (BZ#850674)

All users who require hypervkvpd are advised to install these new packages. After installing the hypervkvpd packages, rebooting all guest machines is recommended, otherwise the Microsoft Windows server with Hyper-V might not be able to get information from these guest machines.

6.3. RHEA-2013:0422 — NEW PACKAGES: LIBJPEG-TURBO

New libjpeg-turbo packages are now available for Red Hat Enterprise Linux 6.

The libjpeg-turbo packages contain a library of functions for manipulating JPEG images. They also contain simple client programs for accessing the libjpeg functions. These packages provide the same functionality and API as libjpeg but with better performance.

This enhancement update adds the libjpeg-turbo packages to Red Hat Enterprise Linux 6. (BZ#788687)

All users who require libjpeg-turbo are advised to install these new packages.

6.4. RHEA-2013:0369 — NEW PACKAGES: PCS

New pcs packages are now available for Red Hat Enterprise Linux 6.

The pcs packages provide a command-line tool and graphical web interface to configure and manage pacemaker and corosync.

This enhancement update adds the pcs package as a Technology Preview. (BZ#657370)

More information about Red Hat Technology Previews is available here:

https://access.redhat.com/support/offerings/techpreview/

All users who want to use the pcs Technology Preview are advised to install these new packages.

6.5. RHEA-2013:0356 — NEW PACKAGE: HAPROXY

A new haproxy package is now available for Red Hat Enterprise Linux 6.

The haproxy package provides a reliable, high-performance network load balancer for TCP and HTTP-based applications. It is particularly suited for web sites crawling under very high loads while needing persistence or Layer7 processing.

This enhancement update adds the haproxy package to Red Hat Enterprise Linux 6 as a Technology Preview. (BZ#846067)

More information about Red Hat Technology Previews is available at

https://access.redhat.com/support/offerings/techpreview/

All users who want to use the haproxy Technology Preview should install this newly-released package, which adds this enhancement.

6.6. RHEA-2013:0355 — NEW PACKAGE: KEEPALIVED

A new keepalived package is now available as a Technology Preview for Red Hat Enterprise Linux 6.

The keepalived package provides simple and robust facilities for load-balancing and high-availability. The load-balancing framework relies on the well-known and widely used Linux Virtual Server kernel module providing Layer4 network load-balancing. The keepalived daemon implements a set of health checkers to load-balanced server pools according their state. The keepalived daemon also implements the Virtual Router Redundancy Protocol (VRRP), allowing router or director failover to achieve high availability.

This enhancement update adds the keepalived package to Red Hat Enterprise Linux 6 as a Technology Preview. (BZ#846064)

More information about Red Hat Technology Previews is available at

https://access.redhat.com/support/offerings/techpreview/

All users who want to use the keepalived Technology Preview should install this newly-released package, which adds this enhancement.

6.7. RHEA-2013:0349 — NEW PACKAGES: LINUXPTP

New linuxptp packages are now available as a Technology Preview for Red Hat Enterprise Linux 6.

The Linux PTP project is a software implementation of the Precision Time Protocol (PTP) according to IEEE standard 1588 for Linux. These packages provide a robust implementation of the standard and use the most relevant and modern Application Programming Interfaces (API) offered by the Linux kernel. Supporting legacy APIs and other platforms is not a goal.

This enhancement update adds the linuxptp packages to Red Hat Enterprise Linux 6 as a Technology preview. (BZ#848856)

More information about Red Hat Technology Previews is available here:

https://access.redhat.com/support/offerings/techpreview/

All users who want to use the linuxptp Technology Preview should install these newly-released packages, which add this enhancement.

6.8. RHEA-2013:0342 — NEW PACKAGES: LIBITM

New libitm packages are now available for Red Hat Enterprise Linux 6.

The libitm packages contain the GNU Transactional Memory runtime library that provides GCC transactional memory support.

This enhancement update adds the libitm packages to Red Hat Enterprise Linux 6. (BZ#813301)

All users who require libitm are advised to install these new packages.

6.9. RHEA-2013:0341 — NEW PACKAGE: SCIPY

New scipy packages are now available for Red Hat Enterprise Linux 6.

The SciPy package provides software for mathematics, science, and engineering. The NumPy package, which is designed to manipulate large multi-dimensional arrays of arbitrary records, is the core library for SciPy. The SciPy library is built to work with NumPy arrays and provides various efficient numerical routines, for example routines for numerical integration and optimization.

This enhancement update adds the scipy packages to Red Hat Enterprise Linux 6. (BZ#697530)

All users who require scipy are advised to install these new package.

6.10. RHEA-2013:0340 — NEW PACKAGES: SUITESPARSE

New suitesparse packages are now available for Red Hat Enterprise Linux 6.

The suitesparse packages are a collection of libraries for computations involving sparse matrices.

This enhancement update adds the suitesparse packages to Red Hat Enterprise Linux 6. (BZ#844974)

All users who require suitespare should install these new packages.

6.11. RHEA-2013:0339 — NEW PACKAGES: TBB

New tbb packages are now available for Red Hat Enterprise Linux 6.

The tbb packages contain a C++ runtime library that abstracts the low-level threading details necessary for optimal multi-core performance.

This enhancement update adds the tbb packages to Red Hat Enterprise Linux 6. (BZ#844976)

All users who require tbb are advised to install these new packages.

6.12. RHEA-2013:0336 — NEW PACKAGE: TUNA

A new tuna package is now available for Red Hat Enterprise Linux 6.

The tuna package provides an interface for changing both scheduler and IRQ tunables, at whole CPU, per-thread or per-IRQ levels. tuna allows CPUs to be isolated for use by a specific application and threads and interrupts to be moved to a CPU simply by dragging and dropping them.

This enhancement update adds the tuna package to Red Hat Enterprise Linux 6. (BZ#812455)

All users who require tuna should install this new package.

6.13. RHEA-2013:0289 — NEW PACKAGE: MTDEV

A new mtdev package is now available for Red Hat Enterprise Linux 6.

The new mtdev package contains a library that converts kernel input events from multitouch protocol A into multitouch protocol B events. Protocol B events provide per-touchpoint tracking which is required by the xorg-x11-drv-evdev and xorg-x11-drv-synaptics packages.

This enhancement update adds the mtdev package to Red Hat Enterprise Linux 6. (BZ#860177)

All users who require mtdev should install this new package.

6.14. RHEA-2013:0284 — NEW PACKAGE: CPUPOWERUTILS

New cpupowerutils packages are now available for Red Hat Enterprise Linux 6.

The cpupowerutils packages provide a suite of tools to manage power states on appropriately enabled central processing units (CPU).

This enhancement update adds the cpupowerutils packages to Red Hat Enterprise Linux 6. (BZ#697418)

All users who require cpupowerutils are advised to install these new packages.

6.15. RHEA-2013:0283 — NEW PACKAGE: CGDCBXD

New cgdcbxd packages are now available for Red Hat Enterprise Linux 6.

The cgdcbxd packages provide a daemon to manage the priority of network traffic in Data Center Bridging (DCB) enabled environments. By using the information exchanged over the DCB Capability Exchange Protocol (DCBX) on a LAN, cgdcbxd enforces network priority on running applications on your host with the net_prio cgroup.

This enhancement update adds the cgdcbxd packages to Red Hat Enterprise Linux 6. (BZ#835171)

All users who require cgdcbxd are advised to install these new packages.

CHAPTER 7. UPDATED PACKAGES

7.1. 389-DS-BASE

7.1.1. RHSA-2013:0503 — Moderate: 389-ds-base security bug fix and enhancement update

Updated 389-ds-base packages that fix one security issue, a number of bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE link(s) associated with each description below.

The 389-ds-base packages provide **389 Directory Server**, which is an LDAPv3 compliant server. The base packages include the **`Lightweight Directory Access Protocol`** (LDAP) server and command-line utilities for server administration.

NOTE

The 389-ds-base packages have been upgraded to upstream version 1.2.11, which provides a number of bug fixes and enhancements over the previous version. (BZ#800051)

Security Fixes

CVE-2012-4450

A flaw was found in the way **389 Directory Server** enforced ACLs after performing an LDAP modify relative distinguished name (modrdn) operation. After modrdn was used to move part of a tree, the ACLs defined on the moved (Distinguished Name) were not properly enforced until the server was restarted. This could allow LDAP users to access information that should be restricted by the defined ACLs.

This issue was discovered by Noriko Hosoi of Red Hat.

Bug Fixes

BZ#742054

Previously, **389 Directory Server** did not support the *Simple Authentication and Security Layer* (SASL) PLAIN mechanism. This mechanism has been added to the list of supported SASL mechanisms.

BZ#742381

Due to certain changes under the **`cn=config`** suffix, when an attribute value was deleted and then added back in the same modify operation, **`error 53`** was returned. Consequently, the configuration could not be reset. This update allows delete operations to succeed if the attribute is added back in the same modify operation and reset the configuration file as expected.

BZ#757836

Previously, the **`logconv.pl`** script used a connection number equal to 0 (**`conn=0`**) as a restart point, which caused the script to return incorrect restart statistics. The underlying source code has been modified and **389 Directory Server** is now configured to use connection number equal to 1 (**conn=1**) as the restart point.

BZ#803873

The **Windows Sync** feature uses the name in a search filter to perform an internal search to find an entry. Parentheses, “(” and “)” are special characters in the **LDAP** protocol and therefore must be escaped. However, an attempt to synchronize an entry containing parentheses in the name from an *Active Directory* (AD) server failed with an error. With this update, **389 Directory Server** properly escapes the parentheses and synchronization now proceeds correctly as expected.

BZ#818762

When having an entry in a *directory server* (DS) with the same user name, group name, or both as an entry in AD and simultaneously the entry in AD was out of scope of the **Windows Sync** feature, the DS entry was deleted. This update adds the new **winSyncMoveAction** DS attribute for the Windows Sync agreement entry, which allows the user to specify the behavior of out-of-scope AD entries. The value could be set to:

- **none**, which means that an out-of-scope AD entry does nothing to the corresponding DS entry;
- **delete**, which means that an out-of-scope AD entry deletes the corresponding DS entry;
- **unsync**, which means that an out-of-scope AD entry is unsynchronized with the corresponding DS entry and changes made to either entry are not synchronized.

By default, the value is set to **none**, which fixes this bug.

BZ#830334

Due to an incorrect interpretation of an error code, a directory server considered an invalid chaining configuration setting as the **disk full** error and shut down unexpectedly. This bug has been fixed by using the correct error code and a directory server now no longer terminates due to an invalid chaining of a configuration setting.

BZ#830335

Previously, restoring an **ldif** file from a replica, which had older changes that other servers did not see yet, could lead to these updates not being replicated to other replicas. With this update, **389 Directory Server** checks the *Change Sequence Numbers* (CSNs) and allows the older updates to be replicated. As a result, all replicas remain synchronized.

BZ#830336

When a directory server was under a heavy read and write load, and an update request was processed, the following error message or other similar **DB_LOCK_DEADLOCK** error messages appeared in the error log:

```
entryrdn-index - _entryrdn_put_data: Adding the parent link (XXX)
failed: DB_LOCK_DEADLOCK: Locker killed to resolve a deadlock (-30994)
```

These errors are common under these circumstances and there is no need to report them in the error log. With this update, **389 Directory Server** ensures that these errors are handled properly and no longer logs these messages in the error log.

BZ#830337

When a directory server was configured to use multi-master replication and the **`Entry USN`** plug-in, the delete operation was not replicated to the other masters. This update modifies the **`Entry USN`** plug-in to prevent it from changing the delete operation into a delete tombstone operation, and from removing the operation before it logs into the change log to replay to other servers. As a result, the delete operation is replicated to all servers as expected.

BZ#830338

Previously, **389 Directory Server** did not refresh its Kerberos cache. Consequently, if a new Kerberos ticket was issued for a host that had already authenticated against a directory server, it would be rejected by this server until it was restarted. With this update, the Kerberos cache is flushed after an authentication failure and **389 Directory Server** works as expected in the described scenario.

BZ#830343

Using the **`Managed Entry`** plug-in in conjunction with other plug-ins, such as **`Distributed Numeric Assignment`** (DNA), **`Member of`**, and **`Auto Member`**, led to problems with delete operations on entries that managed the **`Managed Entry`** plug-in. The **`manager`** entry was deleted, but the **`managed`** entry was not. The deadlock retry handling has been improved so that both entries are deleted during the same database operation.

BZ#830344

Previously, replication errors logged in the error log could contain incorrect information. With this update, the replication errors have been modified to be more useful in diagnosing and fixing problems.

BZ#830346

When audit logging in a directory server was enabled, LDAP ADD operations were ignored and were not logged. This update removes a regression in the audit log code that caused the ADD operation to be ignored, and LDAP ADD operations are now logged to the audit log as expected.

BZ#830348

389 Directory Server with a large number of replication agreements took a considerable amount of time to shut down due to a long sleep interval coded in the replication stop code. This sleep interval has been reduced to speed up the system termination.

BZ#830349

Previously, in a SASL map definition, using a compound search filter that included the“&” character failed because the “&” character was escaped. The underlying source code has been modified and searching with a filter that includes the “&” character works as expected.

BZ#830353

When **389 Directory Server** used the **`Managed Entry`** plug-in or the **`DNA`** plug-in, the **`valgrind`** tool reported memory errors and leaks. With this update, a patch has been applied to prevent these problems, and memory is now used and deleted correctly.

BZ#832560

When replication was configured and a conflict occurred, under certain circumstances, an error check did not reveal this conflict, because a **`to-be-deleted`** attribute was already deleted by another master. Consequently, the conflict terminated the server. This update improves error checks to prevent replication conflicts from crashing the server.

BZ#833202

Previously, internal entries that were in the cache were freed when retrying failed transactions due to a deadlock. This behavior caused problems in a directory server and this server could terminate under a heavy update load. With this update, the cached internal entries are no longer freed and directory servers do not crash in the described scenario.

BZ#833218

Due to improper deadlock handling, the database reported an error instead of retrying the transaction. Consequently, under a heavy load, the directory server got deadlock errors when attempting to write to the database. The deadlock handling has been fixed and **389 Directory Server** works as expected in such a case.

BZ#834047

Internal access control prohibited deleting newly added or modified passwords. This update allows the user to delete any password if they have the modify rights.

BZ#834054

Certain operations, other than **`LDAP Modify`** operations, can cause the **389 Directory Server** to modify internal attributes. For example, a **`BIND`** operation can cause updates to password failure counters. In these cases, **389 Directory Server** was updating attributes that could only be updated during an explicit **`LDAP Modify`** operation, such as the **`modifyTimestamp`** attribute. This update adds a new internal flag to skip the update of these attributes on other than **`Modify`** operations.

BZ#834056

Due to an invalid configuration setup in the **`Auto Memmber`** plug-in, the directory server became unresponsive under certain circumstances. With this update, the configuration file is validated, invalid configurations are not allowed, and the server no longer hangs.

BZ#834057

When using SNMP monitoring, **389 Directory Server** terminated at startup due to multiple **`ldap`** servers listed in the **`ldap-agent.conf`** file. With this update, the buffer between **`ldap`** servers no longer resets and **389 Directory Server** starts up regardless of the number of **`ldap`** servers listed in the configuration file.

BZ#834064

Previously, the **`dnaNextValue`** counter was incremented in the pre-operation stage. Consequently, if the operation failed, the counter was still incremented. This bug has been fixed and the **`dnaNextValue`** counter is not incremented if the operation fails.

BZ#834065

When a replication agreement was added without the LDAP BIND credentials, the replication process failed with a number of errors. With this update, **389 Directory Server** validates the replication configuration and ensures that all needed credentials are supplied. As a result, **389 Directory Server** rejects invalid replication configuration before attempting to replicate with invalid credentials.

BZ#834075

Previously, the **`logconv.pl`** script did not grab the correct search base, and as a consequence, the searching statistics were invalid. A new hash has been created to store connections and operation numbers from search operations. As a result, **logconv.pl** now grabs the correct search base and no longer produces incorrect statistics.

BZ#838706

When using the **Referential Integrity** plug-in, renaming a user DN did not rename the user's DN in the user's groups, unless that case matched exactly. With this update, case-insensitive comparisons or DN normalizations are performed, so that the member attributes are updated when the user is renamed.

BZ#840153

Previously, the **Attribute Uniqueness** plug-in did comparisons of un-normalized values. Consequently, using this plug-in and performing the **LDAP RENAME** operation on an entry containing one of the attributes which were tested for uniqueness by this plug-in caused the **LDAP RENAME** operation to fail with the following error:

```
Constraint Violation - Another entry with the same attribute value
already exists.
```

With this update, **Attribute Uniqueness** ensures that comparisons are performed between values which were normalized the same way, and **LDAP RENAME** works as expected in this situation.

BZ#841600

When the **Referential Integrity** plug-in was used with a delay time greater than 0, and the **LDAP RENAME** operation was performed on a **user** entry with DN specified by one or more **group** entries under the scope of the **Referential Integrity** plug-in, the user entry DN in the **group** entries did not change. The underlying source code has been modified and **LDAP RENAME** operations work as expected in the described scenario.

BZ#842437

Previously, the **DNA** plug-in could leak memory in certain cases for certain **MODIFY** operations. This update applies a patch to fix this bug and the modifications are freed as expected with no memory leaks.

BZ#842438

To improve the performance, the entry cache size is supposed to be larger then the primary database size if possible. Previously, **389 Directory Server** did not alert the user that the size of the entry cache was too small. Consequently, the user could not notice that the size of the entry cache was too small and that they should enlarge it. With this update, the configured entry cache size and the primary database size are examined, and if the entry cache is too small, a warning is logged in the error log.

BZ#842440

Previously, the **Memberof** plug-in code executed redundant DN normalizations and therefore slowed down the system. The underlying source code has been modified to eliminate redundant DN normalizations.

BZ#842441

Previously, the directory server could disallow changes that were made to the **nsds5ReplicaStripAttrs** attribute using the **ldapmodify** operation. Consequently, the attribute could only be set manually in the **dse.ldif** file when the server was shut down. With this update, the user is now able to set the **nsds5ReplicaStripAttrs** attribute using the **ldapmodify** operation.

BZ#850683

Previously, **389 Directory Server** did not check attribute values for the **nsds5ReplicaEnabled** feature which caused this feature to be disabled. With this update, **389 Directory Server** checks if the attribute value for **nsds5ReplicaEnabled** is valid and reports an error if it is not.

BZ#852088

When multi-master replication or database chaining was used with the **TLS/SSL** protocol, a server using client certificate-based authentication was unable to connect and connection errors appeared in the error log. With this update, the internal TLS/SSL and certificate setup is performed correctly and communication between servers works as expected.

BZ#852202

Previously, there was a race condition in the replication code. When two or more suppliers were attempting to update a heavily loaded consumer at the same time, the consumer could, under certain circumstances, switch to total update mode, erase the database, and abort replication with an error. The underlying source code has been modified to prevent the race condition. As a result, the connection is now protected against access from multiple threads and multiple suppliers.

BZ#852839

Due to the use of an uninitialized variable, a heavily loaded server processing multiple simultaneous delete operations could terminate unexpectedly under certain circumstances. This update provides a patch that initializes the variable properly and the directory server no longer crashes under these circumstances.

BZ#855438

Due to an incorrect attempt to send the **cleanallruv** task to the Windows WinSync replication agreements, the task became unresponsive. With this update, the WinSync replication agreements are ignored and the **cleanallruv** task no longer hangs in the described scenario.

BZ#856657

Previously, the **dirsrv** init script always returned 0, even when one or all the defined instances failed to start. This update applies a patch that improves the underlying source code and **dirsrv** no longer returns 0 if any of the defined instances failed.

BZ#858580

The schema reload task reloads schema files in the schema directory. Simultaneously, **Directory server** has several internal schemas which are not stored in the schema directory. These schemas were lost after the schema reload task was executed. Consequently, adding a **posixAccount** class failed. With this update, the internal schemas are stashed in a hash table and reloaded with external schemas. As result, adding a **posixAccount** is successful.

BZ#863576

When abandoning a Simple Paged Result request, **389 Directory Server** tried to acquire a connection lock twice, and because the connection lock is not self reentrant, **389 Directory Server** was waiting for the lock forever and stopped the server. This update provides a patch that eliminates the second lock and **389 Directory Server** works as expected in the described scenario.

BZ#864594

Previously, Anonymous Resource Limits applied to the **Directory Manager**. However, the Directory Manager should never have any limits. With this update, Anonymous Resource Limits no longer apply to Directory Manager.

BZ#868841

Even if an entry in AD did not contain all the required attributes for the POSIX account entry, the entry was synchronized to the DS as a POSIX entry. Consequently, the synchronization failed due to a “missing attribute” error. With this update, if an entry does not have all the required attributes, the POSIX account related attributes are dropped and the entry is synchronized as an ordinary entry. As a result, the synchronization is successful.

BZ#868853

When enabling replication level logging, the **Windows Sync** feature prints out what version of Windows or AD it detects. Previously, if the feature detected Windows Server 2003 or later, it printed out the following message:

```
detected win2k3 peer
```

This message could be confusing for users who had a later version of Windows, such as Windows Server 2008. This update modifies the message and now the following message is printed out:

```
detected win2k3 or later peer
```

BZ#870158

When a directory server was under a heavy load, deleting entries using the **Entry USN** feature caused tombstone entry indexes to be processed incorrectly. Consequently, the server could become unresponsive. This update fixes **389 Directory Server** to process tombstone indexes correctly, so that the server no longer hangs in this situation.

BZ#870162

Previously, the abandon request checked if the operation to abandon existed. When a search operation was already finished and an operation object had been released, a Simple Page Results request could fail due to this check. This update modifies **389 Directory Server** to skip operation existence checking, so that Simple Paged Results requests are always successfully aborted.

BZ#875862

Previously, the **DNA** plug-in attempted to dereference a NULL pointer value for the **dnaMagicRegen** attribute. Consequently, if **DNA** was enabled with no **dnamagicregen** value specified in its configuration and an entry with an attribute that triggered the DNA value generation was added, the server could terminate unexpectedly. This update improves the **389 Directory Server** to check for an empty **dnamagicregen** value before it attempts to dereference this value. As a result, **389 Directory Server** no longer crashes if no **dnamagicregen** attribute is specified.

BZ#876694

Previously, the code to check if a new superior entry existed, returned the “No such object” error only when the operation was requested by the directory manager. Consequently, if an ordinary non-root user attempted to use the **modrdn** operation to move an entry to a non-existing parent, the server terminated unexpectedly. This update provides a patch that removes the operator condition so that the check returns the “No such object” error even if the requester is an ordinary user, and the **modrdn** operation performed to the non-existing parent successfully fails for any user.

BZ#876727

aIf a filter contained a range search, the search retrieved one ID per one **idl_fetch** attribute and merged it to the ID list using the **idl_union()** function. This process is slow, especially when the range search result size is large. With this update, **389 Directory Server** switches to **ALLID** mode by using the **nsslapd-rangelookthroughlimit** switch instead of creating a complete ID list. As a result, the range search takes less time.

BZ#889083

Previously, if an entry was added or created without plug-in interference, the **nsslapd-plugin-track-binddn** feature filled the value of the **internalModifiersname** and **internalCreatorsname** attributes with the original bind DN instead of the name of the actual plug-in that modified or added the entry. This behavior is undesired; thus the **nsslapd-plugin-track-binddn** has been modified to always show the name of the actual plug-in that performed these operations.

BZ#891930

In previous versions of the 389-ds-base packages, an attempt to add a new entry to the **DNA** plug-in when the range of values was depleted caused the following error message to be returned:

```
ipa: ERROR: Operations error: Allocation of a new value for range
cn=posix
ids,cn=distributed numeric assignment plugin,cn=plugins,cn=config
failed!
Unable to proceed.
```

This message was missing all additional information in recent versions of the 389-ds-base packages. With this update, a patch is applied to provide the returned error message with additional information.

BZ#896256

Previously, an upgrade of the 389-ds-base packages affected configuration files. Consequently, custom configuration files were reverted to by default. This update provides a patch to ensure that custom changes in configuration files are preserved during the upgrade process.

Enhancements

BZ#746642

This update allows the **PAM Pass-through** plug-in to pass through the authentication process to different PAM stacks, based on domain membership or some property of the user entry, or both. Users now can login to Red Hat Directory Server using the credentials and account data from the correct AD server.

BZ#768084

This enhancement improves the **automember** plug-in to check existing entries and writes out the changes which occur if these entries are added.

BZ#782975

Previously, certain BINDs could cause only entries with the **modifiersname** or **modifystimestamp** attribute to be updated. This behavior led to unnecessary replication traffic. This enhancement introduces the new **replication** feature to decrease replication traffic caused by BINDs.

BZ#830331

This enhancement adds the new **`Disk Monitoring`** plug-in. When disk partitions fill up, **`Disk Monitoring`** returns a warning.

BZ#830340

Previously, two tasks were needed to be performed to clean an entire replication environment, the clean task and the release task. With this update, these tasks are incorporated in the **`Cleanallruv`** feature.

BZ#830347

Previously, the **`Paged Results`** search was allowed to perform only one request per connection. If the user used one connection, multiple Paged Results requests were not supported. This update adds support for multiple Paged Results requests.

BZ#830355

With this enhancement, obsolete elements in the Database Replica Update Vector (RUV) can be removed with the **`CLEANRUV`** operation, which removes them on a single supplier or master.

BZ#833222

This enhancement improves the **`memberOf`** plug-in to work across multiple back ends or suffixes.

BZ#834046

With this update, the **`Directory Server`** schema has been updated with the **`nsTLS1`** attribute to make **`TLS/SSL`** configuration easier.

BZ#834049

With this update, the **`Directory Server`** schema has been updated to include the **`DNA`** plug-in attributes.

BZ#834052

This enhancement improves the **`Access Control`** feature to control the Directory Manager account.

BZ#834053

This enhancement adds the ability to execute internal modification operations without changing the operational **`modifiersname`** attribute.

BZ#834058

With this update, the **`logconv.pl`** script has been enhanced with the **`getopts()`** function.

BZ#834060

Previously, the password lockout process was triggered not when maximum the number of tries was reached, but the time after. This behavior was not consistent with other vendors' LDAP servers. This enhancement adds the new option which allows users to specify the behavior of password lockout.

BZ#834061

Previously, DS did not include the **`SO_KEEPALIVE`** settings and connections could not be closed properly. This enhancement implements the **`SO_KEEPALIVE`** settings to the DS connections.

BZ#834063

With this update, the new `passwordTrackUpdateTime` attribute has been added. This attribute records a timestamp when the password was last changed.

BZ#834074

This enhancement adds the new `nsds5ReplicaEnabled` attribute to the replication agreement. If the replication agreement is disabled, it appears to be removed, but can be easily re-enabled and resumed.

BZ#847868

Previously, the `Windows Sync` plug-in did not support the RFC 2307 and 2307bis types of POSIX schema which supports Windows Active Directory (AD). Under these circumstances, users had to synchronize data between AD and DS manually which could return errors. This enhancement changes the POSIX attributes to prevent these consequences.

NOTE

Note, that for the initial release, when adding new user and group entries to the DS, the POSIX attributes are not synchronized with AD. Adding new user and group entries to AD synchronizes to DS, and modifying attributes synchronizes both ways.

BZ#852087

This enhancement improves the `Directory Server` schema to allow setting up an access control for the `nsslapd-readonly` attribute.

All users of 389-ds-base are advised to upgrade to these updated packages, which correct this issue and provide numerous bug fixes and enhancements. After installing this update, the 389 server service will be restarted automatically.

7.1.2. RHSA-2013:1182 — Important: 389-ds-base security update

Updated 389-ds-base packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The 389 Directory Server is an LDAPv3 compliant server. The base packages include the Lightweight Directory Access Protocol (LDAP) server and command-line utilities for server administration.

Security Fix

CVE-2013-4283

It was discovered that the 389 Directory Server did not properly handle the receipt of certain MOD operations with a bogus Distinguished Name (DN). A remote, unauthenticated attacker could use this flaw to cause the 389 Directory Server to crash.

All 389-ds-base users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing this update, the 389 server service will be restarted automatically.

7.2. ABRT, LIBREPORT AND BTPARSER

7.2.1. RHBA-2013:0290 — abrt, libreport and btparser bug fix and enhancement update

Updated abrt, libreport and btparser packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

ABRT is a tool to help users to detect defects in applications and to create a problem report with all the information needed by a maintainer to fix it. **ABRT** uses a plug-in system to extend its functionality.

The **`libreport`** libraries provide an API for reporting different problems in applications to different bug targets like Bugzilla, ftp, and trac.

The **btparser** utility is a backtrace parser and analyzer library, which works with backtraces produced by the GNU Project Debugger. It can parse a text file with a backtrace to a tree of C structures, allowing to analyze the threads and frames of the backtrace and process them.

NOTE

The btparser packages have been upgraded to upstream version 0.17, which provides a number of bug fixes and enhancements over the previous version. (BZ#846667)

Bug Fixes

BZ#799909

When the user attempted to remove a non-existing problem directory using the abrt-cli utility, abrt-cli emitted a confusing error message, such as in the following example:

```
# abrt-cli rm sdfsdf
'sdfsdf' does not exist
Can't connect to '/var/run/abrt/abrt.socket': Connection refused
```

With this update, abrt-cli has been modified to display only a message informing that such a problem directory does not exist.

BZ#808721, BZ#814594

When multiple kernel oopses occur in a short period of time, ABRT saves only the first oops because the later oopses are mostly only consequences of the first problem. However, ABRT sorted the processed oopses incorrectly so that the last oops that occurred was saved instead of the first oops. With this update, ABRT has been modified to process multiple kernel oopses in the correct order so that ABRT now saves the first oops as expected.

BZ#810309

Due to incorrect configuration, ABRT attempted to use the abrt-bodhi command, which is not available in Red Hat Enterprise Linux, while analyzing a backtrace. As a consequence, the user could see the following error message in the problem backtrace:

```
/bin/sh: line 6: abrt-bodhi: command not found
```

However, the error message had no influence on the problem reporting process. This update corrects the ABRT configuration so that the abrt-bodhi command is removed from the analyzer events and the error message no longer occurs.

BZ#811901

Previously, ABRT expected the dbus-send command to be always present on a system. However, ABRT does not depend on the related dbus package so there is no guarantee that the command is installed on the system. Therefore, when processing events that use the dbus-send command and the dbus package was not installed, ABRT emitted the following error message to the system log:

```
abrtd: /bin/sh: dbus-send: command not found
```

With this update, ABRT has been modified to verify the existence of dbus-send before attempting to call this command. The aforementioned error messages no longer occur in the system log.

BZ#813283

Previously, when running the report-gtk command with a non-existing problem directory, ABRT GUI attempted to process the problem directory. As a consequence, the terminal was flooded with GTK error messages. With this update, the ABRT GUI has been modified to no longer process non-existing problem directories. GUI now only prints a message informing that the processed directory does not exist and exits gracefully.

BZ#817051

The report tool always had to be executed from a problem directory even to perform actions which do not require the problem directory, such as adding an attachment to the existing bug report. When running from a directory that was not a problem directory, the report tool failed with the following error message:

```
'.' is not a problem directory
```

With this update, the report tool has been modified to not require a problem directory if the "-t" option is specified. The report tool can now be used to update existing bug reports without a need to run inside a problem directory.

BZ#815339, BZ#828673

Due to an error in the default libreport configuration, ABRT attempted to run the reporter-bugzilla command, which is not installed by default. This caused the following warning message to appear during problem reporting:

```
/bin/sh: line 4: reporter-bugzilla: command not found
```

However, the reporting process was not affected by this warning message. With this update, the default configuration of libreport has been corrected and reporter-bugzilla is no longer called by ABRT in the default configuration. The aforementioned warning message is no longer displayed during the reporting process.

BZ#820475

Previously, the abrt-ccpp init script did not emit any status message so that the service abrt-ccpp status command did not display any output. This update corrects the abrt-ccpp init script so that if the abrt-ccpp service is running the "abrt-ccpp hook is installed" message is displayed. If abrt-ccpp is stopped, the "abrt-ccpp hook is not installed" message appears.

BZ#826745

Certain ABRT libraries were previously built with wrong linker parameters and when running prelink on these libraries, the process returned error messages that the library contains "undefined non-weak symbols". With this update, the related makefiles have been corrected and the aforementioned errors no longer occur during prelink phase.

BZ#826924

ABRT ran the sosreport utility whenever a problem was detected. However, if the detected problem was caused by sosreport, ABRT could run sosreport in an infinite loop. Consequently, abrtd became unresponsive with extensive consumption of system resources. This update modifies ABRT to ignore consequent crashes in the same component that occur within a 20-second time period. The abrtd daemon no longer hangs if sosreport crashes.

BZ#847227

ABRT previously moved captured vmcore files from the default location in the /var/crash/ directory to the /var/spool/abrt/ directory. This affected the functioning of various tools that expected a vmcore file to be present in the /var/crash/ directory. This update modifies ABRT to use the CopyVMcore configuration option to specify whether to copy or move the core file. By default, ABRT no longer moves vmcore from the /var/crash/ directory but copies it.

BZ#847291

When disk space usage of the /var/spool/abrt/ directory reaches the specified disk space quota, ABRT finds and removes the largest problem directory. However, ABRT was previously unable to handle situations when the largest directory in /var/spool/abrt/ was not a problem directory. ABRT could not remove this directory and entered an infinite loop while searching for the largest directory to be removed. This update modifies ABRT to exclude unknown directories when determining which problem directory needs to be removed. The abrtd daemon no longer hangs in this scenario.

BZ#856960

When configured for centralized crash collection, ABRT previously printed logging credentials in plain text into the /var/log/messages log file on a dedicated system while uploading a crash report. This was a security risk, and so ABRT has been modified to no longer print the libreport-plugin-reportuploader plug-in credentials in log messages.

BZ#873815

When processing a large amount of problems, the inotify handling code could become out of sync, causing abrtd to be unable to read inotify events. Eventually, abrtd became unresponsive while trying to read an inotify event. If this happened and a Python application attempted to communicate with ABRT, abrtd and the Python application entered a deadlock situation. The daemon was busy trying to read an incoming inotify event and the Python script was waiting for a response from abrtd, which caused the application to become unresponsive as well. With this update, the ABRT exception handler sets timeout on a socket used for communication between abrtd and Python scripts, and also the inotify handling code has been modified. The abrtd daemon and Python applications no longer hang, however under heavy load, the inotify handling code can still become out of sync, which would cause abrtd to stop accepting new problems. If abrtd stops accepting new problems, it has to be restarted to work correctly again.

All users of abrt, libreport and btparser are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.3. ALSA-UTILS

7.3.1. RHBA-2013:0318 — alsa-utils bug fix and enhancement update

Updated alsa-utils packages that fix numerous bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The alsa-utils package contains command line utilities for the Advanced Linux Sound Architecture (ALSA).

NOTE

The alsa-utils package has been upgraded to upstream version 1.0.22, which provides a number of bug fixes and enhancements over the previous version. (BZ#838951)

Enhancement

BZ#814832

The alsa-utils package has been enhanced to work better with the GNOME volume control applet and sound preferences user interface.

Users of alsa-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.4. AMANDA

7.4.1. RHBA-2013:0427 — amanda bug fix update

Updated amanda packages that fix one bug are now available for Red Hat Enterprise Linux 6.

AMANDA, the Advanced Maryland Automatic Network Disk Archiver, is a backup system that allows the administrator of a LAN to set up a single master backup server to back up multiple hosts to one or more tape drives or disk files.

Bug Fix

BZ#752096

Previously, the amandad daemon, which is required for successful running of AMANDA, was located in the amanda-client package; however, this package was not required during installation of the amanda-server package. Consequently, AMANDA did not work properly. The amanda-client package has been added to the amanda-server dependencies and AMANDA works correctly now.

All AMANDA users are advised to upgrade to these updated packages, which fix this bug.

7.5. ANACONDA

7.5.1. RHBA-2013:0373 — anaconda bug fix and enhancement update

Updated anaconda packages that fix numerous bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The anaconda packages contain portions of the Anaconda installation program that can be run by the user for reconfiguration and advanced installation options.

Bug fixes

BZ#803883

Due to a bug in the multipath output parsing code, when installing Red Hat Enterprise Linux 6 on an IBM Power system with JBOD (Joined Body Of Disks — more than one hard drive attached to the same SAS controller), Anaconda could detect these multiple hard drives as a multipath device. This in turn caused the partitioning of the hard drive to fail, causing the installation of the system to fail as well. This update fixes the parsing code and the system is installed correctly.

BZ#848741

The Anaconda installer did not wait for BIOS storage devices to initialize when booted with the **`ks:bd:<bios disk>:/ks.cfg`** command-line option. As a consequence, BIOS storage devices could not be found and the installation could fail. To fix this bug, a delay algorithm for BIOS devices has been added to the code path used when booting with **`ks:bd:<bios disk>:/ks.cfg`**. As a result, Anaconda tries to wait for BIOS devices to initialize.

BZ#828650

The file system migration from ext2 to ext3 did not work because Anaconda did not modify the **`/etc/fstab`** file with the new ext3 file system type. Consequently, after the installation, the file system was mounted as an ext2 file system. With this update, Anaconda properly sets the migrated file system type in **`/etc/fstab`**. Thus, the file system is mounted as expected after installation.

BZ#886150

When installing Red Hat Enterprise Linux 6.4 Beta using the kickstart file, which included the partition scheme, LVM incorrectly removed the dashes from Logical Volume and Volume Group names. This caused the names to be malformed. This update fixes the aforementioned function to correctly format Logical Volume and Volume Group names during the installation process.

BZ#819486

Using IPv6 to install Red Hat Enterprise Linux 6.3 (both Alpha and Beta) on a z/VM guest enabled the user to SSH to the system and proceed with the language selection screen. However, after this step, the installation stopped and the SSH session was closed. With this update, the IPv6 installation on a z/VM guest is successful on Red Hat Enterprise Linux 6.4.

BZ#824963

A kickstart installation on unsupported hardware resulted in a dialog box asking for confirmation before proceeding with the installation process. As a consequence, it was not possible to perform a kickstart installation on unsupported hardware without any user input. To fix this bug, a new **`unsupported_hardware`** kickstart command has been added, which skips the interactive dialog warning when installing a system on unsupported hardware without user input.

BZ#811197

When a **/boot** partition was on a RAID device, inconsistent messages were returned because it was not supported to have this partition on such a device. These varied messages were confusing. To fix this bug, the error messages have been corrected to make sense and to not duplicate each other.

BZ#834689

Kernel modules containing Microsoft paravirtualized drivers were missing in the installation environment. To fix this bug, kernel modules with Microsoft PV have been added to the installation environment. As a result, better support for Microsoft virtualization is provided.

BZ#837835

Modules with VMware PV drivers were not included in the installation environment. This update adds the modules with VMware PV drivers to provide better virtualization support.

BZ#809641

The **udev** device manager was not used to resolve kickstart **raid --onpart** disk references. As a consequence, the **/dev/disk/by-id/** path could not be used properly. With this update, the **udev_resolve_devspec()** function is used to resolve the **--onpart** command option. As a result, the **raid --onpart** command can now use the **/dev/disk/by-id/** paths as expected.

BZ#809640

The Anaconda installer did not use the **udev** device manager to resolve **/dev/disk/by-id/** names. This meant the kickstart installation method did not work with **/dev/disk/by-id/** names. To fix this bug, Anaconda is now using **udev** to resolve **/dev/disk/by-id/** names. As a result, kickstart installations using **/dev/disk/by-id/** names work as expected.

BZ#804557

When installing a system using the text mode on a machine which already had Red Hat Enterprise Linux installed on it, a traceback error occurred when the **Back** button was used to go back from any dialog after the time zone dialog. With this update, disks are rescanned when moving back through the upgrade dialog, thus preventing this bug.

BZ#840723

The Anaconda installer called the **modprobe** tool without the **-b** argument that enabled blacklists. Consequently, modules were not blacklisted. To fix this bug, the required argument has been added to modprobe call. As a result, modules are blacklisted as expected.

BZ#851249

The Anaconda installer appended the ***boot=*** parameter on the command line whenever the ***fips=1*** parameter was used. With this update, Anaconda appends the ***boot=*** parameter only when the ***fips=1*** parameter is used and **/boot** is on a separate partition.

BZ#828029

This update fixes a typographical error in Korean version of a warning message used to alert users of a root password that is too simple.

BZ#681224

The Anaconda installer did not verify package checksums against the checksum in the repository metadata. A package which did not match the repo metadata checksum could be installed by the **Yum** utility. As a consequence, an incorrect package could be installed with no errors returned. This update adds verification of the package checksum against the checksum in the repository metadata.

BZ#656315

IPv6 configuration options of the installer's text UI (user interface) were using descriptions suggesting misleading meaning. Consequently, the description could mislead the users with DHCPv6 configured to use *Dynamic IPv6 configuration* (DHCPv6) which used DHCPv6 exclusively without using SLAAC automatic configuration. To fix this bug, the first option (**`Automatic neighbor discovery`**) has been renamed to **`Automatic`**; it is the (SLAAC) automatic configuration with the option of using a DHCPv6 server based on RA server configuration. The second option (**`Dynamic IP configuration (DHCPv6)`**) was renamed to **`Automatic, DHCP only`**, which describes the actual configuration to be used more accurately. These descriptions are now the same as those used by Network Manager. As a result, it is now clearer that the third option (**`Automatic, DHCP only`**) is using the DHCPv6 server exclusively.

BZ#836321

The command-line interface of the fcoe-utils package in Red Hat Enterprise Linux 6.3 was changed but the installer did not adapt to this change correctly. As a consequence, FCoE initiators were not able to log in to remote storages, which could then not be used for installation. To fix this bug, the **`fipvlan`** command arguments have been fixed to use the new **`-f`** option correctly. As a result, the installer now logs in to a FCoE remote storage correctly, and can be used for installation purposes.

BZ#823690

Repositories without size data caused a divide-by-zero error. Consequently, the installation failed. With this update, repositories without size data do not cause a divide-by-zero error and the installation succeeds.

BZ#848818

Support for the **`--hibernation`** option was only added to the **`part`** command. Consequently, **`--hibernation`** did not work with the **`logvol`** command. To fix this bug, support for **`--hibernation`** has been added to the **`logvol`** command. As a result, **`--hibernation`** now works with the **`logvol`** command.

BZ#784001

The **`linksleep`** option used to be applied only for the ***`ksdevice=`*** boot parameter using the value link. Consequently, when the ***`ksdevice`*** boot parameter was supplied a value containing a device name or a MAC address, the ***`linksleep`*** boot parameter did not take effect. Without waiting for the link, as required by the ***`linksleep`*** boot parameter, the installer could fail. To fix this bug, the ***`linksleep`*** boot parameter has been added to code paths where the to-be-activated device is specified. As a result, the ***`linksleep`*** boot parameter is honored also for installation where the ***`ksdevice`*** boot parameter is supplied a value containing a device name or a MAC address.

BZ#747278

The Anaconda installer did not check lengths of Logical Volume Manager (LVM) Volume Group names or Logical Volume names. As a consequence, an error occurred when creating disk partitions. To fix this bug, the length of LVM Volume Group names has been truncated to 32 characters and Logical Volume names to 16 characters. As a result, the installation completes successfully.

BZ#746925

Previously, Anaconda failed to enable add-on repositories when upgrading the system. Consequently, packages from the add-on repositories were not upgraded. This update allows Anaconda to enable add-on repositories when the system is upgrading and packages from the add-on repositories are upgraded as expected.

Enhancements

BZ#668065

With this update, the **`vlanid=boot`** and **`--vlanid=kickstart`** options can be used to allow users to set a virtual LAN ID (802.1q tag) for a specified network device. By specifying either one of these options, installation of the system can be done over a VLAN.

BZ#838736

This update allows users to select a LUKS encryption type in the kickstart configuration file.

BZ#662007

The **`bond boot`**, **`--bondslaves`** and **`--bondopts kickstart`** options can now be used to configure bonding as a part of the installation process. For more information on how to configure bonding, refer to the following parts of the Red Hat Enterprise Linux 6 Installation Guide: the *Kickstart Options* section and the *Boot Options* chapter.

BZ#813998

When using a kickstart file to install Red Hat Enterprise Linux 6.4, with the new **`fcoe kickstart`** option, users can now specify, which Fibre Channel over Ethernet (FCoE) devices should be activated automatically in addition to those discovered by Enhanced Disk Drive (EDD) services. For more information, refer to the *Kickstart* Options section in *Red Hat Enterprise Linux 6 Installation Guide*.

BZ#838742

RPM signatures are now generated using the **sha256sum** utility instead of the **md5sum** utility. With this update, the **sha256sum** command-line utility is included in Anaconda and is available in the shell during the installation process.

Users of anaconda are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.6. AUTHCONFIG

7.6.1. RHBA-2013:0486 — authconfig bug fix update

Updated authconfig packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The authconfig packages provide a command line utility and a GUI application that can configure a workstation to be a client for certain network user information and authentication schemes, and other user information and authentication related options.

Bug Fixes

BZ#862195

Prior to this update, the authconfig utility used old syntax for configuring the idmap mapping in the smb.conf file when started with the "--smbidmapuid" and "--smbidmapgid" command line options. Consequently, Samba 3.6 ignored the configuration. This update adapts authconfig to use the new syntax of the idmap range configuration so that Samba 3.6 can read it.

BZ#874527

Prior to this update, the authconfig utility could write an incomplete sssd.conf file when using the options "--enablesssd" or "--enablesssdauth". As a consequence, the sssd daemon did not start. With this update, authconfig no longer tries to create the sssd.conf file without complete information, and the sssd daemon can now start as expected.

All users of authconfig are advised to upgrade to these updated packages, which fix these bugs.

7.7. AUTOFS

7.7.1. RHBA-2013:0462 — autofs bug fix and enhancement update

Updated autofs packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The **autofs** utility controls the operation of the automount daemon. The automount daemon automatically mounts file systems when you use them, and unmounts them when they are not busy.

Bug Fixes

BZ#585059

When the automount daemon managed a large number of mount points, unmounting all active mount points could take a longer period of time than expected. If the daemon failed to exit within 45 seconds, the autofs init script timed out and returned a false-positive shutdown failure. To resolve this problem, the init script restart behavior has been modified. If the init script repeatedly fails to stop the daemon, the script terminates the daemon by sending the SIGKILL signal, which allows autofs to be restarted correctly.

BZ#819703

The automount interface matching code was able to detect only IPv4 interfaces. As a consequence, mount points were mounted with an incorrect mount type when using IPv6. To fix this problem, the automount interface matching code has been modified to use the getifaddrs() function insted of ioctl(). The automount interface matching code now properly recognizes IPv6 interfaces and both, IPv4 and IPv6 mounts are now mounted as expected.

BZ#827024, BZ#846852, BZ#847873

Previously, automount could terminate unexpectedly with a segmentation fault when using the internal hosts map. This could happen due to a function name collision between autofs and the libtirpc library. Both utilities called a debug logging function of the same name but with a different call signature. This update applies a series of patches that fix this problem by redefining the internal debug logging function in autofs. Also, several other bugs related to the autofs RPC function have been fixed. The automount daemon no longer crashes when using the internal hosts map and the libtirpc library is installed on the system.

BZ#834641

Due to an incorrectly placed port test in the get_nfs_info() function, autofs attempted to contact the portmap service when mounting NFSv4 file systems. Consequently, if the portmap service was disabled on the server, automount failed to mount the NFSv4 file systems with the following error message:

```
mount(nfs): no hosts available
```

With this update, the port check has been moved to the correct location in the code so that automount no longer contacts the server's port mapper when mounting NFSv4 file systems. NFSv4 file systems are mounted as expected in this scenario.

BZ#836422

Previously, the autofs internal hosts map could not be refreshed until all entries in the map had been unmounted. Consequently, users could not access newly exported NFS shares and any attempt to access such shares failed with the "No such file or directory" error message. This update allows the server export list to be updated by sending a HUP signal to the automount daemon. This causes automount to request server exports so the hosts map and associated automounts can be updated. Newly exported NFS shares can now be accessed as expected.

BZ#845512

Previously, the usage message displayed by the autofs init script did not contain the "usage" command entry. This update corrects the init script so it now displays all commands that can be used with the autofs service as expected.

BZ#856296

When stopping the autofs service, autofs did not correctly handle situations where a null map entry appeared after a corresponding indirect map entry in the autofs master map. As a consequence, automount attempted to unmount a unmount a non-existing automount point and became unresponsive. This update modifies autofs to process null map entries correctly so it no longer attempts to unmount non-existing automount points. The autofs service now stops gracefully as expected.

BZ#860184

Previously, the autofs init script did not allow any commands to be run by unprivileged users. However, it is desirable to let a non-root user check the status of autofs for example for monitoring purposes. Therefore, this update modifies the autofs init script to allow unprivileged users to execute the service autofs status command.

BZ#865311

Previous versions of autofs contained several typographical errors and misleading information in the auto.master(5) man page, and autofs.sysconfig and autofs.conf configuration files. This update corrects these bugs including the description of the MOUNT_NFS_DEFAULT_PROTOCOL and MOUNT_WAIT options.

BZ#868973

When attempting to mount an NFSv4 share from an unreachable NFSv4 server, autofs did not close IPv6 UDP sockets. This could eventually lead to depletion of free file descriptors and an automount failure. This update modifies autofs to close IPv6 UDP sockets as expected, and automount no longer fails due to too many open files in the described scenario.

BZ#892846

When using autofs with LDAP, the code used to perform a base DN search allowed a race between two threads executing the same function simultaneously to occur. As a result of this race, autofs could attempt to access already freed memory and terminate unexpectedly with a segmentation fault.

With this update, the code used to perform base DN searches has been moved to the function protected by a mutex, which prevents the race from occurring. The base DN searches are now performed only when refreshing settings of the map lookup modules.

Enhancements

BZ#846870

This update modifies autofs to allow configuring of separate timeout values for individual direct map entries in the autofs master map.

BZ#859947

With this update, the auto.master(5) man page has been updated to document the "-t, --timeout" option in the FORMAT options section.

BZ#866338

The auto.master(5) man page has been updated to clarify description of the "nobind" option when it is used with direct mount maps.

BZ#866396

The autofs.spec file has been modified to update build dependency of the autofs sss interface library. The library now requires the libsss_autofs package instead of sssd.

BZ#822733

This update improves debug logging of autofs. With debug logging set on, automount now reports whether it needs to read a mount map or not.

All users of autofs are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.7.2. RHBA-2013:0659 — autofs bug fix update

Updated autofs packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The autofs utility controls the operation of the automount daemon. The automount daemon automatically mounts file systems when in use and unmounts them when they are not busy.

Bug Fix

BZ#921147

Previously, when two nearly simultaneous mount requests occurred, NFS mounts mounted by autofs sometimes failed. This caused a fatal error for the host being probed and autofs failed the mount attempt with a "mount(nfs): no hosts available" error message. This update provides a patch which uses numeric protocol IDs, instead of protoent structures, and NFS mount attempts by autofs no longer fail in the described scenario.

Users of autofs are advised to upgrade to these updated packages, which fix this bug.

7.7.3. RHBA-2013:1278 — autofs bug fix update

Updated autofs packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The autofs utility controls the operation of the automount daemon. The automount daemon automatically mounts file systems when in use and unmounts them when they are not busy.

Bug Fix

BZ#1006163

> Previously, when mounting new mounts, the automount daemon stopped responding. This occurred due to an execution order race during an expire thread creation. This update refactors the code handling the expire thread creation and the problem no longer occurs.

Users of autofs are advised to upgrade to these updated packages, which fix this bug.

7.8. AUTOMAKE

7.8.1. RHSA-2013:0526 — Low: automake security update

An updated automake package that fixes one security issue is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Automake is a tool for automatically generating Makefile.in files compliant with the GNU Coding Standards.

Security Fix

CVE-2012-3386

> It was found that the distcheck rule in Automake-generated Makefiles made a directory world-writable when preparing source archives. If a malicious, local user could access this directory, they could execute arbitrary code with the privileges of the user running "make distcheck".

Red Hat would like to thank Jim Meyering for reporting this issue. Upstream acknowledges Stefano Lattarini as the original reporter.

Users of automake are advised to upgrade to this updated package, which corrects this issue.

7.9. AVAHI

7.9.1. RHBA-2013:0368 — avahi bug fix update

Updated avahi packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Avahi is an implementation of the DNS Service Discovery and Multicast DNS specifications for Zero Configuration Networking. It facilitates service discovery on a local network. Avahi and Avahi-aware applications allow you to plug your computer into a network and, with no configuration, view other people to chat with, view printers to print to, and find shared files on other computers.

Bug Fix

BZ#599435

Previously, the Avahi library packages required the Avahi daemon packages as a dependency. Consequently, whenever installing some of the Avahi libraries, the Avahi daemon was installed as well, which could pose a security risk in certain environments. This update removes these dependencies so that the Avahi libraries are now installed without the Avahi daemon.

All users of avahi are advised to upgrade to these updated packages, which fix this bug.

7.10. BACULA

7.10.1. RHBA-2012:1469 — bacula bug fix update

Updated bacula packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

The bacula packages provide a tool set that allows you to manage the backup, recovery, and verification of computer data across a network of different computers.

Bug Fixes

BZ#728693

Prior to this update, the logwatch tool did not check the "/var/log/bacula*" file. As a consequence, the logwatch report was incomplete. This update adds all log files to the logwatch configuration file. Now, the logwatch report is complete.

BZ#728697

Prior to this update, the bacula tool itself created the "/var/spool/bacula/log" file. As a consequence, this log file used an incorrect SELinux context. This update modifies the underlying code to create the /var/spool/bacula/log file in the bacula package. Now, this log file has the correct SELinux context.

BZ#729008

Prior to this update, the bacula packages were built without the CFLAGS variable "$RPM_OPT_FLAGS". As a consequence, the debug information was not generated. This update modifies the underlying code to build the packages with CFLAGS="$RPM_OPT_FLAGS. Now, the debug information is generated as expected.

BZ#756803

Prior to this update, the perl script which generates the my.conf file contained a misprint. As a consequence, the port variable was not set correctly. This update corrects the misprint. Now, the port variable is set as expected.

BZ#802158

Prior to this update, values for the "show pool" command was obtained from the "res->res_client" item. As a consequence, the output displayed incorrect job and file retention values. This update uses the "res->res_pool" item to obtain the correct values.

BZ#862240

Prior to this update, bacula-storage-common utility wrongly removed alternatives for the bcopy function during the update. As a consequence, the Link to bcop.{mysql,sqlite,postgresql} disappeared after updating. This update modifies the underlying code to remove these links directly in storage-

{mysql,sqlite,postgresql} and not in bacula-storage-common.

All users of bacula are advised to upgrade to these updated packages, which fix these bugs.

7.11. BASH

7.11.1. RHBA-2013:0306 — bash bug fix and enhancement update

Updated bash packages that fix three bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The bash packages provide the Bash (Bourne-again shell) shell, which is the default shell for Red Hat Enterprise Linux.

Bug Fixes

BZ#695656

Prior to this update, the trap handler could, under certain circumstances, lose signals during another trap initialization. This update blocks the signal while the trap string and handler are being modified. Now, the signals are no longer lost.

BZ#799958

Prior to this update, the manual page for trap in Bash did not mention that signals ignored upon entry cannot be listed later. This is now fixed and the manual page entry text is amended to "Signals ignored upon entry to the shell cannot be trapped, reset or listed".

BZ#800473

Prior to this update, the Bash shell called the trap handler within a signal handler when a SIGCHLD signal was received in job control mode and a handler for the signal was installed. This was a security risk and could cause Bash to enter a deadlock or to terminate unexpectedly with a segmentation fault due to memory corruption. With this update, the trap handler is now called outside of the signal handler, and Bash no longer enters a deadlock.

Enhancement

BZ#677439

This update enables the system-wide "/etc/bash.bash_logout" file. This allows administrators to write system-wide logout actions for all users.

All users of bash are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.11.2. RHBA-2013:1096 — bash bug fix update

Updated bash packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The GNU Bourne Again shell (Bash) is a shell and command language interpreter compatible with the Bourne shell (sh). Bash is the default shell for Red Hat Enterprise Linux.

Bug Fix

BZ#982610

> When a trap handler was invoked while running another trap handler, which was invoked during a pipeline call, bash was unresponsive. With this update, pipeline calls are saved and subsequently restored in this scenario, and bash responds normally.

All users of bash are advised to upgrade to these updated packages, which fix this bug.

7.12. BFA-FIRMWARE

7.12.1. RHBA-2013:0315 — bfa-firmware bug fix and enhancement update

Updated bfa-firmware packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The bfa-firmware package contains the Brocade Fibre Channel Host Bus Adapter (HBA) Firmware to run Brocade Fibre Channel and CNA adapters. This package also supports the Brocade BNA network adapter.

NOTE

The bfa-firmware packages have been upgraded to upstream version 3.0.3.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#830015)

All users of bfa-firmware are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.13. BIND-DYNDB-LDAP

7.13.1. RHBA-2013:0359 — bind-dyndb-ldap bug fix and enhancement update

Updated bind-dyndb-ldap packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The dynamic LDAP back end is a plug-in for BIND that provides back-end capabilities to LDAP databases. It features support for dynamic updates and internal caching that help to reduce the load on LDAP servers.

NOTE

The bind-dyndb-ldap package has been upgraded to upstream version 2.3, which provides a number of bug fixes and enhancements over the previous version. In particular, many persistent search improvements. Refer to /usr/share/doc/bind-dyndb-ldap/NEWS for a detailed list of the changes. (BZ#827414)

Bug Fixes

BZ#767496

> When persistent search was in use, the plug-in sometimes terminated unexpectedly due to an

assertion failure when the "rndc reload" command was issued and the LDAP server was not reachable. With this update, the code has been improved so that connection failures and reconnects are now handled more robustly. As a result, the plug-in no longer crashes in the scenario described.

BZ#829388

Previously, some relative domain names were not expanded correctly to FQDNs. Consequently, zone transfers sometimes contained relative domain names although they should only contain FQDNs (for example, they contained "name." record instead of "name.example.com."). The plug-in has been patched, and as a result, zone transfers now contain the correct domain names.

BZ#840381

Due to a bug in bind-dyndb-ldap, the named process sometimes terminated unexpectedly when a connection to LDAP timed out. Consequently, when a connection to LDAP timed out (or failed), the named process was sometimes aborted and DNS service was unavailable. The plug-in has been fixed and as a result, the plug-in now handles situations when a connection to LDAP fails gracefully.

BZ#856269

Due to a race condition, the plug-in sometimes caused the named process to terminate unexpectedly when it received a request to reload. Consequently, the DNS service was sometimes unavailable. A patch has been applied and as a result, the race condition during reload no longer occurs.

Enhancements

BZ#733711

LDAP in Red Hat Enterprise Linux 6.4 includes support for persistent search for both zones and their resource records. Persistent search allows the bind-dyndb-ldap plug-in to be immediately informed about all changes in an LDAP database. It also decreases network bandwidth usage required by repeated polling.

BZ#829340

Previously, it was only possible to configure IPv4 forwarders in LDAP. With this update, a patch has been added to the plug-in, and as a result, the plug-in is now able to parse and use IPv6 forwarders. BIND9 syntax for "forwarders" is required.

BZ#829385

Previously, it was impossible to share one LDAP database between multiple master servers; only one master server could be used. A new bind-dyndb-ldap option "fake_mname" which allows for overriding the master server name in the SOA record has been added. With this option it is now possible to override the master server name in the SOA record so that multiple servers can act as master server for one LDAP database.

BZ#840383

When multiple named processes shared one LDAP database and dynamically updated DNS records (via DDNS), they did not update the SOA serial numbers so it was impossible to serve such zones on secondary servers correctly (that is to say, they were not updated on slave servers). With this update, the plug-in can now update SOA serial numbers automatically, if configured to do so. Refer to the new "serial_autoincrement" option in the /usr/share/doc/bind-dyndb-ldap/README file for more details.

BZ#869323

This update provides support for the per-zone disabling of forwarding. Some setups require the disabling of forwarding per-zone. For example, company servers are configured as authoritative for a non-public zone and have global forwarding turned on. When the non-public zone contains delegation for a non-public subdomain, the zone must have explicitly disabled forwarding otherwise the glue records will not be returned. As a result, a server can now return delegation glue records for private zones when global forwarding is turned on. Refer to /usr/share/doc/bind-dyndb-ldap/README for detailed information.

Users of bind-dyndb-ldap are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.13.2. RHBA-2013:0739 — bind-dyndb-ldap bug fix update

Updated bind-dyndb-ldap packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The dynamic LDAP back-end is a plug-in for BIND that provides back-end capabilities to LDAP databases. It features support for dynamic updates and internal caching that helps to reduce the load on LDAP servers.

Bug Fix

BZ#928429

The bind-dyndb-ldap plug-in processed settings too early, which led to the daemon terminating unexpectedly with a segmentation fault during startup or reload. The bind-dyndb-ldap plug-in has been fixed to process its options later, and so, no longer crashes during startup or reload.

Users of bind-dyndb-ldap are advised to upgrade to these updated packages, which fix this bug.

7.14. BIND

7.14.1. RHSA-2013:0550 — Moderate: bind security and enhancement update

Updated bind packages that fix one security issue and add one enhancement are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly. DNS64 is used to automatically generate DNS records so IPv6 based clients can access IPv4 systems through a NAT64 server.

Security Fix

CVE-2012-5689

A flaw was found in the DNS64 implementation in BIND when using Response Policy Zones (RPZ). If a remote attacker sent a specially-crafted query to a named server that is using RPZ rewrite rules, named could exit unexpectedly with an assertion failure. Note that DNS64 support is not enabled by default.

Enhancement

BZ#906312

Previously, it was impossible to configure the maximum number of responses sent per second to one client. This allowed remote attackers to conduct traffic amplification attacks using DNS queries with spoofed source IP addresses. With this update, it is possible to use the new "rate-limit" configuration option in named.conf and configure the maximum number of queries which the server responds to. Refer to the BIND documentation for more details about the "rate-limit" option.

All bind users are advised to upgrade to these updated packages, which contain patches to correct this issue and add this enhancement. After installing the update, the BIND daemon (named) will be restarted automatically.

7.14.2. RHBA-2013:0475 — bind bug fix update

Updated bind packages that multiples bugs are now available for Red Hat Enterprise Linux 6.

BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.

Bug Fixes

BZ#827282

Previously, initscript sometimes reported a spurious error message "initscript: silence spurious "named.pid: No such file or directory" due to a race condition when the DNS server (named) was stopped. This spurious error message has been suppressed and is no longer reported in this scenario.

BZ#837165

Due to a race condition in the rbtdb.c source file, the named daemon could terminate unexpectedly with the INSIST error code. This bug has been fixed in the code and the named daemon no longer crashes in the described scenario.

BZ#853806

Previously, BIND rejected "forward" and "forwarders" statements in static-stub zones. Consequently, it was impossible to forward certain queries to specified servers. With this update, BIND accepts those options for static-stub zones properly, thus fixing this bug.

All users of bind are advised to upgrade to these updated packages, which fix these bugs.

7.14.3. RHSA-2013:0689 — Important: bind security and bug fix update

Updated bind packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

Security Fix

CVE-2013-2266

A denial of service flaw was found in the libdns library. A remote attacker could use this flaw to send a specially-crafted DNS query to named that, when processed, would cause named to use an excessive amount of memory, or possibly crash.

Note: This update disables the syntax checking of NAPTR (Naming Authority Pointer) resource records.

Bug Fix

BZ#928439

Previously, rebuilding the bind-dyndb-ldap source RPM failed with a "/usr/include/dns/view.h:76:21: error: dns/rrl.h: No such file or directory" error.

All bind users are advised to upgrade to these updated packages, which contain patches to correct these issues. After installing the update, the BIND daemon (named) will be restarted automatically.

7.14.4. RHBA-2013:1177 — bind bug fix update

Updated bind packages that fix one bug are now available for Red Hat Enterprise Linux 6.

BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.

Bug Fix

BZ#996955

Due to a missing gss_release_name() call, the BIND DNS server leaked memory when the "tkey-gssapi-credential" option was used in the BIND configuration. This update properly frees all memory in case the "tkey-gssapi-credential" is used, and BIND no longer leaks memory when GSSAPI credentials are used internally by the server for authentication.

Users of bind are advised to upgrade to these updated packages, which fix this bug. After installing the update, the BIND daemon (named) will be restarted automatically.

7.14.5. RHSA-2013:1114 — Important: bind security update

Updated bind packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. BIND includes a DNS server (named); a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating correctly.

Security Fix

CVE-2013-4854

A denial of service flaw was found in BIND. A remote attacker could use this flaw to send a specially-crafted DNS query to named that, when processed, would cause named to crash when rejecting the malformed query.

All bind users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

7.15. BINUTILS

7.15.1. RHBA-2013:0498 — binutils bug fix update

Updated binutils packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The binutils packages provide a set of binary utilities, including "ar" (for creating, modifying and extracting from archives), "as" (a family of GNU assemblers), "gprof" (for displaying call graph profile data), "ld" (the GNU linker), "nm" (for listing symbols from object files), "objcopy" (for copying and translating object files), "objdump" (for displaying information from object files), "ranlib" (for generating an index for the contents of an archive), "readelf" (for displaying detailed information about binary files), "size" (for listing the section sizes of an object or archive file), "strings" (for listing printable strings from files), "strip" (for discarding symbols), and "addr2line" (for converting addresses to file and line).

Bug Fixes

BZ#773526

In order to display a non-printing character, the readelf utility adds the "0x40" string to the character. However, readelf previously did not add that string when processing multibyte characters, so that multibyte characters in the ELF headers were displayed incorrectly. With this update, the underlying code has been corrected and readelf now displays multibyte and non-ASCII characters correctly.

BZ#825736

Under certain circumstances, the linker could fail to produce the GNU_RELRO segment when building an executable requiring GNU_RELRO. As a consequence, such an executable failed upon start-up. This problem affected also the libudev library so that the udev utility did not work. With this update, the linker has been modified so that the GNU_RELRO segment is now correctly created when it is needed, and utilities such as udev now work correctly.

All users of binutils are advised to upgrade to these updated packages, which fix these bugs.

7.16. BIOSDEVNAME

7.16.1. RHBA-2013:0434 — biosdevname bug fix and enhancement update

Updated biosdevname packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The biosdevname packages contain a udev helper utility which provides an optional convention for naming network interfaces; it assigns names to network interfaces based on their physical location. The utility is disabled by default, except for on a limited set of Dell PowerEdge, C Series and Precision Workstation systems.

NOTE

The biosdevname packages have been upgraded to upstream version 0.4.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#825142)

Bug Fixes

BZ#751373

The biosdevname utility ignored the SMBIOS version check for PCI network adapters. Consequently, PCI network adapter interfaces were renamed according to PCI slot and port numbers on systems with unsupported SMBIOS versions. With this update, the new biosdevname utility ensures that if the SMBIOS version is not supported, PCI network adapter interfaces are not renamed. As a result, PCI network adapters are named with the kernel default name in the scenario described.

BZ#804754

When using Single Root I/O Virtualization (SR-IOV) with embedded network interface devices, the biosdevname utility did not check the System Management BIOS (SMBIOS) type of the physical function for corresponding virtual functions. Consequently, biosdevname did not find SMBIOS type 41 structure for the device virtual functions and did not suggest interface names for these onboard network interfaces. With this update, biosdevname now looks up the SMBIOS type 41 structure for the device virtual functions in the corresponding physical function table. As a result, onboard network devices with virtual network interfaces are now renamed according to the biosdevname naming scheme.

BZ#815724

The biosdevname utility did not handle PCI cards with multiple ports. Consequently, only the network interface of the first port of these cards was renamed according to the biosdevname naming scheme. An upstream patch has been applied and biosdevname now handles PCI cards with multiple ports. As a result, all ports of multiple port PCI cards are now renamed according to the biosdevname naming scheme.

All users of biosdevname are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.17. BRIDGE-UTILS

7.17.1. RHEA-2013:0322 — bridge-utils enhancement update

Updated bridge-utils packages that add two enhancements are now available for Red Hat Enterprise Linux 6.

The bridge-utils packages contain utilities for configuration of the Linux Ethernet bridge. The Linux Ethernet bridge can be used to connect multiple Ethernet devices together. This connection is fully transparent: hosts connected to one Ethernet device see hosts connected to the other Ethernet devices directly.

Enhancements

BZ#676355

The man page was missing the multicast option descriptions. This update adds that information to the man page.

BZ#690529

This enhancement adds the missing feature described in the BRCTL(8) man page, that allows the user to get the bridge information for a simple bridge using the "brctl show $BRIDGE" command.

All users of bridge-utils are advise to upgrade to these updated packages, which add these enhancements.

7.18. BRLTTY

7.18.1. RHBA-2012:1231 — brltty bug fix update

Updated brltty packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

BRLTTY is a background process (daemon) which provides access to the Linux console (when in text mode) for a blind person using a refreshable braille display. It drives the braille display, and provides complete screen review functionality.

Bug Fixes

BZ#684526

Previously, building the brltty package could fail on the ocaml's unpackaged files error. This happened only if the ocaml package was pre-installed in the build root. The "--disable-caml-bindings" option has been added in the %configure macro so that the package now builds correctly.

BZ#809326

Previously, the /usr/lib/libbrlapi.so symbolic link installed by the brlapi-devel package incorrectly pointed to ../../lib/libbrlapi.so. The link has been fixed to correctly point to ../../lib/libbrlapi.so.0.5.

All users of brltty are advised to upgrade to these updated packages, which fix these bugs.

7.19. BTRFS-PROGS

7.19.1. RHBA-2013:0456 — btrfs-progs bug fix and enhancement update

Updated btrfs-progs packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The btrfs-progs packages provide user-space programs to create, check, modify, and correct any inconsistencies in a Btrfs file system.

NOTE

The btrfs-progs packages have been upgraded to upstream version 0.2, which provides a number of bug fixes and enhancements over the previous version, including support for slashes in file system labels and new commands "btrfs-find-root", "btrfs-restore", and "btrfs-zero-log". This update also modifies the btrfs-progs utility, so that it is now built with the -fno-strict-aliasing method. (BZ#865600)

All users of btrfs-progs are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.20. CCID

7.20.1. RHSA-2013:0523 — Low: ccid security and bug fix update

An updated ccid package that fixes one security issue and one bug are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Chip/Smart Card Interface Devices (CCID) is a USB smart card reader standard followed by most modern smart card readers. The ccid package provides a Generic, USB-based CCID driver for readers, which follow this standard.

Security Fix

CVE-2010-4530

An integer overflow, leading to an array index error, was found in the way the CCID driver processed a smart card's serial number. A local attacker could use this flaw to execute arbitrary code with the privileges of the user running the PC/SC Lite pcscd daemon (root, by default), by inserting a specially-crafted smart card.

Bug Fix

BZ#808115

Previously, CCID only recognized smart cards with 5V power supply. With this update, CCID also supports smart cards with different power supply.

All users of ccid are advised to upgrade to this updated package, which contains backported patches to correct these issues.

7.21. CDRKIT

7.21.1. RHBA-2012:1451 — cdrkit bug fix update

Updated cdrkit packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The cdrkit packages contain a collection of CD/DVD utilities for generating the ISO9660 file-system and burning media.

Bug Fix

BZ#797990

Prior to this update, overlapping memory was handled incorrectly. As a consequence, newly created paths could be garbled when calling "genisoimage" with the "-graft-points" option to graft the paths at points other than the root directory. This update modifies the underlying code to generate graft paths as expected.

All users of cdrkit are advised to upgrade to these updated packages, which fix this bug.

7.22. CERTMONGER

7.22.1. RHBA-2013:0320 — certmonger bug fix and enhancement update

Updated certmonger packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The certmonger daemon monitors certificates which have been registered with it, and as a certificate's not-valid-after date approaches, the daemon can optionally attempt to obtain a fresh certificate from a supported CA.

NOTE

The certmonger packages have been upgraded to upstream version 0.61, which provides a number of bug fixes and enhancements over the previous version. (BZ#827611)

Bug Fixes

BZ#810016

When certmonger was set up to not attempt to obtain a new certificate and the certificate's valid remaining time crossed a configured time to live (TTL) threshold, certmonger warned of a certificate's impending not-valid-after date. Certmonger then immediately logged the warning again, and continued to do so indefinitely, causing the /var/log/messages file to fill up with warnings. This bug has been fixed and certmonger returns a warning again only when another configured TTL threshold is crossed or the service is restarted.

BZ#893611

When certmonger attempts to save a certificate to an NSS database, it necessarily opens that database for writing. Previously, if any other process, including any other certmonger tasks that could require access to that database, had the database open for writing, that database could become corrupted. This update backports changes from later versions of certmonger which change its behavior. Now, actions that could result in database modifications are only performed one at a time.

All users of certmonger are advised to upgrade to these updated packages which fix these bugs and add these enhancements.

7.23. CIFS-UTILS

7.23.1. RHBA-2013:0408 — cifs-utils bug fix and enhancement update

Updated cifs-utils packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The SMB/CIFS protocol is a standard file sharing protocol widely deployed on Microsoft Windows machines. This package contains tools for mounting shares on Linux using the SMB/CIFS protocol. The tools in this package work in conjunction with support in the kernel to allow one to mount a SMB/CIFS share onto a client and use it as if it were a standard Linux file system.

Bug Fixes

BZ#856729

When the mount.cifs utility ran out of addresses to try, it returned the "System error" error code (EX_SYSERR) to the caller service. The utility has been modified and it now correctly returns the "Mount failure" error code (EX_FAIL).

BZ#826825

Typically, "/" characters are not allowed in user names for Microsoft Windows systems, but they are common in certain types of kerberos principal names. However, mount.cifs previously allowed the use of "/" in user names, which caused attempts to mount CIFS file systems to fail. With this package, "/" characters are now allowed in user names if the "sec=krb5" or "sec=krb5i" mount options are specified, thus CIFS file systems can now be mounted as expected.

BZ#838606

Previously, the cifs-utils packages were compiled without the RELRO (read-only relocations) and PIE (Position Independent Executables) flags. Programs provided by this package could be vulnerable to various attacks based on overwriting the ELF section of a program. The "-pie" and "-fpie" options enable the building of position-independent executables, and the "-Wl","-z","relro" turns on read-only relocation support in gcc. These options are important for security purposes to guard against possible buffer overflows that lead to exploits. The cifs-utils binaries are now built with PIE and full RELRO support. The cifs-utils binary is now more secured against "return-to-text" and memory corruption attacks and also against attacks based on the program's ELF section overwriting.

Enhancements

BZ#843596

With this update, the "strictcache", "actimeo", "cache=" and "rwpidforward" mount options are now documented in the mount.cifs(8) manual page.

BZ#843612

The "getcifsacl", "setcifsacl" and "cifs.idmap" programs have been added to the package. These utilities allow users to manipulate ACLs on CIFS shares and allow the mapping of Windows security IDs to POSIX user and group IDs.

BZ#843617

With this update, the cifs.idmap helper, which allows SID to UID and SID to GID mapping, has been added to the package. Also, the manual page cifs.upcall(8) has been updated and cifs.idmap(8) has been added.

Users of cifs-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.24. CLUSTERMON

7.24.1. RHBA-2013:0469 — clustermon bug fix update

Updated clustermon packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The clustermon packages provide the modclusterd daemon, which is a service for remote cluster management. Modclusterd serves as an abstraction of the cluster status that utilizes other clustermon parts exposed through conga, the Simple Network Management (SNMP), and Common Information Model (CIM).

Bug Fixes

BZ#865588

Prior to this update, the dynamic library that represents the CIM provider of a cluster status was not built with all the required dependencies and therefore certain symbols could not be resolved. As a consequence, the cluster status could not be accessed via CIM. This update adds the missing dependencies to the dynamic library. Now, the cluster status is accessible as expected.

BZ#885830

Prior to this update, the size of XML-formatted cluster configuration (as in cluster.conf file) greater than 200 kB might have crashed modcluster, a program assisting the ricci daemon in handling the cluster configuration file (cluster.conf), or modclusterd, a daemon providing cluster status. This update drops this restriction and both executables no longer abort with larger configurations.

All users of clustermon are advised to upgrade to these updated packages, which fix these bugs.

7.25. CLUSTER AND GFS2-UTILS

7.25.1. RHBA-2013:0287 — cluster and gfs2-utils bug fix and enhancement update

Updated cluster and gfs2-utils packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Cluster Manager is a collection of technologies working together to provide data integrity and the ability to maintain application availability in the event of a failure. Using redundant hardware, shared disk storage, power management, and robust cluster communication and application failover mechanisms, a cluster can meet the needs of the enterprise market.

Bug Fixes

BZ#785866

With this update, a minor typographical error has been fixed in the `/usr/share/cluster/cluster.rng.in.head` RELAX NG schema.

BZ#803477

Previously, the **fsck.gfs2** program printed irrelevant error messages when reclaiming free metadata blocks. These messages could have been incorrectly understood as file system errors. With this update, these messages are no longer displayed.

BZ#814807

The **master_wins** implementation of the **qdiskd** daemon was not sufficiently fast to hand over the master status during the ordered shutdown. Consequently, a temporary loss of quorum in the cluster could have occurred. With this update, **master_wins** has been modified to operate more quickly.

BZ#838047

Previously, the **master_wins** implementation of the **qdiskd** daemon did not check strictly for errors in the **/etc/cluster/cluster.conf** file. Consequently, with several incorrect options in **cluster.conf**, two quorate partitions could have been created at the same time. With this update, **master_wins** has been modified to perform strict error checking to avoid the creation of multiple quorate partitions.

BZ#838945

Prior to this update, an overly long cluster name in the **/etc/cluster/cluster.conf** file could cause a buffer overflow when running the **fsck.gfs2** utility on a GFS2 file system with a corrupt super block. With this update, the cluster name is truncated appropriately when the super block is being rebuilt. Now, the buffer overflow condition no longer occurs in the described case.

BZ#839241

Under certain circumstances, the **cman** cluster manager did not propagate two internal values across configuration reloads. Consequently, runtime inconsistencies could occur. This bug has been fixed, and the aforementioned error no longer occurs. Also, a corner case memory leak has been fixed.

BZ#845341

Prior to this update, the **fenced** daemon created the **/var/log/cluster/fenced.log** file with world readable permissions. With this update, **fenced** has been modified to set more strict security permissions for its log file. Also, permissions of an existing log file are automatically corrected if necessary.

BZ#847234

Previously, an insufficient buffer length limitation did not allow long configuration lines in the **/etc/cluster/cluster.conf** configuration file. Consequently, a long entry in the file caused the **corosync** utility to terminate unexpectedly with a segmentation fault. With this update, the length limit has been extended. As a result, the segmentation fault no longer occurs in this situation.

BZ#853180

When a GFS2 file system was mounted with the **lock_nolock** option enabled, the **cman** cluster manager incorrectly checked the currently used resources. Consequently, **cman** failed to start. This bug has been fixed, and **cman** now starts successfully in the described case.

BZ#854032

In certain corner cases, triggered especially when shutting down all cluster nodes at the same time, the cluster daemons failed to quit within the **cman** shutdown limit (10 seconds). Consequently, the **cman** cluster manager declared a shutdown error. With this update, the default shutdown timeout has been increased to 30 seconds to prevent the shutdown error.

BZ#857952

Under rare circumstances, the **fenced** daemon polled an incorrect file descriptor from the **cman** cluster manager. Consequently, **fenced** entered a loop and the cluster became unresponsive. This bug has been fixed, and the aforementioned error no longer occurs.

BZ#861340

The **fenced** daemon is usually started before the **messagebus** (D-BUS) service, which has no harmful operational effects. Previously, this behavior was recorded as an error message in the **/var/log/cluster/fenced.log** file. To avoid confusion, this error message is now entered into **/var/log/cluster/fenced.log** only when the log level is set to debugging.

BZ#862847

Previously, the **mkfs.gfs2 -t** command accepted non-standard characters, like slash (**/**), in the lock table name. Consequently, only the first cluster node was able to mount a GFS2 file system successfully. The next node attempting to mount a GFS2 file system became unresponsive. With this update, a more strict validation of lock table names has been introduced. As a result, cluster nodes no longer hang when special characters are used in lock table.

BZ#887787

Previously, when the client using the **cman** API called the **cman_stop_notification()** function after **cman** was already closed, the client terminated with the **SIGPIPE** signal. With this update, the underlying source code has been modified to address this issue, and the **MSG_NOSIGNAL** message is now displayed to warn the user in the described scenario.

BZ#888053

Prior to this update, the **gfs2_convert** tool was unable to handle certain corner cases when converting between GFS1 and GFS2 file systems. Consequently, the converted GFS2 file system contained errors. With this update, **gfs2_convert** has been fixed to detect these corner cases and adjust the converted file system accordingly

Enhancements

BZ#661764

The **cman** cluster manager is now supported with the **bonding mode** options **0**, **1**, and **2**. Prior to this update, only **bonding mode 1** was supported.

BZ#738704

This update adds support for clusters utilizing the Red Hat Enterprise Virtualization Manager native shared storage between nodes.

BZ#786118

The hostname aliases from the **/etc/hosts** file are now accepted as cluster node names across cluster applications.

BZ#797952

A new tool, **fence_check**, has been added to provide a method to test the fence configuration in a non disruptive way. The tool has been designed to run via the **crontab** utility for regular monitoring of fence devices.

BZ#821016

This update enables passing additional command line options to the **dlm_controld** daemon using the **/etc/sysconfig/cman** file.

BZ#842370

The Distributed Lock Manager (DLM) now allows tuning of DLM hash table sizes from the **/etc/sysconfig/cman** file. The following parameters can be set in the **/etc/sysconfig/cman** file:

```
DLM_LKBTBL_SIZE=<size_of_table>
DLM_RSBTBL_SIZE=<size_of_table>
DLM_DIRTBL_SIZE=<size_of_table>
```

which, in turn, modifies the values in the following files respectively:

```
/sys/kernel/config/dlm/cluster/lkbtbl_size
/sys/kernel/config/dlm/cluster/rsbtbl_size
/sys/kernel/config/dlm/cluster/dirtbl_size
```

BZ#857299

Previously, it was not possible to modify the default TCP port (21064) of the Distributed Lock Manager (DLM). With this update, the ***DLM_TCP_PORT*** configuration parameter has been added into the **/etc/sysconfig/cman** file. As a result, the DLM TCP port can be manually configured.

BZ#860048

The **fsck.gfs2** program now checks for formal mismatches between disk inode numbers and directory entries in the GFS2 file system.

BZ#860847

This update adds support for two and four node clusters utilizing the **rgmanager** daemon with the **rrp_mode** option enabled.

BZ#878196

This update adds support for clusters utilizing the VMware's VMDK (Virtual Machine Disk) disk image technology with the **multi-writer** option. This allows using VMDK-based storage with the **multi-writer** option for clustered file systems such as GFS2.

All users of cluster and gfs2-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.26. CONTROL-CENTER

7.26.1. RHBA-2013:0335 — control-center bug fix update

Updated control-center packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The control-center packages provide various configuration utilities for the GNOME desktop. These utilities allow the user to configure accessibility options, desktop fonts, keyboard and mouse properties, sound setup, desktop theme and background, user interface properties, screen resolution, and other settings.

Bug Fix

BZ#805069

Prior to this update, the status LEDs on Wacom tablets did not correctly indicate the current mode. With this update, the LEDs now indicate which of the Touch Ring or Touch Strip modes are active.

All users of control-center are advised to upgrade to these updated packages, which fix this bug.

7.27. COOLKEY

7.27.1. RHBA-2013:0397 — coolkey bug fix and enhancement update

Updated coolkey packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 6.

Coolkey is a smart card support library for the CoolKey, CAC (Common Access Card), and PIV (Personal Identity Verification) smart cards.

Bug Fixes

BZ#861108

Previously, Coolkey was unable to recognize PIV-I cards. This update fixes the bug and Coolkey now allows these cards to be read and display certificate information as expected.

BZ#879563

Prior to this update, The pkcs11_listcerts and pklogin_finder utilities were unable to recognize certificates and USB tokens on smart cards after upgrading the Coolkey library. A patch has been provided to address this issue and these utilities now work as expected.

BZ#806038

Previously, the remote-viewer utility failed to utilize a plugged smart card reader when a Spice client was running. Eventually, the client could terminate unexpectedly. Now, remote-viewer recognizes the reader and offers authentication once the card is inserted and the crashes no longer occur.

BZ#884266

Previously, certain new PIV-II smart cards could not be recognized by client card readers, the ESC card manager, or the pklogin_finder utility. A patch has been provided to address this issue and PIV-II cards now work with Coolkey as expected.

Enhancement

BZ#805693

Support for Oberthur Smart Cards has been added to the Coolkey library.

Users of coolkey are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.28. CORE X11 LIBRARIES

7.28.1. RHBA-2013:0294 — Core X11 libraries bug fix and enhancement update

Updated Core X11 libraries packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Core X11 libraries contain the base protocol of the X Window System, which is a networked windowing system for bitmap displays used to build graphical user interfaces on Unix, Unix-like, and other operating systems.

The pixman package has been upgraded to upstream version 0.18.4, which provides a number of bug fixes and enhancements over the previous version. (BZ#644296)

The following packages have been upgraded to their upstream versions to conform to X Window System Test Suite (XTS5):

Table 7.1. Upgraded packages

Package name	Upstream version	BZ number
libxcb	1.8.1	755654
libXcursor	1.1.13	755656
libX11	1.5.0	755657
libXi	1.6.1	755658
libXt	1.1.3	755659
libXfont	1.4.5	755661
libXrender	0.9.7	755662
libXtst	1.2.1	755663
libXext	1.3.1	755665
libXaw	1.0.11	755666
libXrandr	1.4.0	755667
libXft	2.3.1	755668

The following packages have been upgraded to their respective upstream versions, which provides a number of bug fixes and enhancements over the previous versions.

Table 7.2. Upgraded packages

Package name	Upstream version	BZ number
libXau	1.0.6	835172

Package name	Upstream version	BZ number
libXcomposite	0.4.3	835183
libXdmcp	1.1.1	835184
libXevie	1.0.3	835186
libXinerama	1.1.2	835187
libXmu	1.1.1	835188
libXpm	3.5.10	835190
libXres	1.0.6	835191
libXScrnSaver	1.2.2	835192
libXv	1.0.7	835193
libXvMC	1.0.7	835195
libXxf86dga	1.1.3	835196
libXxf86misc	1.0.3	835197
libXxf86vm	1.1.2	835198
libdrm	2.4.39	835202
libdmx	1.1.2	835203
pixman	0.26.2	835204
xorg-x11-proto-devel	7.6	835206
xorg-x11-util-macros	1.17	835207
xorg-x11-xtrans-devel	1.2.7	835276
xkeyboard-config	2.6	835284
libpciaccess	0.13.1	843585
xcb-proto	1.7	843593
libSM	1.2.1	843641

Bug Fixes

BZ#802559

Previously, in the xorg-x11-proto-devel package, the definition of the `_X_NONNULL` macro was incompatible with C89 compilers. Consequently, C89 applications could not be built in C89 mode if the `X11/Xfuncproto.h` file was included. This update fixes the macro definition to be compatible with C89 mode.

BZ#804907

Prior to this update, XI2 events were not properly initialized and could contain garbage values. A patch for the libXi package, which had been setting values to garbage, has been provided to fix this bug. Now, actual events no longer contain garbage values and are initialized as expected.

BZ#871460

Previously, the spec file of the xkeyboard-config package used the `%{dist}` macro in the Version tag. Although the standard Red Hat Enterprise Linux build environment defines this macro, it does not need to be defined. If it was not defined, `%{dist}` appeared literally in the resulting RPM package's version string when the package was rebuilt. The spec file has been corrected to use the conditional `%{?dist}` form, which expands to an empty string if `%{dist}` is not defined.

Users of Core X11 libraries are advised to upgrade to these updated packages, which fix these bugs and add various enhancements.

7.29. CORE X11 CLIENTS

7.29.1. RHSA-2013:0502 — Low: Core X11 clients security, bug fix, and enhancement update

Updated core client packages for the X Window System that fix one security issue, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The Core X11 clients packages provide the xorg-x11-utils, xorg-x11-server-utils, and xorg-x11-apps clients that ship with the X Window System.

Security Fix

CVE-2011-2504

It was found that the x11perfcomp utility included the current working directory in its PATH environment variable. Running x11perfcomp in an attacker-controlled directory would cause arbitrary code execution with the privileges of the user running x11perfcomp.

NOTE

The xorg-x11-utils and xorg-x11-server-utils packages have been upgraded to upstream version 7.5, and the xorg-x11-apps package to upstream version 7.6, which provides a number of bug fixes and enhancements over the previous versions. (BZ#835277, BZ#835278, BZ#835281)

All users of xorg-x11-utils, xorg-x11-server-utils, and xorg-x11-apps are advised to upgrade to these updated packages, which fix these issues and add these enhancements.

7.30. COROSYNC

7.30.1. RHBA-2013:0497 — corosync bug fix update

Updated corosync packages that fix several bugs and add multiple enhancements are now available for Red Hat Enterprise Linux 6.

The corosync packages provide the Corosync Cluster Engine and C Application Programming Interfaces (APIs) for Red Hat Enterprise Linux cluster software.

Bug Fixes

BZ#783068

Prior to this update, the **corosync-notifyd** service did not run after restarting the process. This update modifies the init script to wait for the actual exit of previously running instances of the process. Now, the **corosync-notifyd** service runs as expected after restarting.

BZ#786735

Prior to this update, an incorrect node ID was sent in recovery messages when **corosync** entered recovery. As a consequence, debugging problems in the source code was difficult. This update sets the correct node ID.

BZ#786737

Upon receiving the JoinMSG message in the OPERATIONAL state, a node enters the GATHER state. However, if JoinMSG was discarded, the nodes sending this JoinMSG could not receive a response until other nodes have had their tokens expired. This caused the nodes having entered the GATHER state spend more time to rejoin the ring. With this update, the underlying source code has been modified to address this issue.

BZ#787789

Prior to this update the netfilter firewall blocked input and output multicast packets, corosync coould become suspended, failed to create membership and cluster could not be used. After this update, corosync is no longer dependent on multicast loop kernel feature for local messages delivery, but uses the socpair unix dgram socket.

BZ#794744

Previously, on InfiniBand devices, **corosync** autogenerated the node ID when the configuration file or the cluster manager (**cman**) already set one. This update modifies the underlying code to recognize user-set mode IDs. Now, **corosync** autogenerates node IDs only when the user has not entered one.

BZ#821352

Prior to this update, **corosync** sockets were bound to a PEERs IP address instead of the local IP address when the IP address was configured as peer-to-peer (netmask /32). As a consequence, **corosync** was unable to create memberships. This update modifies the underlying code to use the correct information about the local IP address.

BZ#824902

Prior to this update, the **corosync** logic always used the first IP address that was found. As a consequence, users could not use more than one IP address on the same network. This update modifies the logic to use the first network address if no exact match was found. Now, users can bind to the IP address they select.

BZ#827100

Prior to this update, some sockets were not bound to a concrete IP address but listened on all interfaces in the UDPU mode. As a consequence, users could encounter problems when configuring the firewall. This update binds all sockets correctly.

BZ#847232

Prior to this update, configuration file names that consisted of more than 255 characters could cause **corosync** to abort unexpectedly. This update returns the complete item value. In case of the old ABI, **corosync** prints an error. Now, **corosync** no longer aborts with longer names.

BZ#838524

When corosync was running with the votequorum library enabled, votequorum's register reloaded the configuration handler after each change in the configuration database (confdb). This caused corosync to run slower and to eventually encounter an Out Of Memory error. After this update, a register callback is only performed during startup. As a result, corosync no longer slows down or encounters an Out Of Memory error.

BZ#848210

Prior to this update, the **corosync-notifyd** output was considerably slow and **corosync** memory grew when D-Bus output was enabled. Memory was not freed when **corosync-notifyd** was closed. This update modifies the **corosync-notifyd** event handler not to wait when there is nothing to receive and send from or to D-Bus. Now, **corosync** frees memory when the IPC client exits and **corosync-notifyd** produces output in speed of incoming events.

BZ#830799

Previously, the node cluster did not correspond with the `CPG` library membership. Consequently, the nodes were recognized as `unknown`, and `corosync` warning messages were not returned. A patch with an enhanced log from `CPG` has been provided to fix this bug. Now, the nodes work with `CPG` correctly, and appropriate warning messages are returned.

BZ#902397

Due to a regression, the `corosync` utility did not work with IPv6, which caused the network interface to be down. A patch has been provided to fix this bug. Corosync now works with IPv6 as expected, and the network interface is up.

BZ#838524

When corosync was running with the votequorum library enabled, votequorum's register reloaded the configuration handler after each change in the configuration database (confdb). This caused corosync to run slower and to eventually encounter an Out Of Memory error. After this update, a register

callback is only performed during startup. As a result, corosync no longer slows down or encounters an Out Of Memory error.

BZ#865039

Previously, during heavy cluster operations, one of the nodes failed sending numerous of the following messages to the syslog file:

```
dlm_controld[32123]: cpg_dispatch error 2
```

A patch has been applied to address this issue.

BZ#850757

Prior to this update, **corosync** dropped ORF tokens together with memb_join packets when using CPU timing on certain networks. As a consequence, the RRP interface could be wrongly marked as faulty. This update drops only memb_join messages.

BZ#861032

Prior to this update, the **corosync.conf** parser failed if the ring number was larger than the allowed maximum of 1. As a consequence, **corosync** could abort with a segmentation fault. This update adds a check to the **corosync.conf** parser. Now, an error message is printed if the ring number is larger than 1.

BZ#863940

Prior to this update, **corosync** stopped on multiple nodes. As a consequence, **corosync** could, under certain circumstances, abort with a segmentation fault. This update ensures that the **corosync** service no longer calls callbacks on unloaded services.

BZ#869609

Prior to this update, **corosync** could abort with a segmentation fault when a large number of corosync nodes were started together. This update modifies the underlying code to ensure that the NULL pointer is not dereferenced. Now, **corosync** no longer encounters segmentation faults when starting multiple nodes at the same time.

BZ#876908

Prior to this update, the **parsercorosync-objctl** command with additional parameters could cause the error "Error reloading DB 11". This update removes the reloading function and handles changes of changed objects in the configuration data base (**confdb**). Now, the logging level can be changed as expected.

BZ#873059

Several typos in the corosync(8) manual page have been fixed. Also, manual pages for confdb_* functions have been added.

Enhancements

BZ#770455

With this update, the **corosync** log includes the hostname and the process ID of the processes that join the cluster to allow for better troubleshooting.

BZ#794522

This update adds the manual page confdb_keys.8 to provide descriptions for **corosync** runtime statistics that are returned by **corosync-objctl**.

BZ#838743

This update adds the new trace level to filter **corosync** flow messages to improve debugging.

Users of corosync are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.30.2. RHBA-2013:0824 — corosync bug fix update

An updated corosync package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The Corosync packages provide the Corosync Cluster Engine and C Application Programming Interfaces (APIs) for Red Hat Enterprise Linux cluster software.

Bug Fix

BZ#929101

When running applications which used the Corosync IPC library, some messages in the dispatch() function were lost or duplicated. This update properly checks the return values of the dispatch_put() function, returns the correct remaining bytes in the IPC ring buffer, and ensures that the IPC client is correctly informed about the real number of messages in the ring buffer. Now, messages in the dispatch() function are no longer lost or duplicated.

Users of corosync are advised to upgrade to these updated packages, which fix this bug.

7.31. CPUSPEED

7.31.1. RHBA-2013:0490 — cpuspeed bug fix update

Updated cpuspeed packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The cpuspeed packages contain a daemon that dynamically changes speed of processors depending upon their current workload. This package also supports enabling CPU frequency scaling via in-kernel CPUfreq governors on Intel Centrino and AMD Athlon64/Opteron platforms.

Bug Fix

BZ#876738

Previously, the cpuspeed daemon used a naive method of getting the highest available scaling frequency. Consequently, on certain platforms, cpuspeed did not set the CPU to the correct maximum limit. A patch has been provided to address this issue and cpuspeed now sets the maximum speed correctly.

Users of cpuspeed are advised to upgrade to these updated packages, which fix this bug.

7.31.2. RHBA-2012:1404 — cpuspeed bug fix update

Updated cpuspeed packages that fix four bugs are now available for Red Hat Enterprise Linux 6.

The cpuspeed packages provide a daemon to manage the CPU frequency scaling.

Bug Fixes

BZ#642838

Prior to this update, the PCC driver used the “userspace” governor was loaded instead of the “ondemand” governor when loading. This update modifies the init script to also check the PCC driver.

BZ#738463

Prior to this update, the cpuspeed init script tried to set cpufrequency system files on a per core basis which was a deprecated procedure. This update sets thresholds globally.

BZ#616976

Prior to this update, the cpuspeed tool did not reset MIN and MAX values, when the configuration file was emptied. As a consequence, the MIN_SPEED or MAX_SPEED values were not reset as expected. This update adds conditionals in the init script to check these values. Now, the MIN_SPEED or MAX_SPEED values are reset as expected.

BZ#797055

Prior to this update, the init script did not handle the IGNORE_NICE parameter as expected. As a consequence, "-n" was added to command options when the IGNORE_NICE parameter was set. This update modifies the init script to stop adding the NICE option when using the IGNORE_NICE parameter.

All users of cpuspeed are advised to upgrade to these updated packages, which fix these bugs.

7.31.3. RHBA-2013:1153 — cpuspeed bug fix update

Updated cpuspeed packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The cpuspeed packages provide a daemon to manage the CPU frequency scaling.

Bug Fix

BZ#990474

The cpuspeed init script relied on the presence of the scaling_available_frequencies sysfs file to get the maximum possible scaling frequency for the system. Certain platforms did not provide the scaling_available_frequencies sysfs file, which caused the attempt to set the maximum scaling frequency to fail. With this update, the init script now reads the frequency from cpuinfo_max_speed, and setting the maximum scaling frequency now works on all platforms.

Users of cpuspeed are advised to upgrade to these updated packages, which fix this bug.

7.32. CRASH

7.32.1. RHBA-2013:0317 — crash bug fix and enhancement update

Updated crash packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The crash packages provide a self-contained tool that can be used to investigate live systems, and kernel core dumps created from the netdump, diskdump, kdump, and Xen/KVM "virsh dump" facilities from Red Hat Enterprise Linux.

NOTE

The crash packages have been upgraded to upstream version 6.1.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#840051)

Bug Fix

BZ#843093

A recent time-keeping backport to the Red Hat Enterprise Linux 6 kernel caused the crash utility to fail during initialization with the "crash: cannot resolve: xtime" error message. This update modifies crash to recognize and handle the time-keeping change in the kernel so that crash now successfully starts up as expected.

Enhancements

BZ#739094

The crash utility has been modified to support dump files in the firmware-assisted dump (fadump) format for the 64-bit PowerPC architecture.

BZ#834260

The "struct -o" option has been enhanced to accept a virtual address argument. If an address argument is entered, the structure members are prepended by their virtual address.

BZ#834276

The "bt" command has been enhanced by adding new "-s" and "[-xd]" options that allow displaying symbol names plus their offset in each frame. The default behavior is unchanged where only the symbol name is displayed. The symbol offset is expressed in the default output format, which can be overridden using the "-x" (hexadecimal) or "-d" (decimal) options.

All users of crash are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.33. CREATEREPO

7.33.1. RHBA-2013:0328 — createrepo bug fix and enhancement update

Updated createrepo packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The createrepo packages contain the utility that generates a common metadata repository from a directory of RPM packages.

NOTE

The createrepo packages have been upgraded to upstream version 0.9.9, which provides a number of bug fixes and enhancements over the previous version, including support for multitasking in the createrepo utility. This update also modifies the "--update" option to use the SQLite database instead of the XML files in order to reduce memory usage. (BZ#631989, BZ#716235)

Bug Fix

BZ#833350

Previously, the createrepo utility ignored the "umask" command for files created in the createrepo cache directory. This behavior caused problems when more than one user was updating repositories. The bug has been fixed, and multiple users can now update repositories without complications.

Enhancements

BZ#646644

It is now possible to use the "createrepo" command with both the "--split" and the "--pkglist" options simultaneously.

BZ#714094

It is now possible to remove metadata from the repodata directory using the modifyrepo program. This update also enhances updating of the existing metadata.

All users of createrepo are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.34. CTDB

7.34.1. RHBA-2013:0337 — ctdb bug fix update

Updated ctdb packages that fix various bugs and are now available for Red Hat Enterprise Linux 6.

The ctdb packages provide a clustered database based on Samba's Trivial Database (TDB) used to store temporary data.

NOTE

The ctbd packages have been upgraded to upstream version 1.0.114.5, which provides a number of bug fixes over the previous version. (BZ#838885)

Bug Fixes

BZ#758367

While running ctdb on the GFS2 file system, ctdb could ban a stable node when another node was started or stopped. This bug has been fixed by the rebase and stable nodes get no longer banned in the described scenario.

BZ#821715

Previously, on the Glusterfs file system, the ctdb lock file and configuration files were shared. Consequently, the ctdbd daemon running on a node terminated unexpectedly when another node in the cluster was brought down. This bug has been fixed by the rebase and ctdbd no longer crashes in the described scenario.

BZ#866670

After removing a ctdb node, the "ctdb status" command reported the same number of nodes as before the node was removed. A patch has been provided to address this issue and "ctdb status" now returns an accurate number of nodes after a remove operation.

Users of ctdb are advised to upgrade to these updated packages, which fix these bugs.

7.35. CURL

7.35.1. RHBA-2013:0393 — curl bug fix update

Updated curl packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The curl packages provide the **`cURL`** utility for getting files from HTTP, FTP, FILE, LDAP, LDAPS, DICT, TELNET, and TFTP servers, using any of the supported protocols. This utility offers many useful capabilities, such as proxy support, user authentication, FTP upload, HTTP post, and file transfer resume.

Bug Fixes

BZ#741935

The **`libssh2`** library did not sufficiently reflect its ABI extensions in its version, which prevented the RPM dependency scanner from adding the correct dependency of **`libcurl`** on an updated version of **`libssh2`**. Consequently, if the user updated **`libcurl`** without first updating **`libssh2`**, the update ended with incorrect linkage of **`libcurl`** and the user was then unable to update **`libssh2`** using **`yum`**. An explicit dependency of **`libcurl`** on an update version of **`libssh2`** has been added and **`yum`** can now be used to update **`libcurl`**.

BZ#746629

Previously, **`libcurl`** required certificates loaded from files to have unique file base names due to limitation of the legacy API of NSS (Network Security Services). Some packages using **`libcurl`** did not fulfil this requirement and caused nickname collisions within NSS. Now, **`libcurl`** has been modified to use a newer API of NSS, which does not suffer from this limitation, and packages using **`libcurl`** are now allowed to load certificates from files with unrestricted file names.

BZ#813127

Previously, **`libcurl`** misinterpreted the Content-Length HTTP header when receiving data using the chunked encoding. Consequently, **`libcurl`** failed to read the last chunk of data and the transfer terminated prematurely. An upstream patch has been applied to fix the handling of the header and the chunked encoding in **`libcurl`** now works as expected.

BZ#841905

A sub-optimally chosen identifier in cURL source files clashed with an identifier from a public header file introduced in a newer version of **`libssh2`**, which prevented the curl package from a successful build. An upstream patch has been applied on cURL source files, which fixes the identifier collisions and the package now builds as expected.

BZ#738456

The OpenLDAP suite was recently modified to use NSS instead of OpenSSL as the SSL back end. This change led to collisions between **`libcurl`** and OpenLDAP on NSS initialization and shutdown. Consequently, applications that were using both **`libcurl`** and OpenLDAP failed to establish SSL connections. This update modifies **`libcurl`** to use the same NSS API as OpenLDAP, which prevents collisions from occurring. Applications using OpenLDAP and **`libcurl`** can now connect to the LDAP server over SSL as expected.

BZ#719938

As a solution to a security issue, GSSAPI credential delegation was disabled, which broke the functionality of applications that were relying on delegation, incorrectly enabled by libcurl. To fix this issue, the **`CURLOPT_GSSAPI_DELEGATION`** **`libcurl`** option has been introduced in order to enable delegation explicitly when applications need it. All applications using GSSAPI credential delegation can now use this new **`libcurl`** option to be able to run properly.

BZ#772642

SSL connections could not be established with **`libcurl`** if the selected NSS database was broken or invalid. This update modifies the code of **`libcurl`** to initialize NSS without a valid database, which allows applications to establish SSL connections as expected.

BZ#873789

Previously, **`libcurl`** incorrectly checked return values of the SCP/SFTP write functions provided by **`libssh2`**. Negative values returned by those functions were treated as negative download amounts, which caused applications to terminate unexpectedly. With this update, all negative values are treated as errors and as such are properly handled on the **`libcurl`** level, thus preventing the crashes.

BZ#879592

Prior to this update, **`libcurl`** used an obsolete **`libssh2`** API for uploading files over the SCP protocol, which limited the maximum size of files being transferred on 32-bit architectures. Consequently, the 32-bit packages of **`libcurl`** were unable to transfer large files over SCP. With this update, a new **`libssh2`** API for SCP uploads is used, which does not suffer from this limitation, thus fixing this bug.

Enhancements

BZ#676596

Previously, **`libcurl`** provided only HTTP status codes in error messages when reporting HTTP errors. This could confuse users not familiar with HTTP. Now, **`libcurl`** has been improved to include the HTTP reason phrase in error messages, thus providing more understandable output.

BZ#730445

This update introduces a new option, **`--delegation`**, which enables Kerberos credential delegation in cURL.

Users of curl are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.36. CVS

7.36.1. RHBA-2012:1302 — cvs bug fix update

An updated cvs package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

[Update 19 November 2012] The file list of this advisory was updated to move the new cvs-inetd package from the base repository to the optional repository in the Client and HPC Node variants. No changes have been made to the packages themselves.

The Concurrent Versions System (CVS) is a version control system that can record the history of your files. CVS only stores the differences between versions, instead of every version of every file you have ever created. CVS also keeps a log of who, when, and why changes occurred.

BZ#671145

> Prior to this update, the C shell (csh) did not set the CVS_RSH environment variable to "ssh" and the remote shell (rsh) was used instead when the users accessed a remote CVS server. As a consequence, the connection was vulnerable to attacks because the remote shell is not encrypted or not necessarily enabled on every remote server. The cvs.csh script now uses valid csh syntax and the CVS_RSH environment variable is properly set at log-in.

BZ#695719

> Prior to this update, the xinetd package was not a dependency of the cvs package. As a result, the CVS server was not accessible through network. With this update, the cvs-inetd package, which contains the CVS inetd configuration file, ensures that the xinetd package is installed as a dependency and the xinetd daemon is available on the system.

All users of cvs are advised to upgrade to these updated packages, which fix these bugs.

7.37. DASH

7.37.1. RHBA-2012:1381 — dash bug fix update

Updated dash packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The dash packages provide the POSIX-compliant Debian Almquist shell intended for small media like floppy disks.

Bug Fix

BZ#706147

> Prior to this update, the dash shell was not an allowed login shell. As a consequence, users could not log in using the dash shell. This update adds the dash to the /etc/shells list of allowed login shells when installing or upgrading dash package and removes it from the list when uninstalling the package. Now, users can login using the dash shell.

All users of dash are advised to upgrade to these updated packages, which fix this bug.

7.38. DEVICE-MAPPER-MULTIPATH

7.38.1. RHBA-2013:0458 — device-mapper-multipath

Updated device-mapper-multipath packages that fix numerous bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The device-mapper-multipath packages provide tools for managing multipath devices using the device-mapper multipath kernel module.

Bug Fixes

BZ#578114

When the **`kpartx`** tool tried to delete a loop device that was previously created, and the **udev** utility had this loop device still open, the delete process would fail with the **`EBUSY`** error and **`kpartx`** did not attempt retry this operation. The **`kpartx`** tool has been modified to wait for one second and then retry deleting up to three times after the **`EBUSY`** error. As a result, loop devices created by **`kpartx`** are now always deleted as expected.

BZ#595692

The **`multipathd`** daemon only checked SCSI IDs when determining *World Wide Identifiers* (WWIDs) for devices. However, CCISS devices do not support SCSI IDs and could not be used by **Device Mapper Multipath**. With this update, **`multipathd`** checks CCISS devices for CCISS IDs properly and the devices are detected as expected.

BZ#810755

Some device configurations in the **`/usr/share/doc/device-mapper-multipath-0.X.X/multipath.conf.defaults`** file were out of date. Consequently, if users copied those configurations into the **`/etc/multipath.conf`** file, their devices would be misconfigured. The **`multipath.conf.defaults`** file has been updated and users can now copy configurations from it without misconfiguring their devices. Note that copying configurations from the **`multipath.conf.defaults`** file is not recommended as the configurations in that file are built into dm-multipath by default.

BZ#810788

Previously, **Device Mapper Multipath** stored multiple duplicate blacklist entries, which were consequently shown when listing the device-mapper-multipath's configuration. **Device Mapper Multipath** has been modified to check for duplicates before storing configuration entries and to store only the unique ones.

BZ#813963

Device Mapper Multipath had two *Asymmetric Logical Unit Access* (ALUA) prioritizers, which checked two different values. Certain ALUA setups were not correctly failing back to the primary path using either prioritizer because both values need to be checked and neither prioritizer checked them both. With this update, configuration options of both ALUA prioritizers now select the same prioritizer function, which checks both values as expected.

BZ#816717

When removing **`kpartx`** device partitions, the **`multipath -f`** option accepted only the device name, not the full pathname. Consequently, an attempt to delete a mulitpath device by the full pathname failed if the device had the **`kpartx`** partitions. **Device Mapper Mulitpath** has been modified to except the full pathname, when removing **`kpartx`** device partitions and deleting process no longer fails in the described scenario.

BZ#821885

Previously, the **`multipath -c`** option incorrectly listed SCSI devices, which were blacklisted by device type, as valid mulitpath path devices. As a consequence, **Device Mapper Multipath** could remove the partitions from SCSI devices that never ended up getting multipathed. With this update, **`multipath -c`** now checks if a SCSI device is blacklisted by device type, and reports it as invalid if it is.

BZ#822389

On reload, if a multipath device was not set to use the ***`user_friendly_names`*** parameter or a user-defined alias, **Device Mapper Multipath** would use its existing name instead of setting the WWID. Consequently, disabling ***`user_friendly_names`*** did not cause the multipath device names to change back to WWIDs on reload. This bug has been fixed and **Device Mapper Mulitpath** now sets the device name to its WWID if no ***`user_friendly_names`*** or user defined aliases are set. As a result, disabling ***`user_friendly_names`*** now allows device names to switch back to WWIDs on reload.

BZ#829065

When the *Redundant Disk Array Controller* (RDAC) checker returned the **`DID_SOFT_ERROR`** error, **Device Mapper Multipath** did not retry running the RDAC checker. This behavior caused **Device Mapper Multipath** to fail paths for transient issues that may have been resolved if it retried the checker. **Device Mapper Multipath** has been modified to retry the RDAC checker if it receives the **`DID_SOFT_ERROR`** error and no longer fails paths due to this error.

BZ#831045

When a multipath vector, which is a dynamically allocated array, was shrunk, **Device Mapper Multipath** was not reassigning the pointer to the array. Consequently, if the array location was changed by the shrinking, **Device Mapper Multipath** would corrupt its memory with unpredictable results. The underlying source code has been modified and **Device Mapper Multipath** now correctly reassigns the pointer after the array has been shrunk.

BZ#836890

Device Mapper Multipath was occasionally assigning a WWID with a white space for AIX VDASD devices. As a consequence, there was no single blacklist of WWID entry that could blacklist the device on all machines. With this update, **Device Mapper Multipath** assigns WWIDs without any white space characters for AIX VDASD devices, so that all machines assign the same WWID to an AIX VDASD device and the user is always able to blacklist the device on all machines.

BZ#841732

If two multipath devices had their aliases swapped, **Device Mapper Multipath** switched their tables. Consequently, if the user switched aliases on two devices, any application using the device would be pointed to the incorrect *Logical Unit Number* (LUN). **Device Mapper Multipath** has been modified to check if the device's new alias matches a different multipath device, and if so, to not switch to it.

BZ#860748

Previously, **Device Mapper Multipath** did not check the device type and WWID blacklists as soon as this information was available for a path device. **Device Mapper Multipath** has been modified to check the device type and WWID blacklists as soon as this information is available. As a result, **Device Mapper Multipath** no longer waits before blacklisting invalid paths.

BZ#869253

Previously, the **multipathd** daemon and the **kpartx** tool did not instruct the **libdevmapper** utility to skip the device creation process and let **udev** create it. As a consequence, sometimes **libdevmapper** created a block device in the **/dev/mapper/** directory, and sometimes **udev** created a symbolic link in the same directory. With this update, **multipathd** and **kpartx** prevent **libdevmapper** from creating a block device and **udev** always creates a symbolic link in the **/dev/mapper/** directory as expected.

Enhancements

BZ#619173

This enhancement adds a built-in configuration for SUN StorageTek 6180 to **Device Mapper Multipath**.

BZ#735459

To set up persistent reservations on multipath devices, it was necessary to set it up on all of the path devices. If a path device was added later, the user had to manually add reservations to that path. This enhancement adds the ability to set up and manage SCSI persistent reservations using device-mapper devices with the **mpathpersist** utility. As a result, when path devices are added, persistent reservations are set up as well.

BZ#810989

This enhancement updates the **multipathd init** script to load the **dm-multipathd** module, so that users do not have to do this manually in cases when no **/etc/multipath.conf** file is present during boot. Note that it is recommended to create the **multipath.conf** file by running the **mpathconf --enable** command, which also loads the **dm-multipath** module.

BZ#818367

When the RDAC path device is in service mode, it is unable to handle I/O requests. With this enhancement, **Device Mapper Multipath** puts an RDAC path device into a failed state if it is in the service mode.

BZ#839386

This update adds two new options to the defaults and devices sections of the **multipath.conf** file; the **retain_attached_hw_hander** option and the **detect_prio** option. By default, both of these options are set to **no** in the defaults section of the **multipath.conf** file. However, they are set to **yes** in the NETAPP/LUN device configuration file. If **retain_attach_hw_handler** is set to **yes** and the SCSI layer has attached a hardware handler to the device, **Device Mapper Multipath** sets the hardware as usual. If **detect_prio** is set to **yes**, **Device Mapper Multipath** will check if the device supports ALUA. If so, it automatically sets the prioritizer to the **alua** value. If the device does not support ALUA, **Device Mapper Multipath** sets the prioritizer as usual. This behavior allows NETAPP devices to work in ALUA or non-ALUA mode without making users change to built-in config.

In order for **retain_attached_hw_handler** to work, the SCSI layer must have already attached the device handler. To do this, the appropriate **scsi_dh_XXX** module, for instance **scsi_dh_alua**, must be loaded before the SCSI layer discovers the devices. To guarantee this, add the following parameter to the kernel command line:

```
rdloaddriver=scsi_dh_XXX
```

7.38.2. RHBA-2013:1127 — device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The device-mapper-multipath packages provide tools for managing multipath devices using the device-mapper multipath kernel module.

Bug Fix

BZ#988704

Prior to this update, Device Mapper Multipath did not check for NULL pointers before dereferencing them in the sysfs functions. As a result, the multipathd daemon could crash if a multipath device was resized while a path device was being removed. With this update, Device Mapper Multipath checks for NULL pointers in sysfs functions and no longer crashes when a multipath device is resized at the same time as a path device is removed.

Users of device-mapper-multipath are advised to upgrade to these updated packages, which fix this bug.

7.38.3. RHEA-2013:1176 — device-mapper-multipath enhancement update

Updated device-mapper-multipath packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The device-mapper-multipath packages provide tools for managing multipath devices using the device-mapper multipath kernel module.

Enhancement

BZ#993545

This update adds a new /etc/multipath.conf file default keyword, "reload_readwrite". If set to "yes", multipathd will listen to path device change events, and if the device has read-write access, it will reload the multipath device. This allows multipath devices to automatically have read-write permissions, as soon as the path devices have read-write access, instead of requiring manual intervention. Thus, when all the path devices belonging to a multipath device have read-write access, the multipath device will automatically allow read-write permissions.

Users of device-mapper-multipath are advised to upgrade to these updated packages, which add this enhancement.

7.39. DHCP

7.39.1. RHSA-2013:0504 — Low: dhcp security and bug fix update

Updated dhcp packages that fix one security issue and two bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The dhcp packages provide the Dynamic Host Configuration Protocol (DHCP) that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address.

Security Fix

CVE-2012-3955

> A flaw was found in the way the dhcpd daemon handled the expiration time of IPv6 leases. If dhcpd's configuration was changed to reduce the default IPv6 lease time, lease renewal requests for previously assigned leases could cause dhcpd to crash.

Bug Fixes

BZ#803540

> Prior to this update, the DHCP server discovered only the first IP address of a network interface if the network interface had more than one configured IP address. As a consequence, the DHCP server failed to restart if the server was configured to serve only a subnet of the following IP addresses. This update modifies network interface addresses discovery code to find all addresses of a network interface. The DHCP server can also serve subnets of other addresses.

BZ#824622

> Prior to this update, the dhclient rewrote the /etc/resolv.conf file with backup data after it was stopped even when the PEERDNS flag was set to "no" before shut down if the configuration file was changed while the dhclient ran with PEERDNS=yes. This update removes the backing up and restoring functions for this configuration file from the dhclient-script. Now, the dhclient no longer rewrites the /etc/resolv.conf file when stopped.

All users of DHCP are advised to upgrade to these updated packages, which fix these issues. After installing this update, all DHCP servers will be restarted automatically.

7.39.2. RHBA-2013:1255 — dhcp bug fix update

Updated dhcp packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address. The dhcp packages provide a relay agent and ISC DHCP service required to enable and administer DHCP on a network.

Bug Fix

BZ#1005672

> Previously, the dhcpd daemon or dhclient tool were started to serve on an alias interface for Infiniband network interface card. Consequently, dhcpd/dhclient terminated unexpectedly. One of patches was improved to cover this specific case, thus fixing the bug. Now, both dhcpd and dhclient run correctly.

All users of dhcp are advised to upgrade to these updated packages, which fix this bug.

7.40. DNSMASQ

7.40.1. RHSA-2013:0277 — Moderate: dnsmasq security, bug fix and enhancement update

Updated dnsmasq packages that fix one security issue, one bug, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The dnsmasq packages contain Dnsmasq, a lightweight DNS (Domain Name Server) forwarder and DHCP (Dynamic Host Configuration Protocol) server.

Security Fix

CVE-2012-3411

It was discovered that dnsmasq, when used in combination with certain libvirtd configurations, could incorrectly process network packets from network interfaces that were intended to be prohibited. A remote, unauthenticated attacker could exploit this flaw to cause a denial of service via DNS amplification attacks.

In order to fully address this issue, libvirt package users are advised to install updated libvirt packages. Refer to RHSA-2013:0276 for additional information.

Bug Fix

BZ#815819

Due to a regression, the lease change script was disabled. Consequently, the "dhcp-script" option in the /etc/dnsmasq.conf configuration file did not work. This update corrects the problem and the "dhcp-script" option now works as expected.

Enhancements

BZ#824214

Prior to this update, dnsmasq did not validate that the tftp directory given actually existed and was a directory. Consequently, configuration errors were not immediately reported on startup. This update improves the code to validate the tftp root directory option. As a result, fault finding is simplified especially when dnsmasq is called by external processes such as libvirt.

BZ#850944

The dnsmasq init script used an incorrect Process Identifier (PID) in the "stop", "restart", and "condrestart" commands. Consequently, if there were some dnsmasq instances running besides the system one started by the init script, then repeated calling of "service dnsmasq" with "stop" or "restart" would kill all running dnsmasq instances, including ones not started with the init script. The dnsmasq init script code has been corrected to obtain the correct PID when calling the "stop", "restart", and "condrestart" commands. As a result, if there are dnsmasq instances running in addition to the system one started by the init script, then by calling "service dnsmasq" with "stop" or "restart" only the system one is stopped or restarted.

BZ#887156

When two or more dnsmasq processes were running with DHCP enabled on one interface, DHCP

RELEASE packets were sometimes lost. Consequently, when two or more dnsmasq processes were running with DHCP enabled on one interface, releasing IP addresses sometimes failed. This update sets the SO_BINDTODEVICE socket option on DHCP sockets if running dnsmasq with DHCP enabled on one interface. As a result, when two or more dnsmasq processes are running with DHCP enabled on one interface, they can release IP addresses as expected.

All users of dnsmasq are advised to upgrade to these updated packages, which fix these issues and add these enhancements.

7.41. DOCBOOK-UTILS

7.41.1. RHBA-2012:1321 — docbook-utils bug fix update

Updated docbook-utils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The docbook-utils packages provide a set of utility scripts to convert and analyze SGML documents in general, and DocBook files in particular. The scripts are used to convert from DocBook or other SGML formats into file formats like HTML, man, info, RTF and many more.

Bug Fix

BZ#639866

Prior to this update, the Perl script used for generating manpages contained a misprint in the header. As a consequence, the header syntax of all manual pages that docbook-utils built was wrong. This update corrects the script. Now the manual page headers have the right syntax.

All users of docbook-utils are advised to upgrade to these updated packages, which fix this bug.

7.42. DOVECOT

7.42.1. RHSA-2013:0520 — Low: dovecot security and bug fix update

Updated dovecot packages that fix three security issues and one bug are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Dovecot is an IMAP server, written with security primarily in mind, for Linux and other UNIX-like systems. It also contains a small POP3 server. It supports mail in either of maildir or mbox formats. The SQL drivers and authentication plug-ins are provided as sub-packages.

Security Fixes

CVE-2011-2166, CVE-2011-2167

Two flaws were found in the way some settings were enforced by the script-login functionality of Dovecot. A remote, authenticated user could use these flaws to bypass intended access restrictions or conduct a directory traversal attack by leveraging login scripts.

CVE-2011-4318

A flaw was found in the way Dovecot performed remote server identity verification, when it was configured to proxy IMAP and POP3 connections to remote hosts using TLS/SSL protocols. A remote attacker could use this flaw to conduct man-in-the-middle attacks using an X.509 certificate issued by a trusted Certificate Authority (for a different name).

Bug Fix

BZ#697620

When a new user first accessed their IMAP inbox, Dovecot was, under some circumstances, unable to change the group ownership of the inbox directory in the user's Maildir location to match that of the user's mail spool (/var/mail/$USER). This correctly generated an "Internal error occurred" message. However, with a subsequent attempt to access the inbox, Dovecot saw that the directory already existed and proceeded with its operation, leaving the directory with incorrectly set permissions. This update corrects the underlying permissions setting error. When a new user now accesses their inbox for the first time, and it is not possible to set group ownership, Dovecot removes the created directory and generates an error message instead of keeping the directory with incorrect group ownership.

Users of dovecot are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the dovecot service will be restarted automatically.

7.43. DRACUT

7.43.1. RHBA-2013:0436 — dracut bug fix and enhancement update

Updated dracut packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The dracut packages include an event-driven initramfs generator infrastructure based on the udev device manager. The virtual file system, initramfs, is loaded together with the kernel at boot time and initializes the system, so it can read and boot from the root partition.

Bug Fixes

BZ#835646

Previously, dracut could not handle uppercase MAC addresses for the PXE "BOOTIF=" parameter. As a consequence, a machine with a dracut generated initramfs could not boot over the network, when the "BOOTIF=" parameter contained uppercase MAC addresses. With this update, dracut converts internally the MAC addresses to lowercase. Now, a machine with a dracut generated initramfs can boot over the network successfully when the "BOOTIF=" parameter contains uppercase MAC addresses.

BZ#831338

Previously, the default mount option of the /proc/ directory during boot up was "mount -t proc -o nosuid,noexec,nodev proc/proc". This resulted in inaccessible device nodes in the /proc/ directory for some kernel drivers. The default mount option of the /proc directory has been changed to "mount -t proc proc /proc" and all kernel modules now load successfully.

BZ#794751

Previously, dracut could not use the Internet Small Computer System Interface (iSCSI) and dmsquash-live module together. As a consequence, it was not possible to boot from a live medium over iSCSI. After this update, a dracut-generated initramfs, which contains the iSCSI and dmsquash-live modules, is able to boot a live medium via iSCSI. This can be done using the kernel command "root=live:LABEL=<partition-or-iso-label> netroot=iscsi: ".

BZ#813057

Previously, the new Brocade switch firmware took longer to complete the BCBx negotiation and a dracut-generated initramfs did not wait long enough for the DCBx negotiation. Now, the initramfs sleeps for three seconds after loading the "802q" kernel module and the DCBx negotiation with the new Brocade switch firmware completes successfully.

BZ#843105

When using the "live_ram" parameter for booting from live media, the dracut-generated initramfs ejected the medium. After this action, a reboot caused the machine to not boot from the medium again, even if it was intended. After this update, dracut honors the "no_eject" kernel command-line parameter. Now, if "no_eject" is given on the kernel command-line, the dracut-generated initramfs no longer ejects the live medium after copying it to the RAM.

BZ#850493

In FIPS mode, the kernel image has to be validated by a checksum. The sha512hmac tool reads the absolute path of the file to check from the checksum file. Previously, if "/boot" was not on a separate file system, dracut mounted the root file system to "/sysroot". The "/sysroot/boot" partition was not accessible with the "/boot" path and the sha512hmac tool could not access the file in "/boot" to check for. The check failed and the boot process was cancelled. Consequently, the boot processes did not succeed in FIPS mode if "/boot" was not on a separate file system. Now, dracut creates a symbolic link from the "/sysroot/boot" partition to the "/boot" partition in the initramfs and the sha512hmac tool can check the kernel image and the machine can continue booting, if the check was successful.

BZ#890081

Previously, the kernel module "scsi_dh_alua" was not included in the initramfs and as a consequence, "scsi_dh_alua" could not be preloaded via the "rdloaddriver" kernel command. The "scsi_dh_alua" kernel module is now included in the initramfs and "scsi_dh_alua" can be preloaded successfully using "rdloaddriver".

BZ#854416

Previously, dracut did not strip the kernel modules as mentioned in the man page. Consequently, initramfs size grew very big if the customer had kernel modules with a lot of debug info. The dracut utility now strips the kernel modules, except when in FIPS mode, and as a result, the initramfs size is smaller and can be loaded on machines with small memory.

Enhancements

BZ#823507

Documentation for the "rd_retry=" boot option has been added to the dracut(8) man page.

BZ#858187

The dracut utility can now boot from iSCSI on a network with virtual LANs configured, where the virtual LAN settings are stored in the iSCSI Boot Firmware Table BIOS.

Users of dracut are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.44. DROPWATCH

7.44.1. RHBA-2012:1182 — dropwatch bug fix update

Updated dropwatch packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The dropwatch package contains a utility that provides packet monitoring services.

Bug Fix

BZ#725464

> Prior to this update, the dropwatch utility could become unresponsive because it was waiting for a deactivation acknowledgement to be issued by an already deactivated or stopped service. With this update, dropwatch detects an attempt to deactivate/stop an already deactivated/stopped service and no longer hangs.

All users of dropwatch are advised to upgrade to these updated packages, which fix this bug.

7.45. DVD+RW-TOOLS

7.45.1. RHBA-2012:1320 — dvd+rw-tools bug fix update

Updated dvd+rw-tools packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The dvd+rw-tools packages contain a collection of tools to master DVD+RW/+R media.

BZ#807474

> Prior to this update, the growisofs utility wrote chunks of 32KB and reported an error during the last chunk when burning ISO image files that were not aligned to 32KB. This update allows the written chunk to be smaller than a multiple of 16 blocks.

All users of dvd+rw-tools are advised to upgrade to these updated packages, which fix this bug.

7.46. E2FSPROGS

7.46.1. RHBA-2013:0455 — e2fsprogs bug fix update

Updated e2fsprogs packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The e2fsprogs packages provide a number of utilities for creating, checking, modifying, and correcting any inconsistencies in the ext2 file systems.

Bug Fixes

BZ#806137

> On a corrupted file system, the "mke2fs -S" command could remove files instead of attempting to recover them. This bug has been fixed; the "mke2fs -S" command writes metadata properly and no longer removes files instead of recovering them.

BZ#813820

The resize2fs(8) man page did not list an ext4 file system as capable of on-line resizing. This omission has been fixed and the resize2fs(8) man page now includes all file systems that can be resized on-line.

BZ#858338

A special flag was used to indicate blocks allocated beyond the end of file on an ext4 file system. This flag was sometimes mishandled, resulting in file system corruption. Both the kernel and user space have been reworked to eliminate the use of this flag.

Enhancement

BZ#824126

Previously, users could use the e2fsck utility on a mounted file system, although it was strongly recommended not to do so. Using the utility on a mounted file system led to file system corruption. With this update, e2fsck opens the file system exclusively and fails when the file system is busy. This behavior avoids possible corruption of the mounted file system.

Users of e2fsprogs are advised to upgrade to these updated packages, which fix these bugs and add this enhancement

7.46.2. RHBA-2013:1502 — e2fsprogs bug fix update

Updated e2fsprogs packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The e2fsprogs packages provide a number of utilities for creating, checking, modifying, and correcting any inconsistencies in the ext2 file systems.

Bug Fix

BZ#1023351

The resize2fs utility did not properly handle resizing of an ext4 file system to a smaller size. As a consequence, files containing many extents could become corrupted if they were moved during the resize process. With this update, resize2fs now maintains a consistent extent tree when moving files containing many extents, and such files no longer become corrupted in this scenario.

Users of e2fsprogs are advised to upgrade to these updated packages, which fix this bug.

7.46.3. RHBA-2013:0970 — e2fsprogs bug fix update

Updated e2fsprogs packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The e2fsprogs packages provide a number of utilities for creating, checking, modifying, and correcting any inconsistencies in the ext2 file systems.

Bug Fix

BZ#974193

Some ext4 extent tree corruptions were not detected or repaired by e2fsck. Inconsistencies related to overlapping interior or leaf nodes in the extent tree were not detected, and the file system remained in an inconsistent state after an e2fsck. These inconsistencies were then detected by the kernel at run time. e2fsck is now able to detect and repair this class of corruptions in the file system.

Users of e2fsprogs are advised to upgrade to these updated packages, which fix this bug.

7.47. ECLIPSE-NLS

7.47.1. RHBA-2013:0357 — eclipse-nls bug fix and enhancement update

Updated eclipse-nls packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The eclipse-nls packages provide Native Language Support langpacks for the Eclipse IDE that contain translations into many languages.

NOTE

The clipse-nls packages have been upgraded to upstream version 3.6.0.v20120721114722, which updates the language packs and provides a number of bug fixes and enhancements over the previous version. (BZ#692358)

All users of eclipse-nls are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.48. ENVIRONMENT-MODULES

7.48.1. RHBA-2013:0316 — environment-modules bug fix update

Updated environment-modules packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The environment-modules packages provide for the dynamic modification of a user's environment using modulefiles. Each modulefile contains the information needed to configure the shell for an application. Once the package is initialized, the environment can be modified on a per-module basis using the module command which interprets modulefiles.

NOTE

The environment-modules package has been upgraded to upstream version 3.2.9c, which provides a number of bug fixes over the previous version. (BZ#765630)

Bug Fixes

BZ#818177

Due to an error in the Tcl library, some allocated pointers were invalidated inside the library. Consequently, running the "module switch" command in the tcsh shell led to a segmentation fault. The bug has been fixed and the system memory is now allocated and pointed to correctly.

BZ#848865

> Previously, the /usr/share/Modules/modulefiles/modules file contained an incorrect path. Consequently, an error occurred when the "module load modules" command was executed. With this update, the incorrect path has been replaced and the described error no longer occurs.

All users of environment-modules are advised to upgrade to these updated packages, which fix these bugs.

7.49. ESPEAK

7.49.1. RHBA-2012:1118 — espeak bug fix update

Updated espeak packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The espeak packages contain a software speech synthesizer for English and other languages. eSpeak uses a "formant synthesis" method, which allows many languages to be provided in a small size.

Bug Fix

BZ#789997

> Previously, eSpeak manipulated the system sound volume. As a consequence, eSpeak could set the sound volume to maximum regardless of the amplitude specified. The sound volume management code has been removed from eSpeak, and now only PulseAudio manages the sound volume.

All users of espeak are advised to upgrade to these updated packages, which fix this bug.

7.50. ETHTOOL

7.50.1. RHBA-2013:0366 — ethtool bug fix and enhancement update

Updated ethtool packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The ethtool utility allows the querying and changing of Ethernet adapter settings, such as port speed, auto-negotiation, and device-specific performance options.

NOTE

The ethtool packages have been upgraded to upstream version 3.5, which provides a number of bug fixes and enhancements over the previous version. (BZ#819846)

All users of ethtool are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.51. EVOLUTION-DATA-SERVER

7.51.1. RHBA-2013:0410 — evolution-data-server bug fix update

Updated evolution-data-server packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The evolution-data-server packages provide a unified back end for applications which interact with contacts, task and calendar information. Evolution Data Server was originally developed as a back end for Evolution, but is now used by various other applications.

Bug Fix

BZ#734048

> The CalDav calendar back end was converting Uniform Resource Identifiers (URIs) with unescaped space characters or the "%20" string to "%2520". As a consequence, rendering the back end did not allow to contact the remote CalDav service that caused CalDav calendars to be inaccessible. This bug has been fixed and evolution-data-server works correctly in the described scenario.

All users of evolution-data-server are advised to upgrade to these updated packages, which fix this bug.

7.52. EVOLUTION

7.52.1. RHSA-2013:0516 — Low: evolution security and bug fix update

Updated evolution packages that fix one security issue and three bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Evolution is the GNOME mailer, calendar, contact manager and communication tool. The components which make up Evolution are tightly integrated with one another and act as a seamless personal information-management tool.

Security Fix

CVE-2011-3201

> The way Evolution handled mailto URLs allowed any file to be attached to the new message. This could lead to information disclosure if the user did not notice the attached file before sending the message. With this update, mailto URLs cannot be used to attach certain files, such as hidden files or files in hidden directories, files in the /etc/ directory, or files specified using a path containing "..".

Red Hat would like to thank Matt McCutchen for reporting this issue.

Bug Fixes

BZ#707526

> Creating a contact list with contact names encoded in UTF-8 caused these names to be displayed in the contact list editor in the ASCII encoding instead of UTF-8. This bug has been fixed and the contact list editor now displays the names in the correct format.

BZ#805239

> Due to a bug in the evolution-alarm-notify process, calendar appointment alarms did not appear in some types of calendars. The underlying source code has been modified and calendar notifications work as expected.

BZ#890642

An attempt to print a calendar month view as a PDF file caused Evolution to terminate unexpectedly. This update applies a patch to fix this bug and Evolution no longer crashes in this situation.

All evolution users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. All running instances of Evolution must be restarted for this update to take effect.

7.53. FCOE-TARGET-UTILS

7.53.1. RHBA-2013:0457 — fcoe-target-utils bug fix and enhancement update

Updated fcoe-target-utils packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The fcoe-target-utils packages provide a command-line interface for configuring FCoE LUNs (Fibre Channel over Ethernet Logical Unit Numbers) and backstores.

Bug Fixes

BZ#819698

Prior to this update, stopping the fcoe-target daemon did not stop the target session when rebooting. This update improves the fcoe-target script and the fcoe-target daemon can now properly shut down the kernel target.

BZ#824227

Prior to this update, a delay in the FCoE interface initialization sometimes resulted in the target configuration not being loaded for that interface. This update permits target configuration for absent interfaces, allowing target and interface configuration in any order.

BZ#837730

Prior to this update, specifying a nonexistent backing file when creating a backstore resulted in the unhelpful Python error "ValueError: No such path". This update reports the error in a more helpful way.

BZ#837992

Prior to this update, attempting to remove a storage object in a backstore resulted in a Python error. This update fixes the problem and storage objects can now be removed as expected.

BZ#838442

Prior to this update, attempting to redirect the output of targetcli resulted in a Python error. This update allows targetcli to be successfully redirected.

BZ#846670

Due to a regression, creating a backstore resulted in a Python error. This update allows backstore creation without error.

Enhancements

BZ#828096

Prior to this update, backstore size listing abbreviations did not clearly specify between power of 10 (for example Gigabyte) and power of 2 (Gibibyte). This update lists backstore sizes using power-of-2 sizes and labels them as such.

BZ#828681

The caching characteristics of backstores are now exposed via the SCSI Write Cache Enable (WCE) bit to initiators, instead of being set opaquely via the "buffered-mode" backstore setting. The default setting for WCE is "on".

All users of fcoe-target-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.54. FCOE-UTILS

7.54.1. RHBA-2013:0412 — fcoe-utils bug fix and enhancement update

Updated fcoe-utils packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The fcoe-utils packages provide Fibre Channel over Ethernet (FCoE) utilities, such as the fcoeadm command line tool for configuring FCoE interfaces, and the fcoemon service to configure DCB Ethernet QOS filters.

NOTE

The fcoe-utils packages have been upgraded to upstream version 1.0.24, which provides a number of bug fixes and enhancements over the previous version.

Bug Fix

BZ#867117

When turning off DCB on a Fibre Channel over Ethernet (FCoE) initiator interface connected to a Cisco Fibre Channel Forwarder (FCF), the fcoemon utility disabled the interface but the FCoE interface was re-enabled by a Netlink event before DCB was operational again. Consequently, the interface did not operate in degraded mode with LUNS present as expected and the output of the "ip l" and "fcoeadm -i" commands was contradictory. A patch has been applied to the fcoemon utility to ensure DCB is operational again before enabling the FCoE interface when a link is brought up. In addition, a patch has been applied to fcoe-utils to improve error handling and error messages related to creating and deleting of FCoE interfaces when DCB is not ready.

Enhancement

BZ#826291

Support for VLAN notification with VLAN ID 0 has been added. If a VLAN notification has the tag "VLAN 0", the physical port will now be activated. The VLAN interface will not be created but FCoE will be started on the physical interface itself.

All users of fcoe-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.55. FEBOOTSTRAP

7.55.1. RHBA-2013:0432 — febootstrap bug fix update

Updated febootstrap packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The febootstrap packages provide a tool to create a basic Red Hat Enterprise Linux or Fedora file system, and build initramfs (initrd.img) or file system images.

Bug Fix

BZ#803962

The "febootstrap-supermin-helper" program is used when opening a disk image using the libguestfs API, or as part of virt-v2v conversion. Previously, this tool did not always handle the "-u" and "-g" options correctly when the host used an LDAP server to resolve user names and group names. This caused the virt-v2v command to fail when LDAP was in use. With this update, the "febootstrap-supermin-helper" program has been modified to parse the "-u" and "-g" options correctly, so that virt-v2v works as expected in the described scenario.

Users of febootstrap are advised to upgrade to these updated packages, which fix this bug.

7.56. FENCE-AGENTS

7.56.1. RHBA-2013:0540 — fence-agents bug fix update

Updated fence-agents packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

Red Hat fence agents are a collection of scripts for handling remote power management for cluster devices. They allow failed or unreachable nodes to be forcibly restarted and removed from the cluster.

Bug Fixes

BZ#908409

Previously, when fencing a Red Hat Enterprise Linux cluster node with the fence_soap_vmware fence agent, the agent terminated unexpectedly with a traceback if it was not possible to resolve a hostname of an IP address. With this update, a proper error message is displayed in the described scenario.

BZ#908401

Due to incorrect detection on newline characters during an SSH connection, the fence_drac5 agent could terminate the connection with a traceback when fencing a Red Hat Enterprise Linux cluster node. Only the first fencing action completed successfully but the status of the node was not checked correctly. Consequently, the fence agent failed to report successful fencing. When the "reboot" operation was called, the node was only powered off. With this update, the newline characters are correctly detected and the fencing works as expected.

All users of fence-agents are advised to upgrade to these updated packages, which fix these bugs.

7.56.2. RHBA-2013:0286 — fence-agents bug fix and enhancement update

Updated fence-agents packages that fix multiple bugs and add four enhancements are now available for Red Hat Enterprise Linux 6.

The fence-agents packages provide the Red Hat fence agents to handle remote power management for cluster devices. The fence-agents allow failed or unreachable nodes to be forcibly restarted and removed from the cluster.

Bug Fixes

BZ#769798

The speed of fencing is critical because otherwise, broken nodes have more time to corrupt data. Prior to this update, the operation of the fence_vmware_soap fence agent was slower than expected when used on the VMWare vSphere platform with hundreds of virtual machines. With this update, the fencing process is faster and does not terminate if virtual machines without an UID are encountered.

BZ#822507

Prior to this update, the attribute "unique" in XML metadata was set to TRUE (1) by default. This update modifies the underlying code to use FALSE (0) as the default value because fence agents do not use these attributes.

BZ#825667

Prior to this update, certain fence agents did not generate correct metadata output. As a result, it was not possible to use the metadata for automatic generation of manual pages and user interfaces. With this update, all fence agents generate their metadata as expected.

BZ#842314

Prior to this update, the fence_apc script failed to log into APC power switches where firmware changed the end-of-line marker from CR-LF to LF. This update modifies the script to log into a fence device as expected.

BZ#863568

Prior to this update, the fence_rhevm agent failed to run the regular expression get_id regex when using a new href attribute. As a consequence, the plug status was not available. This update modifies the underlying code to show the correct status either as ON or OFF.

Enhancements

BZ#740869

This update adds the fence_ipdu agent to support IBM iPDU fence devices in Red Hat Enterprise Linux 6.

BZ#752449

This update adds the fence_eaton agent to support Eaton ePDU (Enclosure Power Distribution Unit) devices in Red Hat Enterprise Linux 6.

BZ#800650

This update adds symlinks for common fence types that utilize standards-based agents in Red Hat Enterprise Linux 6.

BZ#818337

This update adds the fence_bladecenter agent to the fence-agents packages in Red Hat Enterprise Linux 6 to support the --missing-as-off feature for the HP BladeSystem to handle missing nodes as switched off nodes so that fencing can end successfully even if a blade is missing.

BZ#837174

This update supports action=metadata via standard input for all fence agents.

All users of fence-agents are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.57. FENCE-VIRT

7.57.1. RHBA-2013:0419 — fence-virt bug fix and enhancement update

Updated fence-virt packages that fix two bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The fence-virt packages provide a fencing agent for virtual machines as well as a host agent, which processes fencing requests.

Bug Fixes

BZ#761228

Previously, the fence_virt man page contained incorrect information in the "SERIAL/VMCHANNEL PARAMETERS" section. With this update, the man page has been corrected.

BZ#853927

Previously, the fence_virtd daemon returned an incorrect error code to the fence_virt agent when the virt domain did not exist. Consequently, the fence_node utility occasionally failed to detect fencing. With this update, the error codes have been changed and the described error no longer occurs.

Enhancements

BZ#823542

The "delay" (-w) option has been added to the fence_virt and fence_xvm fencing agents. The delay option can be used, for example, as a method of preloading a winner in a fence race in a CMAN cluster.

BZ#843104

With this update, the documentation of the "hash" parameter in the fence_virt.conf file has been improved to notify that hash is the weakest hashing algorithm allowed for client requests.

All users of fence-virt are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.58. FILE

7.58.1. RHBA-2012:1339 — file bug fix update

Updated file packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

The "file" command is used to identify a particular file according to the type of data contained in the file. The command can identify various file types, including ELF binaries, system libraries, RPM packages, and different graphics formats.

Bug Fixes

BZ#795425

The file utility did not contain a "magic" pattern for detecting QED images and was therefore not able to detect such images. A new "magic" pattern for detecting QED images has been added, and the file utility now detects these images as expected.

BZ#795761

The file utility did not contain a "magic" pattern for detecting VDI images and was therefore not able to detect such images. A new "magic" pattern for detecting VDI images has been added, and the file utility now detects these images as expected.

BZ#797784

Previously, the file utility did not attempt to load "magic" patterns from the ~/.magic.mgc file, which caused "magic" patterns stored in this file to be unusable. This update modifies the file utility so it now attempts to load the ~/.magic.mgc file. The file is loaded if it exists and "magic" patterns defined in this file work as expected.

BZ#801711

Previously, the file utility used read timeout when decompressing files using the "-z" option. As a consequence, the utility was not able to detect files compressed by the bzip2 tool. The underlying source code has been modified so that file no longer uses read timeout when decompressing compressed files. Compressed files are now detected as expected when using the "-z" option.

BZ#859834

Previously, the file utility contained multiple "magic" patterns to detect output of the "dump" backup tool. On big-endian architectures, the less detailed "magic" pattern was used and output of the file utility was inconsistent. The less detailed "magic" pattern has been removed, and only one, more detailed, "magic" pattern to detect "dump" output is used now.

All users of file are advised to upgrade to these updated packages, which fix these bugs.

7.59. FIRSTBOOT

7.59.1. RHEA-2013:0488 — firstboot enhancement update

Updated firstboot packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The firstboot utility runs after installation and guides the user through a series of steps that allows for easier configuration of the machine.

Enhancement

BZ#831818

Previously, the Firstboot utility allowed displaying only the English version of the End User Licence

Agreement (EULA), which could be problematic for users who do not understand English. This update modifies Firstboot so that it uses the $LANG environment variable to find the localized EULA file according to the language set during installation. If the EULA file in the selected language is not found, the default EULA file, which is in English, is used. Users can now read the EULA document in the language chosen during installation before accepting it.

All users of firstboot are advised to upgrade to these updated packages, which add this enhancement.

7.60. FTP

7.60.1. RHBA-2012:1192 — ftp bug fix update

Updated ftp packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The ftp package provides the standard UNIX command line File Transfer Protocol (FTP) client. FTP is a widely used protocol for transferring files over the Internet, and for archiving files.

Bug Fix

BZ#783868

Prior to this update, using the ftp command "put" when the stack size was set to unlimited caused the sysconf(_SC_ARG_MAX) function to return -1, which in turn resulted in the malloc() function being called with an argument of 0 and causing an "Out of memory" message to be displayed. With this update, the underlying source code has been improved to allocate a reasonable minimum of memory. As a result, the "Out of memory" message no longer appears if the stack size was previously set to unlimited.

All users of ftp are advised to upgrade to these updated packages, which fix this bug.

7.60.2. RHBA-2012:1444 — ftp bug fix update

Updated ftp packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The ftp packages provide the standard UNIX command line File Transfer Protocol (FTP) client. FTP is a widely used protocol for transferring files over the Internet, and for archiving files.

Bug Fixes

BZ#869858

Prior to this update, the ftp client could encounter a buffer overflow and aborted if a macro longer than 200 characters was defined and then used after a connection. This update modifies the underlying code and the buffer that holds memory for the macro name was extended. Now, ftp matches the length of the command line limit and the ftp client no longer aborts when a macro with a long name is executed.

All users of ftp are advised to upgrade to these updated packages, which fix this bug.

7.60.3. RHBA-2012:1354 — ftp bug fix update

Updated ftp packages that fix four bugs are now available for Red Hat Enterprise Linux 6.

The ftp packages provide the standard UNIX command line File Transfer Protocol (FTP) client. FTP is a widely used protocol for transferring files over the Internet, and for archiving files.

Bug Fixes

BZ#665337

Previously, the command line width in the ftp client was limited to 200 characters. With this update, the maximum possible length of the FTP command line is extended to 4296 characters.

BZ#786004

Prior to this update, "append", "put", and "send" commands were causing system memory to leak. The memory holding the ftp command was not freed appropriately. With this update, the underlying source code has been improved to correctly free the system resources and the memory leaks are no longer present.

BZ#849940

Previously, the ftp client could not be invoked to run directly in the active mode. This functionality has been added to the source code and documented in the manual page. The client can now be executed with an additional "-A" command line parameter and will run in the active mode.

BZ#852636

Previously, the ftp client hung up when the ftp-data port (20) was not available (e.g. was blocked). The client then had to be terminated manually. Additional logic has been added to the source code. With this update, ftp has an internal timeout set to 30 seconds. If there is no answer from the server when this time has passed, ftp will now gracefully time out and not hang up.

All users of ftp are advised to upgrade to these updated packages, which fix these bugs.

7.61. GAWK

7.61.1. RHBA-2012:1146 — gawk bug fix update

Updated gawk packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The gawk packages provide the GNU version of the text processing utility awk. Awk interprets a special-purpose programming language to do quick and easy text pattern matching and reformatting jobs.

Bug Fix

BZ#829558

Prior to this update, the "re_string_skip_chars" function incorrectly used the character count instead of the raw length to estimate the string length. As a consequence, any text in multi-byte encoding that did not use the UTF-8 format failed to be processed correctly. This update modifies the underlying code so that the correct string length is used. multi-byte encoding is processed correctly.

All users of gawk requiring multi-byte encodings that do not use UTF-8 are advised to upgrade to these updated packages, which fix this bug.

7.62. GCC

7.62.1. RHBA-2013:0420 — gcc bug fix update

Updated gcc packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The gcc packages provide compilers for C, C++, Java, Fortran, Objective C, and Ada 95 GNU, as well as related support libraries.

Bug Fixes

BZ#801144

Due to the incorrect size of a pointer in GCC GNAT code, GNAT used an incorrect function of the libgcc library when compiling 32-bit Ada binaries on PowerPC architecture. Consequently, these programs could not be linked and the compilation failed. This update fixes the problem so that the sizeof operator now returns the correct size of a pointer, and the appropriate function from libgcc is called. GNAT compiles Ada binaries as expected in this scenario.

BZ#808590

The Standard Template Library (STL) contained an incomplete move semantics implementation, which could cause GCC to generate incorrect code. The incorrect headers have been fixed so that GCC now produce the expected code when depending on move semantics.

BZ#819100

GCC did not, under certain circumstances, handle generating a CPU instruction sequence that would be independent of indexed addressing on PowerPC architecture. As a consequence, an internal compiler error occurred if the "__builtin_bswap64" built-in function was called with the "-mcpu=power6" option. This update corrects the relevant code so that GCC now generates an alternate instruction sequence that does not depend on indexed addressing in this scenario.

BZ#821901

A bug in converting the exception handling region could cause an internal compiler error to occur when compiling profile data with the "-fprofile-use" and "-freorder-basic-blocks-and-partition" options. This update fixes the erroneous code and the compilation of profile data now proceeds as expected in this scenario.

BZ#826882

Previously, GCC did not properly handle certain situations when an enumeration was type cast using the static_cast operator. Consequently, an enumeration item could have been assigned an integer value greater than the highest value of the enumeration's range. If the compiled code contained testing conditions using such enumerations, those checks were incorrectly removed from the code during code optimization. With this update, GCC was modified to handle enumeration type casting properly and C++ now no longer removes the mentioned checks.

BZ#831832

Previously, when comparing the trees equality, the members of a union or structure were not handled properly in the C++ compiler. This led to an internal compiler error. This update modifies GCC so that unions and structures are now handled correctly and code that uses tree equality comparing is now compiled successfully.

BZ#867878

GCC previously processed the "srak" instructions without the z196 flag, which enables a compiler to work with these instructions. Consequently, some binaries, such as Firefox, could not be compiled on IBM System z and IBM S/390 architectures. With this update, GCC has been modified to support the z196 flag for the srak instructions, and binaries requiring these instructions can now be compiled successfully on IBM System z and IBM S/390 architectures.

All users of gcc are advised to upgrade to these updated packages, which fix these bugs.

7.63. GDB

7.63.1. RHSA-2013:0522 — Moderate: gdb security and bug fix update

Updated gdb packages that fix one security issue and three bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The GNU Debugger (GDB) allows debugging of programs written in C, C++, Java, and other languages by executing them in a controlled fashion and then printing out their data.

Security Fix

CVE-2011-4355

GDB tried to auto-load certain files (such as GDB scripts, Python scripts, and a thread debugging library) from the current working directory when debugging programs. This could result in the execution of arbitrary code with the user's privileges when GDB was run in a directory that has untrusted content.

NOTE

With this update, GDB no longer auto-loads files from the current directory and only trusts certain system directories by default. The list of trusted directories can be viewed and modified using the "show auto-load safe-path" and "set auto-load safe-path" GDB commands. Refer to the GDB manual for further information:

http://sourceware.org/gdb/current/onlinedocs/gdb/Auto_002dloading-safe-path.html#Auto_002dloading-safe-path

http://sourceware.org/gdb/current/onlinedocs/gdb/Auto_002dloading.html#Auto_002dloading

Bug Fixes

BZ#795424

When a struct member was at an offset greater than 256 MB, the resulting bit position within the struct overflowed and caused an invalid memory access by GDB. With this update, the code has been modified to ensure that GDB can access such positions.

BZ#811648

When a thread list of the core file became corrupted, GDB did not print this list but displayed the "Cannot find new threads: generic error" error message instead. With this update, GDB has been modified and it now prints the thread list of the core file as expected.

BZ#836966

GDB did not properly handle debugging of multiple binaries with the same build ID. This update modifies GDB to use symbolic links created for particular binaries so that debugging of binaries that share a build ID now proceeds as expected. Debugging of live programs and core files is now more user-friendly.

All users of gdb are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

7.63.2. RHBA-2013:0811 — gdb bug fix update

Updated gdb packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The GNU Debugger (GDB) allows debugging of programs written in C, C++, Java, and other languages by executing them in a controlled fashion and then printing out their data.

Bug Fixes

BZ#952090

When users tried to execute the "maintenance set python print-stack" command, gdb did not recognize it and issued an error stating the command was undefined. With this update, gdb now correctly recognizes and executes the command.

BZ#952100

When debugging a C++ program which declared a local static variable inside a class, gdb was unable to locate the local static variable. This caused problems when debugging some issues that required examining these kinds of variables. With this update, gdb now correctly identifies that the variable exists, and the debugging process functions normally.

BZ#954300

Previously, users experienced an internal error in the debugger when using a Thread Local Storage (TLS) modifier in a static variable declared inside a class on a C++ program, and asking gdb to print its value. This caused the debugging session to be compromised. With this update, gdb is now able to correctly deal with a static variable declared as a TLS inside a class and errors no longer occur in the described scenario.

Users of gdb are advised to upgrade to these updated packages, which fix these bugs.

7.64. GDM

7.64.1. RHBA-2013:0381 — gdm bug fix and enhancement update

Updated gdm packages that fix four bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The gdm packages provide the GNOME Display Manager (GDM), which implements the graphical login screen, shown shortly after boot up, log out, and when user-switching.

Bug Fixes

BZ#616755

Previously, the gdm_smartcard_extension_is_visible() function returned "TRUE" instead of the "ret" variable. Consequently, the smartcard login could not be disabled in the system-config-authentication window if the pcsd package was installed. With this update, gdm_smartcard_extension_is_visible() has been modified to return the correct value. As a result, the described error no longer occurs.

BZ#704245

When GDM was used to connect to a host via XDMCP (X Display Manager Control Protocol), another connection to a remote system using the "ssh -X" command resulted in failed authentication with the X server. Consequently, applications such as xterm could not be displayed on a remote system. This update provides a compatible MIT-MAGIC-COOKIE-1 key in the described scenario, thus fixing this incompatibility.

BZ#738462

Previously, X server audit messages were not included by default in the X server log. Now, those messages are unconditionally included in the log. Also, with this update, verbose messages are added to the X server log if debugging is enabled in the /etc/gdm/custom.conf file by setting "Enable=true" in the "debug" section.

BZ#820058

Previously, after booting the system, the following message occurred in the /var/log/gdm/:0-greeter.log file:

```
gdm-simple-greeter[PID]: Gtk-WARNING: gtkwidget.c:5460: widget not
within a GtkWindow
```

With this update, this warning is no longer displayed.

Enhancements

BZ#719647

With this update, GDM has been modified to allow smartcard authentication when the visible user list is disabled.

BZ#834303

Previously, the GDM debugging logs were stored in the /var/log/messages file. With this update, a separate /var/log/gdm/daemon.log file has been established for these debugging logs.

All users of gdm are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.65. GD

7.65.1. RHBA-2012:1274 — gd bug fix update

Updated gd packages that fix one bug is now available for Red Hat Enterprise Linux 6.

The gd packages provide the gd graphics library. GD allows code to draw images as PNG or JPEG files.

BZ#790400

Prior to this update, ,the gd graphics library handled inverted Y coordinates incorrectly, when changing the thickness of a line. As a consequence, lines with changed thickness were drawn incorrectly. This update modifies the underlying code to draw lines with changed thickness correctly.

All users of gd are advised to upgrade to these updated packages, which fix this bug.

7.66. GERONIMO-SPECS

7.66.1. RHBA-2012:1397 — geronimo-specs bug fix update

Updated geronimo-specs packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The geronimo-specs packages provide the specifications for Apache's ASF-licenced J2EE server Geronimo.

Bug Fix

BZ#818755

Prior to this update, the geronimo-specs-compat package description contained inaccurate references. This update removes these references so that the description is now accurate.

All users of geronimo-specs are advised to upgrade to these updated packages, which fix this bug.

7.67. GLIBC

7.67.1. RHBA-2013:0279 — glibc bug fix update

Updated glibc packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

The glibc packages provide the standard C and standard math libraries, which are used by multiple programs on the system. These libraries are required for the Linux system to function correctly.

Bug Fixes

BZ#804686

Prior to this update, a logic error caused the DNS code of **glibc** to incorrectly handle rejected responses from DNS servers. As a consequence, additional servers in the **`/etc/resolv.conf`** file could not be searched after one server responded with a REJECT. This update modifies the logic in the DNS. Now, **glibc** cycles through the servers listed in **`/etc/resolv.conf`** even if one returns a REJECT response.

BZ#806404

Prior to this update, the **`nss/getnssent.c`** file contained an unchecked malloc call and an incorrect loop test. As a consequence, **glibc** could abort unexpectedly. This update modifies the malloc call and the loop test.

BZ#809726

Prior to this update, locale data for the characters in the range a-z were incorrect in the Finnish locale. As a consequence, some characters in the range a-z failed to print correctly in the Finnish locale. This update modifies the underlying code to provide the correct output for these characters. Now, characters in the Finnish locale print as expected.

BZ#823909

If a file or a string was in the IBM-930 encoding, and contained the invalid multibyte character "0xffff", attempting to use **`iconv()`** (or the **`iconv`** command) to convert that file or string to another encoding, such as UTF-8, resulted in a segmentation fault. Now, the conversion code for the IBM-930 encoding recognizes this invalid character and calls an error handler, rather than causing a segmentation fault.

BZ#826149

Prior to this update, the **`fnmatch()`** function failed with the return value -1 when the wildcard character "*" was part of the pattern argument and the **`file name argument`** contained an invalid multibyte encoding. This update modifies the **`fnmatch()`** code to recognize this case. Now, the invalid characters are treated as not matching and then the process proceeds.

BZ#827362

Prior to this update, the internal **`FILE`** offset was set incorrectly in wide character streams. As a consequence, the offset returned by **`ftell`** was incorrect. In some cases, this could result in over-writing data. This update modifies the **`ftell`** code to correctly set the internal **`FILE`** offset field for wide characters. Now, **`ftell`** and **`fseek`** handle the offset as expected.

BZ#829222

Prior to this update, the **`/etc/rpc`** file was not set as a configuration file in the glibc build. As a consequence, updating glibc caused the **`/etc/rpc`** file to be replaced without warning or creating a backup copy. This update correctly marks **`/etc/rpc`** as a configuration file. Now, the existing **`/etc/rpc`** file is left in place, and the bundled version can be installed in **`/etc/rpc.rpmnew`**.

BZ#830127

Prior to this update, the **`vfprintf`** command returned the wrong error codes when encountering an overflow. As a consequence, applications which checked return codes from **`vfprintf`** could get unexpected values. This update modifies the error codes for overflow situations.

BZ#832516

Prior to this update, the **`newlocale`** flag relied entirely on failure of an underlying open() call to set the errno variable for an incorrect locale name. As a consequence, the **`newlocale()`** function did not set the **`errno`** variable to an appropriate value when failing, if it has already been asked about the same incorrect locale name. This update modifies the logic in the **`loadlocale`** call so that subsequent attempts to load a non-existent locale more than once always set the **`errno`** variable appropriately.

BZ#832694

Prior to this update, the ESTALE error message referred only to **`NFS`** file systems. As a consequence, users were confused when non-**`NFS`** file systems triggered this error. This update modifies the error message to apply the error message to all file systems that can trigger this error.

BZ#835090

Prior to this update, an internal array of name servers was only partially initialized when the **`/etc/resolv.conf`** file contained **IPV6** name servers. As a consequence, applications could, depending on the exact contents of a nearby structure, abort. This update modifies the underlying code to handle IPV6 name servers listed in **`/etc/resolv.conf`**.

BZ#837695

Prior to this update, a buffer in the resolver code for **glibc** was too small to handle results for certain DNS queries. As a consequence, the query had to be repeated after a larger buffer was allocated and wasted time and network bandwidth. This update enlarges the buffer to handle the larger DNS results.

BZ#837918

Prior to this update, the logic for the functions `exp`, `exp2`, `pow`, `sin`, `tan`, and `rint` was erroneous. As a consequence, these functions could fail when running them in the non-default rounding mode. With this update, the functions return correct results across all 4 different rounding modes.

BZ#841787

Prior to this update, **glibc** incorrectly handled the `options rotate` option in the `/etc/resolv.conf` file if this file also contained one or more IPv6 name servers. As a consequence, DNS queries could unexpectedly fail, particularly when multiple queries were issued by a single process. This update modifies the internalization of the listed servers from `/etc/resolv.conf` into internal structures of **glibc**, as well as the sorting and rotation of those structures to implement the `options rotate` capability. Now, DNS names are resolved correctly in **glibc**.

BZ#846342

Prior to this update, certain user-defined 32 bit executables could issue calls to the `memcpy()` function with overlapping arguments. As a consequence, the applications invoked undefined behavior and could fail. With this update, users with 32 bit applications which issue the `memcpy` function with overlapping arguments can create the `/etc/sysconfig/32bit_ssse3_memcpy_via_32bit_ssse3_memmove`. If this file exists, **glibc** redirects all calls to the **SSSE3 memcpy** copiers to the **SSSE3 memmove** copier, which is tolerant of overlapping arguments.

IMPORTANT

We strongly encourage customers to identify and fix these problems in their source code. Overlapping arguments to `memcpy()` is a clear violation of the ANSI/ISO standards and Red Hat does not provide binary compatibility for applications which violate these standards.

BZ#847932

Prior to this update, the `strtod()`, `strtof()`, and `strtold()` functions to convert a string to a numeric representation in **glibc** contained multiple integer overflow flaws. This caused stack-based buffer overflows. As a consequence, these functions could cause an application to abort or, under certain circumstances, execute arbitrary code. This update modifies the underlying code to avoid these faults.

BZ#848082

Prior to this update, the `setlocale()` function failed to detect memory allocation problems. As a consequence, the `setlocale()` function eventually core dumped, due to NULL pointers or uninitialized strings. This update modifies the `setlocale` code to insure that memory allocation succeeded. Now, the `setlocale()` function no longer core dumps.

BZ#849651

Prior to this update, the **expf()** function was considerably slowed down when saving and restoring the FPU state. This update adds a hand optimized assembler implementation of the **expf()** function for Intel 64 and AMD64 platforms. Now, the **expf()** function is considerably faster.

BZ#852445

Prior to this update, the PowerPC specific **pthread_once** code did not correctly publish changes it made. As a consequence, the changes were not visible to other threads at the right time. This update adds release barriers to the appropriate thread code to ensure correct synchronization of data between multiple threads.

BZ#861167

This update adds the **MADV_DONTDUMP** and **MADV_DODUMP** macros to the **mman.h** file to compile code that uses these macros.

BZ#863453

Prior to this update, the **nscd** daemon attempted to free a pointer that was not provided by the **malloc()** function, due to an error in the memory management in glibc. As a consequence, **nscd** could terminate unexpectedly, when handling groups with a large number of members. This update ensures that memory allocated by the pool allocator is no longer passed to **free**. Now, the pool allocator's garbage collector reclaims the memory. As a result, **nscd** no longer crashes on groups with a large number of members.

BZ#864322

Prior to this update, the **IPTOS_CLASS** definition referenced the wrong object. As a consequence, applications that referenced the **IPTOS_CLASS** definition from the **ip.h** file did not build or failed to operate as expected. This update modifies the definition to reference the right object and applications that reference to the **IPTOS_CLASS** definition.

Users of glibc are advised to upgrade to these updated packages, which fix these bugs ...

7.67.2. RHBA-2013:1179 — glibc bug fix update

Updated glibc packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The glibc packages provide the standard C libraries (libc), POSIX thread libraries (libpthread), standard math libraries (libm), and the Name Server Caching Daemon (nscd) used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

Bug Fix

BZ#989558

The C library security framework was unable to handle dynamically loaded character conversion routines when loaded at specific virtual addresses. This resulted in an unexpected termination with a segmentation fault when trying to use the dynamically loaded character conversion routine. This update enhances the C library security framework to handle dynamically loaded character conversion routines at any virtual memory address, and crashes no longer occur in the described scenario.

Users of glibc are advised to upgrade to these updated packages, which fix this bug.

7.67.3. RHBA-2013:1046 — glibc bug fix update

Updated glibc packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The glibc packages provide the standard C and standard math libraries used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

Bug Fixes

BZ#964044

A fix to prevent logic errors in various mathematical functions, including exp, exp2, expf, exp2f, pow, sin, tan, and rint, caused by inconsistent results when the functions were used with the non-default rounding mode, creates performance regressions for certain inputs. The performance regressions have been analyzed and the core routines have been optimized to bring performance back to reasonable levels.

BZ#970992

A program that opens and uses dynamic libraries which use thread-local storage variables may terminate unexpectedly with a segmentation fault when it is being audited by a module that also uses thread-local storage. This update modifies the dynamic linker to detect such a condition, and crashes no longer occur in the described scenario.

Users of glibc are advised to upgrade to these updated packages, which fix these bugs.

7.67.4. RHBA-2013:1421 — glibc bug fix update

Updated glibc packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The glibc packages provide the standard C libraries (libc), POSIX thread libraries (libpthread), standard math libraries (libm), and the name service cache daemon (nscd) used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

Bug Fix

BZ#1001050

A defect in the name service cache daemon (nscd) caused cached DNS queries, under certain conditions, to return only IPv4 addresses when querying for an address using the AF_UNSPEC address family, even though IPv4 and IPv6 results existed. The defect has been corrected and nscd correctly returns both IPv4 and IPv6 results if they both exist.

Users of glibc are advised to upgrade to these updated packages, which fix this bug.

7.68. GNOME-DESKTOP

7.68.1. RHBA-2012:1352 — gnome-desktop bug fix update

Updated gnome-desktop packages that fix a bug are now available.

The gnome-desktop package contains an internal library (libgnome-desktop) used to implement some portions of the GNOME desktop, and also some data files and other shared components of the GNOME user environment.

Bug Fix

BZ#829891

Previously, when a user hit the system's hot-key (most commonly Fn+F7) to change display configurations, the system could potentially switch to an invalid mode, which would fail to display. With this update, gnome-desktop now selects valid XRandR modes and correctly switching displays with the hot-key works as expected.

All users of gnome-desktop are advised to upgrade to these updated packages, which fix this bug.

7.69. GNOME-PACKAGEKIT

7.69.1. RHBA-2013:0280 — gnome-packagekit bug fix update

An updated gnome-packagekit package that fixes four bugs is now available.

gnome-packagekit provides session applications for the PackageKit API.

Bug Fixes

BZ#744980

If a package adds or removes a .repo file while updates are being installed, PackageKit (packagekitd) sends a RepoListChanged() message. If Software Update (/usr/bin/gpk-update-viewer) was being used to install these updates it responded to the message by attempting to refresh the available updates list. This resulted in said list going blank. As of this update, gpk-update-viewer ignores such signals from packagekitd, leaving the available updates list visible and unchanged.

BZ#744906

When a 64-bit Red Hat Enterprise Linux instance had both 32-bit and 64-bit versions of a package installed, and an update for both packages was available and presented in the Software Update (/usr/bin/gpk-update-viewer) window, the summary and package name appeared for both architectures. Package size and the errata note only presented for the 32-bit version, however. For the 64-bit version, the size column remained blank. And, when the 64-bit version was selected in Software list, the display pane below presented a ‘Loading...’ message rather than the errata note. With this update, gpk-update-viewer seeks out the exact package ID before falling back to the package name, ensuring both package versions are found and associated meta-data displayed when more than one package architecture is installed.

BZ#694793

When an application is installed using the Add/Remove Software interface (/usr/bin/gpk-application), a dialogue box appears immediately post-install offering a Run button. Clicking this button launches the newly-installed program. Previously, under some circumstances, an improperly assigned pointer value meant clicking this Run button caused gpk-application to crash (segfault). With this update, the pointer is correctly assigned and gpk-application no longer crashes when launching a newly-installed application.

BZ#669798

Previously, it was possible for an ordinary user to shutdown their system or log-out from a session while the PackageKit update tool was running. Depending on the transaction PackageKit was engaged in when the shutdown or logout was initiated, this could damage the RPM database and, consequently, damage the system. With this update, when ordinary users attempting to shutdown or log out while PackageKit is running an update, PackageKit inhibits the process and presents the user with an alert:

```
A transaction that cannot be interrupted is running.
```

Note: this update does not prevent a root user (or other user with equivalent administrative privileges) from shutting the system down or logging an ordinary user out of their session.

All PackageKit users should install this update which resolves these issues.

7.70. GNOME-SCREENSAVER

7.70.1. RHBA-2013:0390 — gnome-screensaver bug fix update

Updated gnome-screensaver packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The gnome-screensaver packages contain the GNOME project's official screen saver program. The screen saver is designed for improved integration with the GNOME desktop, including themeability, language support, and Human Interface Guidelines (HIG) compliance. It also provides screen-locking and fast user-switching from a locked screen.

Bug Fixes

BZ#648869

Previously, NVIDIA hardware did not support the X Resize and Rotate Extension (xRandR) gamma changes. Consequently, the fade-out function did not work on the NVIDIA hardware. With this update, xRandR gamma support detection code fails on NVIDIA cards, and the XF86VM gamma fade extension is automatically used as a fallback so the fade-out function works as expected.

BZ#744763

Previously, the mouse cursor could be moved to a non-primary monitor so the unlock dialog box did not appear when the user moved the mouse. This bug has been fixed and the mouse cursor can no longer be moved to a non-primary monitor. As a result, the unlock dialog box comes up anytime the user moves the mouse.

BZ#752230

Previously, the shake animation of the unlock dialog box could appear to be very slow. This was because the background was updated every time the window's size allocation changed, and the widget's size allocation consequently changed every frame of the shake animation. The underlying source code has been modified to ensure a reasonable speed of the shake animation.

BZ#759395

When a Mandatory profile was enabled, the "Lock screen when screen saver is active" option in the Screensaver Preferences window was not disabled. This bug could expose the users to a security risk. With this update, the lock-screen option is disabled as expected in the described scenario.

BZ#824752

When using dual screens, moving the mouse did not unlock gnome-screensaver after the initial timeout. The users had to press a key to unlock the screen. The underlying source code has been modified and the user can now unlock gnome-screensaver by moving the mouse.

All users of gnome-screensaver are advised to upgrade to these updated packages, which fix these bugs.

7.70.2. RHBA-2013:1178 — gnome-screensaver bug fix update

Updated gnome-screensaver packages that fix one bug are now available for Red Hat Enterprise Linux 6..

The gnome-screensaver packages contain the GNOME project's official screen saver program. It is designed for improved integration with the GNOME desktop, including themeability, language support, and Human Interface Guidelines (HIG) compliance. It also provides screen-locking and fast user-switching from a locked screen.

Bug Fix

BZ#994868

Previously, when using virt-manager, virt-viewer, and spice-xpi applications, users were unable to enter the gnome-screensaver password after the screen saver started. This happened only when the VM system used the Compiz composting window manager. After users released the mouse cursor, then pressed a key to enter a password, the dialog did not accept any input. This happened due to incorrect assignment of window focus to applications that did not drop their keyboard grab. With this update, window focus is now properly assigned to the correct place, and attempts to enter the gnome-screensaver password no longer fail in the described scenario.

Users of gnome-screensaver are advised to upgrade to these updated packages, which fix this bug.

7.71. GNOME-SETTINGS-DAEMON

7.71.1. RHBA-2013:0312 — gnome-settings-daemon bug fix and enhancement update

Updated gnome-settings-daemon packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The gnome-settings-daemon packages contain a daemon to share settings from GNOME with other applications. It also handles global key bindings, as well as a number of desktop-wide settings.

Bug Fixes

BZ#805064

Previously, the LED indicators of some Wacom graphics tablets were not supported in the gnome-settings-daemon package. Consequently, the status LEDs on Wacom tablets would not accurately indicate the current control mode. With this update, LED support has been added to gnome-settings-daemon. As a result, the tablet LEDs now work as epected.

BZ#812363

Previously, using function keys without modifiers (F1, F2, and so on) as keyboard shortcuts for custom actions did not work. With this update, a patch has been added to fix this bug. As a result, gnome-settings-daemon now allows unmodified function keys to be used as keyboard shortcuts for custom actions.

BZ#824757

In certain cases, the gnome-settings-daemon did not properly handle the display configuration settings. Consequently, using the system's hot-key to change the display configuration either did not select a valid XRandR configuration or kept monitors in clone mode. This bug has been fixed and gnome-settings-daemon now selects valid XRandR modes and handles the clone mode as expected.

BZ#826128

Previously, connecting a screen tablet to a computer before activation of the tablet screen caused the input device to be matched with the only available monitor - the computer screen. Consequently, the stylus motions were incorrectly mapped to the computer screen instead of the tablet itself. With this update, a patch has been introduced to detect the tablet screen as soon as it becomes available. As a result, the device is correctly re-matched when the tablet screen is detected.

BZ#839328

Previously, using the shift key within a predefined keyboard shortcut mapped to the tablet's ExpressKey button caused gnome-settings-daemon to crash after pressing ExpressKey. This bug has been fixed, and the shortcuts which use the shift key can now be mapped to ExpressKey without complications.

BZ#853181

Prior to this update, the mouse plug-in in the gnome-settings-daemon package interfered with Wacom devices. Consequently, using ExpressKey on a tablet after hot-plugging generated mouse click events. With this update, the mouse plug-in has been fixed to ignore tablet devices and the interference no longer occurs.

BZ#886922

Previously, on tablets with multiple mode-switch buttons such as the Wacom Cintiq 24HD, all mode-switch buttons would cycle though the different modes. With this update, each different mode-switch button will select the right mode for the given button.

BZ#861890

Due to a bug in the gnome settings daemon, changing the monitor layout led to incorrect tablet mapping. With this update, the graphics tablet mapping is automatically updated when the monitor layout is changed. As a result, the stylus movements are correctly mapped after the layout change and no manual update is needed.

Enhancements

BZ#772728

With this update, several integration improvements for Wacom graphics tablets have been backported from upstream: - touchscreen devices are now automatically set in absolute mode instead of relative - memory leaks on tablet hot plug have been fixed - ExpressKeys no longer fail after the layout rotation - test applications are now included in the package to help with debugging issues.

BZ#858255

With this update, the touch feature of input devices has been enabled in the default settings of gnome-settings-daemon.

All users of gnome-settings-daemon are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.72. GNOME-TERMINAL

7.72.1. RHBA-2012:1311 — gnome-terminal bug fix update

Updated gnome-terminal packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Gnome-terminal is a terminal emulator for GNOME. It supports translucent backgrounds, opening multiple terminals in a single window (tabs) and clickable URLs.

Bug Fix

BZ#819796

Prior to this update, gnome-terminal was not completely localized into Asamese. With this update, the Assamese locale has been updated.

All gnome-terminal users are advised to upgrade to these updated packages, which fix this bug.

7.73. GNUTLS

7.73.1. RHBA-2013:0425 — gnutls bug fix update

Updated gnutls packages that fix four bugs are now available for Red Hat Enterprise Linux 6.

The gnutls packages provide the GNU Transport Layer Security (GnuTLS) library, which implements cryptographic algorithms and protocols such as SSL, TLS, and DTLS.

Bug Fixes

BZ#648297

Previously, the gnutls_priority_init.3 man page contained incorrect information on the gnutls-2.8.5-safe-renegotiation patch, particularly on special control keywords. The manual page has been updated to provide accurate information about the described subject.

BZ#745242

Prior to this update, the gnutls_x509_privkey_import() function failed to load private keys in the PKCS#8 format. Consequently, these keys were not processed by applications which use gnutls_x509_privkey_import(). This bug has been fixed, and gnutls_x509_privkey_import() now allows loading of private keys formatted in PKCS#8.

BZ#771378

Multiple bugs were present in the implementation of the TLS-1.2 protocol in the gnutls package. Consequently, gnutls was incompatible with clients and servers conforming to the TLS-1.2 protocol standard. With this update, the TLS-1.2 implementation has been fixed. As a result, the compatibility of gnutls with other TLS-1.2 clients and servers is now assured.

BZ#807746

Previously, the gnutls-cli-debug man page contained typographical errors and incorrect information on the command-line options. The manual page has been updated, and no longer contains the aforementioned errors.

All users of gnutls are advised to upgrade to these updated packages, which fix these bugs.

7.73.2. RHSA-2013:0883 — Important: gnutls security update

Updated gnutls packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The GnuTLS library provides support for cryptographic algorithms and for protocols such as Transport Layer Security (TLS).

Security Fix

CVE-2013-2116

It was discovered that the fix for the CVE-2013-1619 issue released via RHSA-2013:0588 introduced a regression in the way GnuTLS decrypted TLS/SSL encrypted records when CBC-mode cipher suites were used. A remote attacker could possibly use this flaw to crash a server or client application that uses GnuTLS.

Users of GnuTLS are advised to upgrade to these updated packages, which correct this issue. For the update to take effect, all applications linked to the GnuTLS library must be restarted.

7.74. GRAPHVIZ

7.74.1. RHBA-2012:1291 — graphviz bug fix update

Updated graphviz packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

Graphviz is open-source graph-visualization software. Graph visualization is a way of representing structural information as diagrams of abstract graphs and networks. It has important applications in networking, bioinformatics, software engineering, database and web design, machine learning, and in visual interfaces for other technical domains.

Bug Fixes

BZ#772637

Previously, the dot tool could generate different images on 32-bit and 64-bit architectures, which could consequently lead to multilib conflicts of packages that use graphviz during its build process. The problem was caused by different instructions used for floating points processing. On 32-bit Intel architecture, the code is now compiled with the "--ffloat-store" compiler flag, which ensures that identical images are generated regardless of the used architecture.

BZ#821920

The graphviz-tcl package included the "demo" directory, which contained examples in various languages. This caused implicit dependencies to be introduced. With this update, all examples are installed as documentation, which reduces the number of implicit dependencies.

BZ#849134

The "dot -c" command which is run in the %postun scriptlet recreates graphviz configuration files to be up-to-date with the current state of the installed plug-ins. Previously, if the command failed to load plug-ins specified in the configuration files, warning messages were printed when removing the graphviz-gd package. These messages could have been confusing, and have been therefore removed.

All users of graphviz are advised to upgrade to these updated packages, which fix these bugs.

7.75. GRUB

7.75.1. RHBA-2013:0428 — grub bug fix and enhancement update

Updated grub packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The GRUB utility is a powerful boot loader, which can load a wide variety of operating systems.

Bug Fixes

BZ#783169

When the BIOS was set to Unified Extensible Firmware Interface (UEFI) mode, all legacy option ROMs in the setup were disabled, and the grub.efi utility was loaded, an attempt to access the network with the NET0 protocol was not successful and the "nd" root command did not work. This bug has been fixed and GRUB works correctly in this situation.

BZ#814014

Previously, the GRUB utility did not scan for KVM virtio disks when creating a device map. Consequently, these disks were not added to this map. This bug has been fixed and GRUB now scans for vd* devices located in the /dev/ directory, so virtio disks are added to a device map as expected.

BZ#825054

The GRUB utility did not pass high order address bits for the Extensible Firmware Interface (EFI) memory map and system table high order bits. As a consequence, the EFI system map and memory map did not work correctly on computers with RAM bigger then 4 GB. This bug has been fixed by passing high order address bits, so that grub works properly in the described scenario.

BZ#870420

When symbolic links in the /dev/mapper/ directory were resolved to the original file, this file did not match proper file entry in the device.map file. Consequently, the grub-install package failed and an error message was returned. With this update, symbolic links are now prevented to resolve in the /dev/mapper/ directory. As a result, grub-install proceeds as expected.

BZ#876519

Due to an error in the underlying source code, an incorrect attempt to dereference a NULL pointer could previously cause GRUB to terminate unexpectedly. This update corrects the underlying source code to prevent this error so that GRUB no longer crashes.

Enhancements

BZ#642396

This enhancement includes support for IPV6 UEFI 2.3.1 netboot, which was previously missing.

BZ#737732

With this update, the users can use EFI boot partition as a root partition, which can be specified in the grub.conf file. As a consequence, the users do not have to specify particular drive, but can use the one specified in the EFI boot manager.

All users of GRUB are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.76. GSTREAMER-PLUGINS-BASE

7.76.1. RHEA-2012:1473 — gstreamer-plugins-base enhancement update

Updated gstreamer-plugins-base packages thatadd one enhancement are now available for Red Hat Enterprise Linux 6.

The gstreamer-plugins-base packages provide a collection of base plug-ins for the GStreamer streaming media framework.

Enhancement

BZ#755777

This update adds color-matrix support for color conversions to the ffmpegcolorspace plugin.

All users of gstreamer-plugins-base are advised to upgrade to these updated packages, which add this enhancement.

7.77. GTK2

7.77.1. RHBA-2013:0493 — gtk2 bug fix update

Updated gtk2 packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

GIMP Toolkit (GTK+) is a multi-platform toolkit for creating graphical user interfaces.

Bug Fixes

BZ#882346

Due to a recent change in the behavior of one of the X.Org Server components, GTK+ applications could not use certain key combinations for key bindings. This update makes GTK+ compatible with the new behavior, which ensures that no regressions occur in applications that use the library.

BZ#889172

Previously, when switching between the "Recently Used" and "Search" tabs in the “Open Files” dialog box, the "Size" column in the view disappeared. This update ensures the column is visible when the relevant option is selected.

Users of GTK+ are advised to upgrade to these updated packages, which fix these bugs.

7.78. GVFS

7.78.1. RHBA-2012:1124 — gvfs bug fix and enhancement update

Updated gvfs packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

GVFS is the GNOME desktop's virtual file system layer, which allows users to easily access local and remote data, including via the FTP, SFTP, WebDAV, CIFS and SMB protocols, among others. GVFS integrates with the GIO (GNOME I/O) abstraction layer.

Bug Fixes

BZ#599055

Previously, rules for ignoring mounts were too restrictive. If the user clicked on an encrypted volume in the Nautilus' sidebar, an error message was displayed and the volume could not be accessed. The underlying source code now contains additional checks so that encrypted volumes have proper mounts associated (if available), and the file system can be browsed as expected.

BZ#669526

Due to a bug in the kernel, a freshly formatted Blu-ray Disk Rewritable (BD-RE) medium contains a single track with invalid data that covers the whole medium. This empty track was previously incorrectly detected, causing the drive to be unusable for certain applications, such as Brasero. This update adds a workaround to detect the empty track, so that freshly formatted BD-RE media are properly recognized as blank.

BZ#682799, BZ#746977, BZ#746978, BZ#749369, BZ#749371, BZ#749372

The code of the gvfs-info, gvfs-open, gvfs-cat, gvfs-ls and gvfs-mount utilities contained hard-coded exit codes. This caused the utilities to always return zero on exit. The exit codes have been revised so that the mentioned gvfs utilities now return proper exit codes.

BZ#746905

When running gvfs-set-attribute with an invalid command-line argument specified, the utility terminated unexpectedly with a segmentation fault. The underlying source code has been modified so that the utility now prints a proper error message when an invalid argument is specified.

BZ#809708

Due to missing object cleanup calls, the gvfsd daemon could use excessive amount of memory, which caused the system to become unresponsive. Proper object cleanup calls have been added with this update, which ensures that the memory consumption is constant and the system does not hang in this scenario.

All users of gvfs are advised to upgrade to these updated packages, which fix these bugs.

7.79. HIVEX

7.79.1. RHBA-2013:0433 — hivex bug fix update

Updated hivex packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

Hivex is a library for extracting the contents of Windows Registry "hive" files, which is designed to be secure against corrupted or malicious registry files. Hive files are undocumented binary files.

Bug Fixes

BZ#822741

Previously, the description of the package contained inappropriate text. This update provides a correction of the language used and now, the spec file contains only neutral expressions.

BZ#841924

Certain hive files that had a very large number of child nodes under a single parent node could not be parsed. A patch has been added to allow read-only access to these child nodes.

Users of hivex are advised to upgrade to these updated packages, which fix these bugs.

7.80. HPLIP

7.80.1. RHSA-2013:0500 — Low: hplip security, bug fix and enhancement update

Updated hplip packages that fix several security issues, multiple bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The hplip packages contain the Hewlett-Packard Linux Imaging and Printing Project (HPLIP), which provides drivers for Hewlett-Packard printers and multi-function peripherals.

Security Fix

CVE-2013-0200, CVE-2011-2722

Several temporary file handling flaws were found in HPLIP. A local attacker could use these flaws to perform a symbolic link attack, overwriting arbitrary files accessible to a process using HPLIP.

The CVE-2013-0200 issues were discovered by Tim Waugh of Red Hat.

NOTE

The hplip packages have been upgraded to upstream version 3.12.4, which provides a number of bug fixes and enhancements over the previous version. (BZ#731900)

Bug Fixes

BZ#829453

Previously, the hpijs package required the obsolete cupsddk-drivers package, which was provided by the cups package. Under certain circumstances, this dependency caused hpijs installation to fail. This bug has been fixed and hpijs no longer requires cupsddk-drivers.

BZ#683007

The configuration of the Scanner Access Now Easy (SANE) back end is located in the /etc/sane.d/dll.d/ directory, however, the hp-check utility checked only the /etc/sane.d/dll.conf file. Consequently, hp-check checked for correct installation, but incorrectly reported a problem with the way the SANE back end was installed. With this update, hp-check properly checks for installation problems in both locations as expected.

All users of hplip are advised to upgrade to these updated packages, which fix these issues and add these enhancements.

7.80.2. RHSA-2013:1274 — Important: hplip security update

Updated hplip packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The hplip packages contain the Hewlett-Packard Linux Imaging and Printing Project (HPLIP), which provides drivers for Hewlett-Packard printers and multi-function peripherals.

Security Fix

CVE-2013-4325

HPLIP communicated with PolicyKit for authorization via a D-Bus API that is vulnerable to a race condition. This could lead to intended PolicyKit authorizations being bypassed. This update modifies HPLIP to communicate with PolicyKit via a different API that is not vulnerable to the race condition.

All users of hplip are advised to upgrade to these updated packages, which contain a backported patch to correct this issue.

7.81. HSQLDB

7.81.1. RHBA-2013:0334 — hsqldb bug fix update

Updated hsqldb packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The hsqldb packages provide a relational database management system written in Java. The Hyper Structured Query Language Database (HSQLDB) contains a JDBC driver to support a subset of ANSI-92 SQL.

Bug Fix

BZ#827343

Prior to this update, the hsqldb database did not depend on java packages of version 1:1.6.0 or later. As a consequence, the build-classpath command failed on systems without the java-1.6.0-openjdk package installed and the hsqldb packages could be installed incorrectly. This update adds a requirement for java-1.6.0-openjdk. Now, the installation of hsqldb proceeds correctly as expected.

All users of hsqldb are advised to upgrade to these updated packages, which fix this bug.

7.82. HTTPD

7.82.1. RHSA-2013:0512 — Low: httpd security, bug fix and enhancement update

Updated httpd packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The httpd packages contain the Apache HTTP Server (httpd), which is the namesake project of The Apache Software Foundation.

Security Fixes

CVE-2008-0455, CVE-2012-2687

An input sanitization flaw was found in the mod_negotiation Apache HTTP Server module. A remote attacker able to upload or create files with arbitrary names in a directory that has the MultiViews options enabled, could use this flaw to conduct cross-site scripting attacks against users visiting the site.

CVE-2012-4557

It was discovered that mod_proxy_ajp, when used in configurations with mod_proxy in load balancer mode, would mark a back-end server as failed when request processing timed out, even when a previous AJP (Apache JServ Protocol) CPing request was responded to by the back-end. A remote attacker able to make a back-end use an excessive amount of time to process a request could cause mod_proxy to not send requests to back-end AJP servers for the retry timeout period or until all back-end servers were marked as failed.

Bug Fixes

BZ#787247

When the Apache module **mod_proxy** was configured, and a particular back-end URL was reverse proxied into the server two or more times, a spurious warning in the following format was given:

```
[warn] worker [URL] already used by another worker
```

The level of this message has been changed from WARNING to INFO as it is not incorrect to proxy more than one URL to the same back-end server.

BZ#822587

The **mod_cache** module did not handle **`206`** partial **`HTTP`** responses correctly. This resulted in incorrect responses being returned to clients if a cache was configured. With this update, **mod_cache** no longer caches **`206`** responses, thus ensuring correct responses are returned.

BZ#829689

If **`LDAP`** authentication was used with a Novell eDirectory LDAP server, **mod_ldap** could return **`500 Internal Server Error`** response if the LDAP server was temporarily unavailable. This update fixes **mod_ldap** to retry LDAP requests if the server is unavailable, and the **`500`** errors will not be returned in this case.

BZ#837086

Previously, **mod_proxy_connect** performed unnecessary **`DNS`** queries when ***`ProxyRemote`*** was configured. Consequently, in configurations with ***`ProxyRemote`***, **mod_proxy_connect** could either fail to connect, or be slow to connect to the remote server. This update changes **mod_proxy** to omit DNS queries if ***`ProxyRemote`*** is configured. As a result, the proxy no longer fails in such configurations.

BZ#837613

When an **`SSL`** request failed and the **`-v 2`** option was used, the *ApacheBench* (ab) benchmarking tool tried to free a certificate twice. Consequently, ab terminated unexpectedly due to a double **`free()`** error. The ab tool has been fixed to free certificates only once. As a result, the ab tool no longer crashes in the scenario described.

BZ#848954

Previously, **mod_ssl** presumed the private key was set after the certificate in ***`SSLProxyMachineCertificateFile`***. Consequently, **httpd** terminated unexpectedly if the private key had been set before the certificate in SSLProxyMachineCertificateFile. This update improves **mod_ssl** to check if the private key is set before the certificate. As a result, **mod_ssl** no longer crashes in this situation and prints an error message instead.

BZ#853160

Prior to this update, **mod_proxy_ajp** did not correctly handle a **`flush`** message from a Java application server if received before the **`HTTP`** response headers had been sent. Consequently, users could receive a truncated response page without the correct HTTP headers. This update fixes **mod_proxy_ajp** to ignore **`flush`** messages before the HTTP response headers have been sent. As a result, truncated responses are no longer sent in scenario described.

BZ#853348

In a proxy configuration, certain response-line strings were not handled correctly. If a response-line without a **`description`** string was received from the origin server, for a non-standard status code, such as the **`450`** status code, a **`500 Internal Server Error`** would be returned to the client. This bug has been fixed so that the original response line is returned to the client.

BZ#867268

Previously, the value of **`${cookie}C`** in the ***`LogFormat`*** directive's definition matched substrings of cookie. Consequently, a bad cookie could be printed if its name contained a substring of the name defined in ***`LogFormat`*** using the **`${cookie}C`** string. With this update, the code is improved so that cookie names are now matched exactly. As a result, a proper cookie is returned even when there are other cookies with its substring in their name.

BZ#867745

Previously, no check was made to see if the **`/etc/pki/tls/private/localhost.key`** file was a valid key prior to running the **`%post`** script for the **mod_ssl** package. Consequently, when **`/etc/pki/tls/certs/localhost.crt`** did not exist and **`localhost.key`** was present but invalid, upgrading the Apache HTTP Server daemon (httpd) with **mod_ssl** failed. The **`%post`** script has been fixed to test for an existing **`SSL`** key. As a result, upgrading **httpd** with **mod_ssl** now proceeds as expected.

BZ#868253

Previously, in a reverse proxy configuration, **mod_cache** did not correctly handle a **`304 Not Modified`** response from the origin server when refreshing a cache entry. Consequently, in some cases an empty page was returned to a client requesting an entity which already existed in the cache.

This update fixes handling of `304 Not Modified` responses in **mod_cache** and as a result no empty pages will be displayed in the scenario described.

BZ#868283

Due to a regression, when **mod_cache** received a non-cacheable `304` response, the headers were served incorrectly. Consequently, compressed data could be returned to the client without the cached headers to indicate the data was compressed. An upstream patch has been applied to merge response and cached headers before data from the cache is served to the client. As a result, cached data is now correctly interpreted by the client.

Enhancements

BZ#748400

The Apache module **mod_proxy** now allows changing the **BalancerMember** state in the web interface.

BZ#757735

The **rotatelogs** program now provides a new `rotatelogs -p` option to execute a custom program after each log rotation.

BZ#757739

The **rotatelogs** program now provides a new `rotatelogs -c` option to create log files for each set interval, even if empty.

BZ#796958

The *`LDAPReferrals`* configuration directive has been added, as an alias for the existing *`LDAPChaseReferrals`* directive.

BZ#805720

The **mod_proxy** and **mod_ssl** modules have been updated to support the concurrent use of the **mod_nss** (NSS) and **mod_ssl** (OpenSSL) modules.

BZ#805810

An init script for the `htcacheclean` daemon has been added.

BZ#824571

The *`failonstatus`* parameter has been added for balancer configuration in **mod_proxy**.

BZ#828896

Previously, **mod_authnz_ldap** had the ability to set environment variables from received `LDAP` attributes, but only by LDAP authentication, not by LDAP authorization. Consequently, if the **mod_authnz_ldap** module was used to enable LDAP for authorization but not authentication, the `AUTHORIZE_` environment variables were not populated. This update applies a patch to implement setting of `AUTHORIZE_` environment variables using LDAP authorization. As a result, other methods of authentication can be used while using LDAP authorization for setting environment variables for all configured LDAP attributes.

BZ#833064

The **%posttrans** scriptlet which automatically restarts the **httpd** service after a package upgrade can now be disabled. If the file `/etc/sysconfig/httpd-disable-posttrans` exists, the scriptlet will not restart the daemon.

BZ#833092

The output of `httpd -S` now includes configured alias names for each virtual host.

BZ#838493

The **rotatelogs** program has been updated to support the `-L` option to create a hard link from the current log to a specified path.

BZ#842375

New certificate variable names are now exposed by **mod_ssl** using the `_DN_userID` suffix, such as `SSL_CLIENT_S_DN_userID`, which uses the commonly used object identifier (OID) definition of `userID`, OID 0.9.2342.19200300.100.1.1.

BZ#842376

Chunked Transfer Coding is described in *RFC 2616*. Previously, the Apache server did not correctly handle a chunked encoded POST request with a `chunk-size` or `chunk-extension` value of 32 bytes or more. Consequently, when such a POST request was made the server did not respond. An upstream patch has been applied and the problem no longer occurs.

Users of httpd are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.83. HWDATA

7.83.1. RHEA-2013:0376 — hwdata enhancement update

An updated hwdata package that adds various enhancements is now available for Red Hat Enterprise Linux 6.

The hwdata package contains tools for accessing and displaying hardware identification and configuration data.

Enhancements

BZ#839221

The PCI ID numbers have been updated for the Beta and the Final compose lists.

BZ#739816

Support for NVidia graphic card N14E-Q5, 0x11BC has been added.

BZ#739819

Support for NVidia graphic card N14E-Q3, 0x11BD has been added.

BZ#739821

Support for NVidia graphic card N14E-Q1, 0x11BE has been added.

BZ#739824

Support for NVidia graphic card N14P-Q3, 0x0FFB has been added.

BZ#739825

Support for NVidia graphic card N14P-Q1, 0x0FFC has been added.

BZ#760031

Support for Broadcom BCM943228HM4L 802.11a/b/g/n 2x2 Wi-Fi Adapter has been added.

BZ#830253

Support for Boot from Dell PowerEdge Express Flash PCIe SSD devices has been added.

BZ#841423

Support for the Intel C228 chipset and a future Intel processor based on Socket H3 has been added.

BZ#814114

This update also adds the current hardware USB IDs file from the upstream repository. This file provides support for Broadcom 20702 Bluetooth 4.0 Adapter Softsailing.

All users of hwdata are advised to upgrade to this updated package, which adds these enhancements.

7.84. HWLOC

7.84.1. RHBA-2013:0331 — hwloc bug fix and enhancement update

Updated hwloc packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The hwloc package provides Portable Hardware Locality, which is a portable abstraction of the hierarchical topology of current architectures.

NOTE

The hwloc packages have been upgraded to upstream version 1.5, which provides a number of bug fixes and enhancements over the previous version. (BZ#797576)

Users of hwloc are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.85. ICEDTEA-WEB

7.85.1. RHBA-2013:0491 — icedtea-web bug fix update

Updated icedtea-web packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The IcedTea-Web project provides a Java web browser plug-in and an implementation of Java Web Start, which is based on the Netx project. It also contains a configuration tool for managing deployment settings for the plug-in and Web Start implementations.

Bug Fix

BZ#838084

Previously, the IcedTea-Web plug-in was built against JDK 6, but in runtime it was possible to use it with JDK 7. Consequently, IcedTea-Web sometimes failed to run. With this update, the icedtea-web package is built against JDK 7 and IcedTea-Web is using JDK 7 in runtime, thus preventing this bug. Note that the end of public updates for JDK 6 is scheduled to go into effect in upcoming weeks.

Users of icedtea-web are advised to upgrade to these updated packages, which fix this bug.

7.85.2. RHBA-2013:0959 — icedtea-web bug fix update

Updated icedtea-web packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The IcedTea-Web project provides a Java web browser plug-in and an implementation of Java Web Start, which is based on the Netx project. It also contains a configuration tool for managing deployment settings for the plug-in and Web Start implementations.

Bug Fix

BZ#975426

A java-1.7.0-openjdk package change released via RHSA-2013:0957 caused the icedtea-web browser plug-in and the javaws application to exit with a NullPointerException. This update fixes icedtea-web to work correctly with the updated java-1.7.0-openjdk packages.

Users of icedtea-web are advised to upgrade to these updated packages, which fix this bug.

7.86. INFINIPATH-PSM

7.86.1. RHBA-2013:0536 — infinipath-psm bug fix update

Updated infinipath-psm packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The PSM Messaging API, or PSM API, is Intel's (formerly QLogic's) low-level, user-level communication interface for the Truescale family of products. PSM users can use mechanisms necessary to implement higher-level communication interfaces in parallel environments.

Bug Fix

BZ#907361

Due to a packaging error, not all object files required for the infinipath-psm library were built into the library, rendering it non-functional. This update fixes the infinipath-psm Makefile, which now properly includes all required object files, and the library works as expected.

All users of infinipath-psm are advised to upgrade to these updated packages, which fix this bug.

7.87. INITSCRIPTS

7.87.1. RHBA-2013:0518 — initscript bug fix and enhancement update

Updated iniscripts package that fixes several bugs and adds two enhancements are now available for Red Hat Enterprise Linux 6.

The initscripts package contains basic system scripts to boot the system, change runlevels, activate and deactivate most network interfaces, and shut the system down cleanly.

Bug Fixes

BZ#893395

Previously, an **ip link** command was called before the master device was properly set. Consequently, the slaves could be in the **unknown** state. This has been fixed by calling **ip link** for master after the device is installed properly, and all slaves are up. As a result, all slaves are in the expected state and connected to the master device.

BZ#714230

Previously, the naming policy for VLAN names was too strict. Consequently, the **ifdown** utility failed to work with descriptively-named interfaces. To fix this bug, the name format check has been removed and **ifdown** now works as expected.

BZ#879243

Prior to this update, there was a typographic error in the **/etc/sysconfig/network-scripts/ifup-aliases** file, which caused the duplicate check to fail. The typo has been corrected and the check works again.

BZ#885235

The **BONDING_OPTS** variable was applied by the **ifup** utility on a slave interface, even if the master was already on and had active slaves. This caused an error message to be returned by **ifup**. To address this bug, it is now checked whether the master does not have any active slaves before applying **BONDING_OPTS**, and no error messages are returned.

BZ#880684

Prior to this update, the **arping** utility, which checks for IP address duplicates in the network, failed when the parent device was not up. Consequently, the failure was handled the same way as finding of a second IP address in the network. To fix this bug, **ifup-aliases** files have been set to be checked whether the master device is up before the duplicity check is run. As a result, no error messages are returned when the parent device is down in the described scenario.

BZ#723936

The **rename_device.c** file did not correspond with VLAN interfaces, and thus could lead to improperly named physical interfaces. A patch has been provided to address this bug and interfaces are now named predictably and properly.

BZ#856209

When calling the **vgchange -a y** command instead of **vgchange -a ay** on the **netfs** interface by the **rc.sysinit** daemon, all volumes were activated. This update provides a patch to fix this bug. Now, only the volumes declared to be activated are actually activated. If the list is not declared, all volumes are activated by default.

BZ#820430

Previously, when a slave was attached to a master interface, which did not have a correct mode set, the interface did not work properly and could eventually cause a kernel oops. To fix this bug, the **BONDING_OPTS** variables are set before the master interface is brought up, which is the correct order of setting.

BZ#862788

If there was a process blocking a file system from unmounting, the **/etc/init.d/halt** script tried to kill all processes currently using the file system, including the script itself. Consequently, the system became unresponsive during reboot. With this update, shutdown script PIDs are excluded from the kill command, which enables the system to reboot normally.

BZ#874030

When the **ifup** utility was used to set up a master interface, the **BONDING_OPTS** variables were not applied. Consequently, bonding mode configuration done through the **ifcfg** utility had no effect. A patch has been provided to fix this bug. **BONDING_OPTS** are now applied and bonding mode works in the described scenario.

BZ#824175

If a network bond device had a name that was a substring of another bond device, both devices changed their states due to an incorrect test of the bond device name. A patch has been provided in the regular expression test and bond devices change their states as expected.

BZ#755699

The **udev** daemon is an event-driven hot-plug agent. Previously, an **udev** event for serial console availability was emitted only on boot. If runlevels were changed, the process was not restarted, because the event had already been processed. Consequently, the serial console was not restarted when entering and then exiting runlevel 1. With this update, the ***fedora.serial-console-available*** event is emitted on the post-stop of the serial console, and the console is now restarted as expected.

BZ#852005

Prior to this update, no check if an address had already been used was performed for alias interfaces. Consequently, an already used IP address could be assigned to an alias interface. To fix this bug, the IP address is checked whether it is already used. If it is, an error message is returned and the IP address is not assigned.

BZ#852176

Previously, the **init** utility tried to add a bond device even if it already existed. Consequently, a warning message was returned. A patch that checks whether a bond device already exists has been provided and warning messages are no longer returned.

BZ#846140

Prior to this update, the **crypttab(5)** manual page did not describe handling white spaces in passwords. Now, the manual page has been updated and contains information concerning a password with white spaces.

BZ#870025

Previous **crypttab (5)** manual page contained a typografic error (crypptab insted of crypttab), which has now been corrected.

BZ#795778

Previously, usage description was missing in the **/init/tty.conf** and **/init/serial.conf** files and this information was not returned in error messages. With this update, the information has been added to the aforementioned files and is now returned via an error message.

BZ#669700

Prior to this update, the **/dev/shm** file system was mounted by the **dracut** utility without attributes from the **/etc/fstab** file. To fix this bug, **/dev/shm** is now remounted by the **rc.sysinit** script. As a result, **/dev/shm** now contains the attributes from **/etc/fstab**.

BZ#713757

Previous version of the **sysconfig.txt** file instructed users to put the **VLAN=yes** option in the global configuration file. Consequently, interfaces with names containing a dot were recognized as VLAN interfaces. The **sysconfig.txt**file has been changed so that the VLAN describing line instructs users to include the VLAN option in the interface configuration file, and the aforementioned devices are no longer recognized as VLAN interfaces.

BZ#869075

The **sysconfig.txt** file advised users to use the **saslauthd -a** command instead of **saslauthd -v**, which caused the command to fail with an error message. In **sysconfig.txt**, the error in the command has been corrected and the **saslauthd** utility now returns expected results.

BZ#714250

When the **ifup** utility initiated VLAN interfaces, the **sysctl** values were not used. With this update, **ifup** rereads the **sysctl** values in the described scenario and VLAN interfaces are configured as expected.

Enhancements

BZ#851370

The **brctl** daemon is used to connect two Ethernet segments in a protocol-independent way, based on an Ethernet address, rather than an IP address. In order to provide a simple and centralized bridge configuration, bridge options can now be used via **BRIDGING_OPTS**. As a result, a space-separated list of bridging options for either a bridge device or a port device can be added when the **ifup** utility is used.

BZ#554392

The updated **halt.local** file has been enhanced with new variables to reflect the character of call. This change leaves users with better knowledge of how **halt.local** was called during a halt sequence.

BZ#815431

With this update, it is possible to disable duplicate address detection in order to allow administrators to use direct routing without ARP checks.

Users of initscripts are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

7.88. IOK

7.88.1. RHBA-2012:1164 — iok bug fix update

Updated iok packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The iok package contains an Indic on-screen virtual keyboard that supports the Assamese, Bengali, Gujarati, Hindi, Kannada, Marathi, Malayalam, Punjabi, Oriya, Sindhi, Tamil and Telugu languages. Currently, iok works with Inscript and xkb keymaps for Indian languages, and is able to parse and display non-Inscript keymaps as well.

Bug Fixes

BZ#814541, BZ#814548

Previously, when saving a keymap with a specified name, predefined naming convention was followed and the file name was saved with the "-" prefix without noticing the user. With this update, if the user attempts to save a keymap, a dialog box displaying the required file name format appears.

BZ#819795

This update provides the complete iok translation for all supported locales.

All users of iok are advised to upgrade to these updated packages, which fix these bugs.

7.89. IPA

7.89.1. RHSA-2013:0528 — Low: ipa security, bug fix and enhancement update

Updated ipa packages that fix one security issue, several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Red Hat Identity Management is a centralized authentication, identity management and authorization solution for both traditional and cloud-based enterprise environments. It integrates components of the Red Hat Directory Server, MIT Kerberos, Red Hat Certificate System, NTP, and DNS. It provides web browser and command-line interfaces. Its administration tools allow an administrator to quickly install, set up, and administer a group of domain controllers to meet the authentication and identity management requirements of large-scale Linux and UNIX deployments.

NOTE

The ipa packages have been upgraded to upstream version 3.0.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#827602)

Security Fix

CVE-2012-4546

It was found that the current default configuration of IPA servers did not publish correct CRLs (Certificate Revocation Lists). The default configuration specifies that every replica is to generate its own CRL, however this can result in inconsistencies in the CRL contents provided to clients from different Identity Management replicas. More specifically, if a certificate is revoked on one Identity Management replica, it will not show up on another Identity Management replica.

Bug Fixes

BZ#784378

When a master was removed from a replicated environment via the "ipa-replica-manage del" command, the metadata for that master was still contained in the other servers, thus the Directory Server replication plug-in produced warnings about the outdated metadata. Now, the Directory Server CLEANALLRUV task is triggered to handle outdated metadata in the whole replicated Directory Server environment and deleting an Identity Management replica no longer causes problems.

BZ#790515

When the "ipactl" command was used to start Identity Management, it waited only 6 seconds for the Directory Server to start and when the Directory Server did not start in time, the start procedure was aborted. A higher default start up wait value was added. A configurable value, "startup_timeout", can be added to /etc/ipa/default.conf or /etc/ipa/server.conf files when the default value of 120 seconds is not sufficient to start the Directory Server.

BZ#809565

Previously, DNS records could not be renamed and administrators had to re-enter all DNS records under certain names when the name changed. Now, rename operations for DNS records names and the rename option in the Identity Management CLI interface are able to rename a DNS name and all of its records to other names within the same zone.

BZ#811295

Before, when installing Identity Management, there was an option to choose a certificate subject base with a Common Name (CN) as one component. However, it is illegal to have more than one CN attribute in a certificate subject. This caused the Identity Management installation to fail. Now, the CN attribute in a subject base option is no longer allowed, administrators are warned when they choose an incorrect certificate subject base and Identity Management installs properly.

BZ#815837

The Identity Management Certificate Authority component did not accept Directory Manager passwords which were set to a non-ASCII control character, "&" or "\". Use of these characters in passwords caused a malformed XML error and the Identity Management installation failed when such characters were a part of the Directory Manager password. Currently, these characters are not allowed in the Identity Management installer and IdM installs successfully.

BZ#816317

The Identity Management server or client used programs from the policycoreutils package when SELinux was enabled. However, the installers did not check if the package was actually installed. This caused the Identity Management installation to terminate with a python backtrace when SELinux was enabled and the policycoreutils package was not installed on a system. Currently, the Identity Management installers no longer fail when SELinux is enabled and the policycoreutils package is missing, but, instead, ask the administrator to install it first.

BZ#817865

The "ipa" command or Identity Management installers forced a set of address families (IPv4, IPv6) when a network connection was established, instead of letting the system choose the right address family for the new connection. In some cases this caused the connection, command or installer to fail, or the connection to take longer than normal. Automatic address family detection has been implemented and is now respected, with the result that network connections established with an "ipa" command are faster and less vulnerable to errors caused by non-common network settings.

BZ#819629

Identity Management DNS modules used a "pull" model for updating DNS records provisioned to the BIND name server by a bind-dyndb-ldap plug-in. When a DNS zone LDAP entry or DNS records present in bind-dyndb-ldap cache were changed via Identity Management CLI or Web UI, the update was not provisioned to the BIND nameserver until a zone was checked with a periodic poll or the DNS record in the cache expired. Now, persistent search is enabled by default for new Identity Management installations and for running Identity Management server instances. A change to the DNS zone LDAP entry or to the DNS record that is already cached by bind-dydnb-ldap is instantly provisioned to the BIND name server and thus resolvable.

BZ#820003

The default value of the Directory Server in-memory entry cache was configured to a lower value than the size of an administrator's deployment, which caused the Directory Server to underperform. Now, the Identity Management package requires an updated version of the Directory Server, which warns administrators when the in-memory cache is too small and allows administrators to adjust the value appropriate to ratio of deployment.

BZ#822608

When users were migrated from the remote Directory Server, entries in the Identity Management Directory Server did not have complete Kerberos data needed for Kerberos authentication, even though the users passed the Identity Management password migration page. The migrated Identity Management user was not able to authenticate via Identity Management until the password was manually reset. Currently, the Kerberos authentication data generates properly during the migration process and users can successfully access Identity Management.

BZ#824488

The Identity Management Kerberos data back end did not support an option to control automatic user log-on attributes, which were updated with every authentication. Administrators with large deployments and high numbers of authentication events in their Identity Management realm could not disable these automatic updates to avoid numerous Directory Server modification and replication events. Now, users can utilize options in Identity Management to customize automatic Kerberos authentication attribute updates.

BZ#824490

Previously, Identity Management enforced lowercase letters for all user IDs which caused some operations, such as password changes, to fail when the user ID was uppercase. Also, the WinSync agreement with Active Directory replicated such user information into the Identity Management database. Currently, the Identity Management WinSync plug-in can convert user names and Kerberos principal user parts to lowercase, and passwords replicated from Active Directory via the Winsync agreement can now be changed.

BZ#826677

When Identity Management replicas were deleted using the "ipa-replica-manage" command, the script did not verify if the deletion would orphan other Identity Management replicas. Users unaware of the Identity Management replication graph structure might accidentally delete a replica forcing them to reinstall the orphaned replicas. Now, the "ipa-replica-manage" command will not allow users to delete a remote replica if such operation would orphan a replica with a replication agreement.

BZ#832243

Identity Management Web UI was not fully compatible with the Microsoft Internet Explorer browser, which caused glitches when working with the Identity Management administration interface. Identity Management Web UI is now compatible with Microsoft Internet Explorer versions 9 or later and glitches no longer occur when working with the Web UI.

BZ#837356

Several attributes in the Identity Manager Directory Server that are used to store links to other objects in the directory were not added to the Directory Server Referential Integrity plug-in configuration. When a referred object was deleted or renamed it caused some links to break in the affected attribute and made them point to an invalid object. This update adds all attributes storing links to other objects to the Referential Integrity plug-in configuration, which are updated when the referred object is deleted or renamed.

BZ#839008

The Identity Management Web UI Administrator interface was not enabled for users who were indirect members of administrative roles. These users were not able to perform administrative tasks in the Web UI. Presently, indirect members of administrative roles can use the Web UI Administrator interface and are able to perform administrative tasks within the Identity Management Web UI.

BZ#840657

Normally, Identity Management SSH capabilities allow storage of public user or host SSH keys, but the keys did not accept the OpenSSH-style public key format. This caused Identity Management to estimate public key type based on the public key blob, which could have caused an issue in the future with new public key types. Now, Identity Management stores SSH public keys in extended OpenSSH format and SSH public keys now contain all required parts, making the functionality acceptable in more deployments.

BZ#855278

Previously, Identity Management Web UI used a jQuery library to raise errors when processing Directory Server records with some strings, for example, sudo commands with the "??" string in the name, which, in turn, caused the Web UI to be unable to show, modify or add such records. With this jQuery library update, Identity Management Web UI no longer reports errors for these strings and processes them normally.

BZ#859968

Firefox 15 and newer versions did not allow signed JavaScript JAR files to gain privilege escalation to change browser configuration. The Identity Management browser auto configuration configured the browser to access Web UI through Kerberos authentication, which affects these versions of Firefox. Now Identity Management is deployed with its own Firefox extension and is able to auto configure and authenticate using Kerberos.

BZ#868956

The Identity Management "dnszone-add" command accepts the "--name-server" option specifying a host name of the primary name server resolving the zone. The option considered all host names as fully qualified domain names (FQDN) even though they were not FQDN, for example, name server "ns.example.com." for zone example.com and were relative to the zone name, such as, name server "ns" for zone "example.com." Users were not able to specify the name server in the relative name format when using the Identity Management "dnszone-add" command. Presently, Identity Management detects the name server format correctly and the "dnszone-add" command can process both relative and fully qualified domain names.

BZ#877324

After upgrading to Red Hat Identity Management 2.2, it was not possible to add SSH public keys in the Web UI. However, SSH public keys could be added on the command line by running the "ipa user-mod user --sshpubkey" command. This update allows SSH public keys to be added in the Web

UI normally.

BZ#883484

Previously, the IPA automatic certificate renewal, in some cases, did not function properly and some certificates were not renewed while other certificates with the same "Not After" values were renewed. Certmonger is now updated, users can serialize access to the NSS databases to prevent corruption and do not have to renew and restart all the services at the same time.

BZ#888956

A 389-ds-base variable set during the PKI install "nsslapd-maxbersize" was not dynamically initialized and a restart was required for it to take effect. This caused installation to fail during the replication phase when building a replica from a PKI-CA master with a large CRL. This update includes an LDIF file (/usr/share/pki/ca/conf/database.ldif) to set the default maxbersize to a larger value and allows PKI-CA Replica Installs when CRL exceeds the default maxber value.

BZ#891980

Previously, on new IPA server installations, the root CA certificate lifetime was only valid for 8 years and users had to renew the certificate after it expired, which caused some inconvenience. This issue was fixed in Dogtag and this update increases the FreeIPA root CA validity to 20 years.

BZ#894131

The "ipa-replica-install" command sometimes failed to add the idnsSOAserial attribute for a new zone and in some cases, zones were added, but with missing data and did not replicate back to the master. With this update, the idnsSOAserial attribute sets properly and synchronizes across all servers and zones are added correctly.

BZ#894143

The "ipa-replica-prepare" command failed when a reverse zone did not have SOA serial data and reported a traceback error, which was difficult to read, when the problem occurred. Now, the "ipa-replica-prepare" command functions properly and if SOA serial data is missing, returns a more concise error message.

BZ#895298

When either dirsrv or krb5kdc were down, the "service named restart" command in the ipa-upgradeconfig failed during the upgrade of the ipa packages. With this update, the "service named restart" command functions normally and installation no longer fails during upgrades.

BZ#895561

Previously, the IPA install on a server with no IPv4 address failed with a "Can't contact LDAP server" error. With this update, both the server and replica install correctly and error messages no longer occur.

BZ#903758

Users who upgraded from IPA version 2.2 to version 3.0 encountered certmonger errors and the update failed with the error message, "certmonger failed to start tracking certificate." With this update, IPA 2.2 properly upgrades to version 3.0 without any errors.

BZ#905594

Before, users were unable to install the ipa-server-trust-ad package on a 32-bit platform and when doing so received the error message "Unable to read consumer identity." This update provides fixes in the spec file, and the package now installs properly on 32-bit platforms.

Enhancements

BZ#766007

This update introduces SELinux User Mapping rules which can be used in Identity Management in conjunction with HBAC rules to define the users, groups and hosts to which the rules apply.

BZ#766068

Support for SSH public key management added to the IPA server and OpenSSH on IPA clients is automatically configured to use the public keys stored on the IPA server. Now, when a host enrolled in Identity Management connects to another enrolled host, the SSH public key is verified in the central Identity Management storage.

BZ#766179

The Cross Realm Kerberos Trust functionality provided by Identity Management is included as a Technology Preview. This feature allows users to create a trust relationship between an Identity Management and an Active Directory domain. Users from the Active Directory domain can access resources and services from the Identity Management domain with their AD credentials and data does not need to be synchronized between the Identity Management and Active Directory domain controllers.

BZ#767379

An automated solution to configure automount on clients for automount maps configured in the central Identity Management server was added. After an Identity Management client has been configured, administrators may use the provided ipa-client-automount script to configure client hosts to use automount maps configured in the Identity Management server.

BZ#782981

Users using the Identity Management Web UI were previously forced to log in to client machines enrolled in Identity Management in order to update a password that had expired or been reset. With this update, users are able to more conveniently change an expired or reset password from the Web UI itself.

BZ#783166

This update allows the ipa-client-install interface to accept prioritization of IPA servers that clients connect to. Previously, administrators could not configure a prioritized IPA server that SSSD should connect to before connecting to other servers which were potentially returned in a SRV DNS query. Now, when a new option "--fixed-primary" is passed to the "ipa-client-install" command, the discovered or user-provided server is configured as the first value in the ipa_server directive in the "/etc/sssd/sssd.conf" file. Thus, SSSD will always try to connect to this host first.

BZ#783274

This enchancement allows MAC address attributes for host entries in Identity Management and publishes them in the Identity Management NIS server. Users can utilize the "--macaddress" option to configure MAC addresses for an Identity Management host entry and, when NIS is enabled, MAC address can be read by an ethers map.

BZ#786199

Each ipa command line request previously required full and time-consuming Kerberos authentication, particularly when a series of commands were scripted. This update enhances the command line to take advantage of server-side sessions using a secure cookie, which provides a significant performance improvement due to avoidance of full Kerberos authentication for each ipa command. The session cookie is stored in the session keyring; refer to the keyctl(1) man page for more information about the key management facility.

BZ#798363

This update introduces Web UI and CLI "Create Password Policy" entry labels and specifies measurement units, for example, "seconds" for all configured policy fields. Previously, missing measurement units in the Identity Management Web UI or CLI "Create Password Policy" might have confused some users. Now, all missing measurement units are specified in configured policy fields.

BZ#801931

This update allows administrators to delegate write privileges to a selected zone only, whereas, when administrators wanted to delegate privileges to update the DNS zone to other Identity Management users, they had to allow write access to the entire DNS tree. Now, administrators can use the "dnszone-add-permission" command to create a system permission allowing its assignee to read and write only a selected DNS zone managed by Identity Management.

BZ#804619

Prior to this update, administrators could not configure a slave DNS server because it could not function properly unless an SOA serial number was changed every time a DNS record was changed. With this update, SOA serial numbers are automatically increased when a record in a DNS zone managed by Identity Management is updated. This feature takes advantage of and requires the persistent search data refresh mechanism, which is enabled by default in the Identity Management server install script. Administrators can now configure a slave DNS server for zones managed by Identity Management.

BZ#805233

This update prevents deletion of the last administrator, because administrators could accidentally delete the last user from the Identity Management Administrators group, which could only be repaired with direct LDAP modification by the Directory Manager. Now, Identity Management does not allow administrators to delete or disable the last member in the administrator group and Identity Management always has at least one active administrator.

BZ#813402

This enhancement warns users in the Identity Management Web UI when their password is about to expire. When the Identity Management user password is about to expire in a configurable number of days, the user is notified in the Identity Management Web UI about this and is offered a link to reset the password.

BZ#821448

The Identity Management Firefox browser configuration script now checks if the browser is configured to send Referrer header in HTTP requests for Identity Management. Previously, Firefox browsers which did not have the "network.http.sendRefererHeader" configuration option set to "True" would fail to connect to the Identity Management Web UI, even though they ran the configuration script. Presently, the configuration option is set correctly and the Firefox browser can connect to the Web UI.

BZ#831010

This enhancement allows Identity Management client installer to accept a fixed set of Identity

Management servers and circumvent automatic server discovery via DNS SRV records. Some network environments may contain SRV records which are not suitable for Identity Management client and should not be used by the client at all. The "--fixed-primary" option of ipa-client-install can now be used to configure SSSD to not use DNS SRV records to auto-discover Identity Management servers and the client install script now accepts a fixed list of Identity Management servers which is then passed to SSSD.

BZ#835643

This update introduces an auto-renew of Identity Management Subsystem Certificates. The default validity period for a new Certificate Authority is 10 years and the CA issues a number of certificates for its subsystems (OCSP, audit log, and others). Subsystem certificates are normally valid for two years and if the certificates expire, the CA does not start up or does not function properly. Therefore, in Red Hat Enterprise Linux 6.4, Identity Management servers are capable of automatically renewing their subsystem certificates and the subsystem certificates are tracked by certmonger, which automatically attempts to renew the certificates before they expire.

Users of ipa are advised to upgrade to these updated packages, which address this security issue, fix these bugs and add these enhancements.

7.90. IPROUTE

7.90.1. RHBA-2013:0417 — iproute bug fix and enhancement update

Updated iproute packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The iproute packages contain networking utilities (ip and rtmon, for example) which are designed to use the advanced networking capabilities of the Linux kernel.

Bug Fix

BZ#811219

Invoking the socket stat utility, ss, with the "-ul" arguments did not list open UDP sockets. Consequently, users could not list open or listening UPD sockets. A patch has been applied to the ss utility to list UDP sockets and now the utility correctly reports all open UDP sockets.

Enhancement

BZ#821106

The iproute packages were distributed without the libnetlink library for accessing the netlink service. Consequently, it was not possible for users to utilize the libnetlink library features. The libnetlink library is now included in the newly introduced "iproute-devel" subpackage. As a result, users can now utilize libnetlink features.

All users of iproute are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

7.91. IPRUTILS

7.91.1. RHBA-2013:0378 — iprutils bug fix and enhancement update

An updated iprutils package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The iprutils package provides utilities to manage and configure SCSI devices that are supported by the IBM Power RAID SCSI storage device driver.

NOTE

The iprutils package has been upgraded to upstream version 2.3.12, which provides a number of bug fixes and enhancements over the previous version and adds support for the suspend/resume utility for IBM BlueHawk. (BZ#822648, BZ#860532, BZ#829761)

Bug Fixes

BZ#826907

Previously, showing disk details caused the iprconfig utility, which is used to configure Hardware RAID devices, to terminate unexpectedly. Now, disk details are shown properly and iprconfig no longer crashes.

BZ#830982

Previously, in some situations, iprconfig failed to change the IOA asymmetric access mode if the saved mode in the configuration file located in the "/etc/ipr/" directory was different than the current mode. With this update, iprconfig sets the mode correctly and a warning message is returned when this inconsistency is detected.

BZ#869751

Previously, iprutils showed the wrong disk platform location within the system location string when the "iprconfig -c show-details sgx" command was used. Now, the platform location for the hard disk is combined with the location of "secured easy setup" (SES) and the physical location slot number which prevents this error from occurring.

Users of iprutils are advised to upgrade to this updated package, which fixes these bugs.

7.92. IPTABLES

7.92.1. RHBA-2013:0332 — iptables bug fix and enhancement update

Updated iptables packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The iptables utility controls the network packet filtering code in the Linux kernel.

Bug Fixes

BZ#800208

The sysctl values for certain netfilter kernel modules, such as nf_conntrack and xt_conntrack, were not restored after a firewall restart. Consequently, the firewall did not always perform as expected after a restart. This update allows iptables to load sysctl settings on start if specified by the user in the /etc/sysctl.conf file. Users can now define sysctl settings to load on start and restart.

BZ#809108

The iptables(8) and ip6tables(8) man pages were previously missing information about the AUDIT target module, which allows creating audit records of the packet flow. This update adds the missing description of the audit support to these man pages.

BZ#821441

The iptables and ip6tables commands did not correctly handle calculation of the maximum length of iptables chains. Consequently, when assigning a firewall rule to an iptables chain with a name longer than 28 characters, the iptables or ip6tables command terminated with a buffer overflow and the rule was not assigned. This update corrects the related code so that iptables and ip6tables now handle names of iptable chains correctly and a firewall rule is assigned in the described scenario as expected.

BZ#836286

The iptables init script calls the /sbin/restorecon binary when saving firewall rules so that the iptables packages depend on the policycoreutils packages. However, the iptables packages previously did not require the policycoreutils as a dependency. Consequently, the "/etc/init.d/iptables save" command failed if the policycoreutils packages were not installed on the system. This update modifies the iptables spec file to require the policycoreutils packages as its prerequisite and thus prevents this problem from occurring.

Enhancements

BZ#747068

The iptables packages has been modified to support the update-alternatives mechanism to allow easier delivery of new iptables versions for the MRG Realtime kernel.

BZ#808272

Fallback mode has been added for the iptables and ip6tables services. A fallback firewall configuration can be stored in the /etc/sysconfig/iptables.fallback and /etc/sysconfig/ip6tables.fallback files in the iptables-save file format. The firewall rules from the fallback file are used if the service fails to apply the firewall rules from the /etc/sysconfig/iptables file (or the /etc/sysconfig/ip6tables file in case of ip6tables).

All users of iptables are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.93. IRQBALANCE

7.93.1. RHBA-2013:0367 — irqbalance bug fix and enhancement update

Updated irqbalance packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The irqbalance packages provide a daemon that evenly distributes interrupt request (IRQ) load across multiple CPUs for enhanced performance.

NOTE

The irqbalance packages have been upgraded to upstream version 1.0.4, which provides a number of bug fixes and enhancements over the previous version. Among other changes, the irqbalance daemon has been enhanced to support multiple MSI-X interrupts for PCI devices, which significantly boosts speed of devices producing high-rate interrupts, such as network cards. Also, the irqbalance logic has been modified to consider PCI bus topology when making IRQ mapping decisions. (BZ#789946)

Bug Fixes

BZ#813078

The irqbalance(1) man page did not contain documentation for the IRQBALANCE_BANNED_CPUS environment variable. This update adds the extensive documentation to this man page.

BZ#843379

The irqbalance daemon assigns each interrupt source in the system to a "class", which represents the type of the device (for example Networking, Storage or Media). Previously, irqbalance used the IRQ handler names from the /proc/interrupts file to decide the source class, which caused irqbalance to not recognize network interrupts correctly. As a consequence, systems that use NIC biosdevnames did not have their hardware interrupts distributed and pinned as expected. With this update, the device classification mechanism has been improved, which ensures a better interrupts distribution.

BZ#860627

Previously, the irqbalance init script started the irqbalance daemon with the "--foreground" option, which caused irqbalance to become unresponsive. With this update, the "--foreground" option has been removed from the init script and irqbalance now starts as expected.

All users of irqbalance are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.94. IRSSI

7.94.1. RHBA-2012:1171 — irssi bug fix update

Updated irssi packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

Irssi is a modular IRC client with Perl scripting. Only the text-mode front end is currently supported.

Bug Fix

BZ#639258

Prior to this update, when the user attempted to use the "/unload" command to unload a static module, Irssi incorrectly marked this module as unavailable, rendering the user unable to load this module again without restarting the client. This update adapts the underlying source code to ensure that only dynamic modules can be unloaded.

BZ#845047

The previous version of the irssi(1) manual page documented "--usage" as a valid command line option. This was incorrect, because Irssi no longer supports this option and an attempt to use it causes it to fail with an error. With this update, the manual page has been corrected and no longer documents unsupported command line options.

All users of irssi are advised to upgrade to these updated packages, which fix these bugs.

7.95. ISCSI-INITIATOR-UTILS

7.95.1. RHBA-2013:0438 — iscsi-initiator-utils bug fix and enhancement update

Updated iscsi-initiator-utils packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The iscsi-initiator-utils packages provide the server daemon for the Internet Small Computer System Interface (iSCSI) protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol (IP) networks.

NOTE

The iSCSI user-space driver, iscsiuio, has been upgraded to upstream version 0.7.6.1, which provides a number of bug fixes and enhancements over the previous version. In particular, VLAN and routing support. (BZ#826300)

Bug Fixes

BZ#826300

The iSCSI user-space driver, iscsiuio, has been upgraded to upstream version 0.7.6.1, which provides a number of bug fixes and enhancements over the previous version. In particular, VLAN and routing support.

BZ#811428

The "iscsiadm --version" command was missing the main version number, the leading "6.". This update corrects the version number value and "iscsiadm --version" now shows the main version number correctly.

BZ#854776

For some bnx2i cards, the network interface must be active for the iSCSI interface to report a valid MAC address. This sometimes lead to a failure to connect to an iSCSI target and consequently, iSCSI root setups failing to boot. This update changes iscsistart to put the network interface associated with the iSCSI context into an active state. As a result, iSCSI boot with bnx2i cards now works correctly.

BZ#868305

Due to a regression in the iscsiuio 0.7.4.3 update, iSCSI discovery and login failed on certain hardware. This has been corrected as part of the iscsiuio 0.7.6.1 update. As a result, iSCSI is functional again.

All users of iscsi-initiator-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.96. JSS

7.96.1. RHBA-2013:0424 — jss bug fix and enhancement update

Updated jss packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

Java Security Services (JSS) provides an interface between Java Virtual Machine and Network Security Services (NSS). It supports most of the security standards and encryption technologies supported by NSS including communication through SSL/TLS network protocols. JSS is primarily utilized by the Certificate Server.

Bug Fix

BZ#797352

Previously, some JSS calls to certain NSS functions were to be replaced with calls to the JCA interface. The original JSS calls were therefore deprecated and as such caused warnings to be reported during refactoring. However, the deprecated calls have not been fully replaced with their JCA-based implementation in JSS 4.2. With this update, the calls are now no longer deprecated and the warnings now longer occur.

Enhancement

BZ#804838

This update adds support for Elliptic Curve Cryptography (ECC) key archival in JSS. It provides new methods, such as getCurve(), Java_org_mozilla_jss_asn1_ASN1Util_getTagDescriptionByOid() and getECCurveBytesByX509PublicKeyBytes().

All users of jss are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

7.97. KABI-WHITELISTS

7.97.1. RHEA-2013:0485 — kabi-whitelists enhancement update

Updated kabi-whitelists packages that add various enhancements are now available for Red Hat Enterprise Linux 6.

The kabi-whitelists packages contain reference files documenting interfaces provided by the Red Hat Enterprise Linux 6 kernel that are considered to be stable by Red Hat engineering, and safe for long-term use by third-party loadable device drivers, as well as for other purposes.

Enhancements

BZ#826795

The "blk_queue_physical_block_size", "close_bdev_exclusive", "filemap_fdatawrite_range", "get_sb_nodev", "kill_anon_super", "open_bdev_exclusive", "jiffies_to_timespec", "kernel_getsockopt", "kernel_setsockopt", "radix_tree_delete", "pagevec_lookup", "recalc_sigpending", "path_put", and "simple_write_end" symbols have been added to the kernel application binary interface (ABI) whitelists.

BZ#831247

The "unlock_rename", "vfs_rename", "path_put", "default_llseek", "d_find_alias", "d_invalidate", "file_fsync", "strspn", "vfs_writev", "path_get", "nobh_truncate_page", "nobh_write_begin", "nobh_write_end", "nobh_writepage", "____pagevec_lru_add", "add_to_page_cache_locked", and "filemap_flush" symbols have been added to the kernel ABI whitelists.

BZ#902825

The "__generic_file_aio_write", "blk_queue_resize_tags", and "blk_queue_segment_boundary" symbols have been added to the kernel ABI whitelists.

BZ#849732

The following symbols have been added to the kernel ABI whitelists: "__alloc_pages", "__bitmap_weight", "__down_failed", "__free_pages", "__init_rwsem", "__init_waitqueue_head", "__kmalloc", "__memcpy", "__put_cred", "__raw_local_save_flags", "__stack_chk_fail", "__tasklet_schedule", "__tracepoint_kmalloc", "__up_wakeup", "__vmalloc", "__wake_up", "_cond_resched", "_spin_lock", "_spin_lock_irqsave", "_spin_unlock_irqrestore", "add_disk", "alloc_disk", "alloc_pages_current", "allow_signal", "autoremove_wake_function", "bio_endio", "bio_init", "bio_put", "blk_alloc_queue", "blk_cleanup_queue", "blk_queue_hardsect_size", "blk_queue_logical_block_size", "blk_queue_make_request", "blkdev_put", "complete", "complete_and_exit", "cond_resched", "contig_page_data", "copy_from_user", "copy_to_user", "cpu_present_map", "cpu_present_mask", "create_proc_entry", "daemonize", "del_gendisk", "do_gettimeofday", "down", "down_read", "down_read_trylock", "down_write", "down_write_trylock", "dump_stack", "filp_close", "filp_open", "finish_wait", "get_user_pages", "init_waitqueue_head", "jiffies", "jiffies_to_msecs", "jiffies_to_timeval", "kernel_thread", "kfree", "kmem_cache_alloc", "kmem_cache_alloc_notrace", "kmem_cache_create", "kmem_cache_destroy", "kmem_cache_free", "malloc_sizes", "mcount", "mem_map", "mem_section", "memcpy", "memset", "mod_timer", "msecs_to_jiffies", "msleep", "msleep_interruptible", "open_by_devnum", "override_creds", "panic", "per_cpu__current_task", "per_cpu__kernel_stack", "prepare_creds", "prepare_to_wait", "printk", "proc_mkdir", "put_disk", "put_page", "pv_irq_ops", "register_blkdev", "remove_proc_entry", "revert_creds", "schedule", "schedule_timeout", "send_sig", "set_user_nice", "sigprocmask", "slab_buffer_size", "snprintf", "sprintf", "strchr", "strcpy", "strncmp", "strncpy", "strnicmp", "strspn", "strstr", "submit_bio", "tasklet_init", "unregister_blkdev", "up", "up_read", "up_write", "vfree", "vfs_writev", "vscnprintf", and "wait_for_completion".

BZ#864893

The following symbols have been added to the kernel ABI whitelists: "blkdev_get", "send_sig_info", "__task_pid_nr_ns", "register_shrinker", "set_page_dirty_lock", "current_umask", "balance_dirty_pages_ratelimited_nr", "dentry_open", "generic_file_llseek_unlocked", "posix_acl_alloc", "posix_acl_from_xattr", "posix_acl_to_xattr", "posix_acl_valid", "read_cache_pages", "cancel_dirty_page", "clear_page", "grab_cache_page_nowait", "inode_init_always", "memparse", "put_unused_fd", "radix_tree_tag_set", "congestion_wait", "shrink_dcache_sb", "fd_install", "blk_make_request", "lookup_bdev", "__register_binfmt", "unregister_binfmt", "vm_stat", "kill_pid", and "kobject_get".

BZ#869353

A kernel checker tool (KSC) has been added to the kabi-whitelists packages.

Users of kabi-whitelists are advised to upgrade to these updated packages, which add these enhancements.

7.98. KDEBASE

7.98.1. RHBA-2012:1371 — kdebase bug fix update

Updated kdebase packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The K Desktop Environment (KDE) is a graphical desktop environment for the X Window System. The kdebase packages include core applications for KDE.

Bug Fixes

BZ#608007

Prior to this update, the Konsole context menu item "Show menu bar" was always checked in new windows even if this menu item was disabled before. This update modifies the underlying code to handle the menu item "Show menu bar" as expected.

BZ#729307

Prior to this update, users could not define a default size for xterm windows when using the Konsole terminal in KDE. This update modifies the underlying code and adds the functionality to define a default size.

All users of kdebase are advised to upgrade to these updated packages, which fix these bugs.

7.99. KDEBASE-WORKSPACE

7.99.1. RHBA-2012:1286 — kdebase-workspace bug fix update

Updated kdebase-workspace packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The kdebase-workspace packages contain utilities for basic operations with the desktop environment. The utilities allow users for example, to change system settings, resize and rotate X screens or set panels and widgets on the workspace.

Bug Fix

BZ#749460

Prior to this update, the task manager did not honor the order of manually arranged items. As a consequence, manually arranged taskbar entries were randomly rearranged when the user switched desktops. This update modifies the underlying code to make manually arranged items more persistent.

All users of kdebase-workspace are advised to upgrade to these updated packages, which fix this bug.

7.100. KDELIBS3

7.100.1. RHBA-2012:1244 — kdelibs3 bug fix update

Updated kdelibs3 packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The kdelibs3 packages provide libraries for the K Desktop Environment (KDE).

Bug Fixes

BZ#681901

Prior to this update, the kdelibs3 libraries caused a conflict for the subversion version control tool. As a consequence, subvervision was not correctly built if the kdelibs3 libraries were installed. This update modifies the underlying code to avoid this conflict. Now, subversion builds as expected with kdelibs3.

BZ#734447

kdelibs3 provided its own set of trusted Certificate Authority (CA) certificates. This update makes kdelibs3 use the system set from the ca-certificates package, instead of its own copy.

All users of kdelibs3 are advised to upgrade to these updated packages, which fix these bugs.

7.101. KDELIBS

7.101.1. RHBA-2012:1251 — kdelibs bug fix update

Updated kdelibs packages that fix various bugs are now available for Red Hat Enterprise Linux 6.

The kdelibs packages provide libraries for the K Desktop Environment (KDE).

Bug Fixes

BZ#587016

Prior to this update, the KDE Print dialog did not remember previous settings, nor did it allow the user to save the settings. Consequent to this, when printing several documents, users were forced to manually change settings for each printed document. With this update, the KDE Print dialog retains previous settings as expected.

BZ#682611

When the system was configured to use the Traditional Chinese language (the zh_TW locale), Konqueror incorrectly used a Chinese (zh_CN) version of its splash page. This update ensures that Konqueror uses the correct locale.

BZ#734734

Previously, clicking the system tray to display hidden icons could cause the Plasma Workspaces to consume an excessive amount of CPU time. This update applies a patch that fixes this error.

BZ#754161

When using Konqueror to recursively copy files and directories, if one of the subdirectories was not accessible, no warning or error message was reported to the user. This update ensures that Konqueror displays a proper warning message in this scenario.

BZ#826114

Prior to this update, an attempt to add "Terminal Emulator" to the Main Toolbar caused Konqueror to terminate unexpectedly with a segmentation fault. With this update, the underlying source code has been corrected to prevent this error so that users can now use this functionality as expected.

All users of kdelibs are advised to upgrade to these updated packages, which fix these bugs.

7.101.2. RHSA-2012:1418 — Critical: kdelibs security update

Updated kdelibs packages that fix two security issues are now available for Red Hat Enterprise Linux 6 FasTrack.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The kdelibs packages provide libraries for the K Desktop Environment (KDE). Konqueror is a web browser.

CVE-2012-4512

> A heap-based buffer overflow flaw was found in the way the CSS (Cascading Style Sheets) parser in kdelibs parsed the location of the source for font faces. A web page containing malicious content could cause an application using kdelibs (such as Konqueror) to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2012-4513

> A heap-based buffer over-read flaw was found in the way kdelibs calculated canvas dimensions for large images. A web page containing malicious content could cause an application using kdelibs to crash or disclose portions of its memory.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The desktop must be restarted (log out, then log back in) for this update to take effect.

7.102. KDEPIM

7.102.1. RHBA-2012:1287 — kdepim bug fix update

Updated kdepim packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The KDE Personal Information Management (kdepim) suite helps to organize your mail, tasks, appointments, and contacts.

Bug Fix

BZ#811125

> Prior to this update, the cyrus-sasl-plain package was not a dependency of the kdepim package. As a consequence, Kmail failed to send mail. This update modifies the underlying code to include the cyrus-sasl-plain dependency.

All users of kdepim are advised to upgrade to these updated packages, which fix this bug.

7.103. KERNEL

7.103.1. RHSA-2014:0634 — Important: kernel security and bug fix update

Updated kernel packages that fix three security issues and several bugs are now available for Red Hat Enterprise Linux 6.4 Extended Update Support.

The Red Hat Security Response Team has rated this update as having Important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2014-2523, Important

A flaw was found in the way the Linux kernel's netfilter connection tracking implementation for Datagram Congestion Control Protocol (DCCP) packets used the skb_header_pointer() function. A remote attacker could use this flaw to send a specially crafted DCCP packet to crash the system or, potentially, escalate their privileges on the system.

CVE-2013-6383, Moderate

A flaw was found in the way the Linux kernel's Adaptec RAID controller (aacraid) checked permissions of compat IOCTLs. A local attacker could use this flaw to bypass intended security restrictions.

CVE-2014-0077, Moderate

A flaw was found in the way the handle_rx() function handled large network packets when mergeable buffers were disabled. A privileged guest user could use this flaw to crash the host or corrupt QEMU process memory on the host, which could potentially result in arbitrary code execution on the host with the privileges of the QEMU process.

The CVE-2014-0077 issue was discovered by Michael S. Tsirkin of Red Hat.

Bug Fixes

BZ#1078512

The memory page allocation mechanism of the mlx4 driver used exclusively "order 2" allocations when allocating memory for incoming frames. This led to a high memory page allocation failure rate on systems with high memory fragmentation. With this update, the mlx4 driver firstly attempts to perform "order 3" allocations and then continues with lower order allocations up to "order 0" if the memory is too fragmented. As a result, performance of mlx4 cards is now significantly higher and mlx4 no longer generates memory page allocation failures when the system is under memory pressure.

BZ#1091161

Due to a ndlp list corruption bug in the lpfc driver, systems with Emulex LPe16002B-M6 PCIe 2-port 16Gb Fibre Channel Adapters could trigger a kernel panic during I/O operations. A series of patches has been backported to address this problem so the kernel no longer panics during I/O operations on the aforementioned systems.

BZ#1064912

Previously, the GFS2 kernel module leaked memory in the gfs2_bufdata slab cache and allowed a use-after-free race condition to be triggered in the gfs2_remove_from_journal() function. As a consequence after unmounting the GFS2 file system, the GFS2 slab cache could still contain some objects, which subsequently could, under certain circumstances, result in a kernel panic. A series of patches has been applied to the GFS2 kernel module, ensuring that all objects are freed from the slab cache properly and the kernel panic is avoided.

BZ#1078492

Due to a regression bug in the mlx4 driver, Mellanox mlx4 adapters could become unresponsive on heavy load along with IOMMU allocation errors being logged to the systems logs. A patch has been applied to the mlx4 driver so that the driver now calculates the last memory page fragment when allocating memory in the Rx path.

BZ#1086845

A system could enter a deadlock situation when the Real-Time (RT) scheduler was moving RT tasks between CPUs and the wakeup_kswapd() function was called on multiple CPUs, resulting in a kernel panic. This problem has been fixed by removing a problematic memory allocation and therefore calling the wakeup_kswapd() function from a deadlock-safe context.

BZ#1079868

Due to a bug in the hrtimers subsystem, the clock_was_set() function called an inter-processor interrupt (IPI) from soft IRQ context and waited to its completion, which could result in a deadlock situation. A patch has been applied to fix this problem by moving the clock_was_set() function call to the working context. Also during the resume process, the hrtimers_resume() function reprogrammed kernel timers only for the current CPU because it assumed that all other CPUs are offline. However, this assumption was incorrect in certain scenarios, such as when resuming a Xen guest with some non-boot CPUs being only stopped with IRQs disabled. As a consequence, kernel timers were not corrected on other than the boot CPU even though those CPUs were online. To resolve this problem, hrtimers_resume() has been modified to trigger an early soft IRQ to correctly reprogram kernel timers on all CPUs that are online.

BZ#1094621

When processing a directory with a huge amount of files (over five hundred thousand) on a GFS2 file system, the respective task could become unresponsive and memory allocation failures could occur. This happened because the GFS2 was updating atime in a memory reclamation path, resulting in occasional failures under memory pressure. To handle atime updates effectively, this update introduces a new super block operation, dirty_inode(). GFS2 now processes large directories as expected without any memory allocation failures or hanging tasks.

BZ#1092352

Prior to this update, a guest-provided value was used as the head length of the socket buffer allocated on the host. If the host was under heavy memory load and the guest-provided value was too large, the allocation could have failed, resulting in stalls and packet drops in the guest's Tx path. With this update, the guest-provided value has been limited to a reasonable size so that socket buffer allocations on the host succeed regardless of the memory load on the host, and guests can send packets without experiencing packet drops or stalls.

All kernel users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

7.103.2. RHSA-2014:0432 — Important: kernel security and bug fix update

Updated kernel packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 6.4 Extended Update Support.

The Red Hat Security Response Team has rated this update as having Important security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2014-0101, Important

A flaw was found in the way the Linux kernel processed an authenticated COOKIE_ECHO chunk during the initialization of an SCTP connection. A remote attacker could use this flaw to crash the system by initiating a specially crafted SCTP handshake in order to trigger a NULL pointer dereference on the system.

Red Hat would like to thank Nokia Siemens Networks for reporting this issue.

Bug Fixes

BZ#1077872

Previously, the vmw_pwscsi driver could attempt to complete a command to the SCSI mid-layer after reporting a successful abort of the command. This led to a double completion bug and a subsequent kernel panic. This update ensures that the pvscsi_abort() function returns SUCCESS only after the abort is completed, preventing the driver from invalid attempts to complete the command.

BZ#1028593

A bug in the kernel's file system code allowed the d_splice_alias() function to create a new dentry for a directory with an already-existing non-DISCONNECTED dentry. As a consequence, a thread accessing the directory could attempt to take the i_mutex on that directory twice, resulting in a deadlock situation. To resolve this problem, d_splice_alias() has been modified so that in the problematic cases, it reuses an existing dentry instead of creating a new dentry.

BZ#1063198

Recent changes in the d_splice_alias() function introduced a bug that allowed d_splice_alias() to return a dentry from a different directory than was the directory being looked up. As a consequence in cluster environment, a kernel panic could be triggered when a directory was being removed while a concurrent cross-directory operation was performed on this directory on another cluster node. This update avoids the kernel panic in this situation by correcting the search logic in the d_splice_alias() function so that the function can no longer return a dentry from an incorrect directory.

BZ#1078873

The Red Hat GFS2 file system previously limited a number of ACL entries per inode to 25. However, this number was insufficient in some cases, causing the setfacl command to fail. This update increases this limit to maximum of 300 ACL entries for the 4 KB block size. If the block size is smaller, this value is adjusted accordingly.

BZ#1078640

A bug in the megaraid_sas driver could cause the driver to read the hardware status values incorrectly. As a consequence, the RAID card was disabled during the system boot and the system could fail to boot. With this update, the megaraid_sas driver has been corrected so that the RAID card is now enabled on system boot as expected.

BZ#1017904

Previously, the kernel did not support unsharing for PID name spaces. With this update, a series of patches has been applied to the relevant kernel code to support the unshare() system call for PID name spaces.

BZ#1075553

When allocating kernel memory, the SCSI device handlers called the sizeof() function with a structure name as its argument. However, the modified files were using an incorrect structure name, which resulted in an insufficient amount of memory being allocated and subsequent memory corruption. This update modifies the relevant sizeof() function calls to rather use a pointer to the structure instead of the structure name so that the memory is now always allocated correctly.

BZ#1085307

Previously, GFS2 marked files that were written to for in-core data flushing only if the file size was actually increased. When the gfs2_fsync() function was called on a file that was not marked for in-core data flushing, any metadata or journaled data was not synchronized to the disk. This could, under certain circumstances, cause writes to files that were open for synchronous I/O to return before the data was written to the disk, allowing the data to be lost during a crash. A patch has been applied to mark files correctly whenever metadata has been updated during a write, ensuring that all in-core data are written to the disk with synchronous I/O operations.

BZ#1086590

Due to a bug in the GFS2 resource group code, the GFS2 block allocator did not switch from using blocking locks to non-blocking locks after the selected reservation group was found unsatisfactory for the allocation request with a block reservation. As a consequence, the block allocator used only blocking locks for all resource groups since that point, greatly reducing performance of the file system unless it was periodically remounted. This update ensures that the GFS2 block allocator overrides the non-blocking lock only for the appropriate resource group, and the file system performs as expected without any intervention.

All kernel users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

7.103.3. RHSA-2014:0284 — Important: kernel security and bug fix update

Updated kernel packages that fix several security issues and bugs are now available for Red Hat Enterprise Linux 6.4 Extended Update Support.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2013-4387, Important

A flaw was found in the way the Linux kernel's IPv6 implementation handled certain UDP packets when the UDP Fragmentation Offload (UFO) feature was enabled. A remote attacker could use this flaw to crash the system or, potentially, escalate their privileges on the system.

CVE-2013-4470, Important

A flaw was found in the way the Linux kernel's TCP/IP protocol suite implementation handled sending of certain UDP packets over sockets that used the UDP_CORK option when the UDP Fragmentation Offload (UFO) feature was enabled on the output device. A local, unprivileged user could use this flaw to cause a denial of service or, potentially, escalate their privileges on the system.

CVE-2013-6367, Important

A divide-by-zero flaw was found in the apic_get_tmcct() function in KVM's Local Advanced Programmable Interrupt Controller (LAPIC) implementation. A privileged guest user could use this flaw to crash the host.

CVE-2013-6368, Important

A memory corruption flaw was discovered in the way KVM handled virtual APIC accesses that crossed a page boundary. A local, unprivileged user could use this flaw to crash the system or, potentially, escalate their privileges on the system.

CVE-2013-6381, Important

A buffer overflow flaw was found in the way the qeth_snmp_command() function in the Linux kernel's QETH network device driver implementation handled SNMP IOCTL requests with an out-of-bounds length. A local, unprivileged user could use this flaw to crash the system or, potentially, escalate their privileges on the system.

CVE-2013-4591, Moderate

It was found that the fix for CVE-2012-2375 released via RHSA-2012:1580 accidentally removed a check for small-sized result buffers. A local, unprivileged user with access to an NFSv4 mount with ACL support could use this flaw to crash the system or, potentially, escalate their privileges on the system.

CVE-2013-2851, Low

A format string flaw was found in the Linux kernel's block layer. A privileged, local user could potentially use this flaw to escalate their privileges to kernel level (ring0).

Red Hat would like to thank Hannes Frederic Sowa for reporting CVE-2013-4470, Andrew Honig of Google for reporting CVE-2013-6367 and CVE-2013-6368, and Kees Cook for reporting CVE-2013-2851.

Bug Fixes

BZ#1063353

Previously, the sysfs_dev_char_kobj variable was freed on shutdown, but the variable could be used later by the USB stack, and possibly other code, which could cause the system to terminate unexpectedly. The underlying source code has been modified to prevent "kobjects" in the device_shutdown() function from being removed, as the /sys/dev/block/ and /sys/dev/char/ directories must be kept because of the symbolic links pointing to the devices. As a result, the system no longer crashes in the described scenario.

BZ#1062112

Previously, when hot adding memory to the system, the memory management subsystem always performed unconditional page-block scans for all memory sections being set online. The total duration of the hot add operation depends on both, the size of memory that the system already has and the size of memory that is being added. Therefore, the hot add operation took an excessive amount of time to complete if a large amount of memory was added or if the target node already had a considerable amount of memory. This update optimizes the code so that page-block scans are performed only when necessary, which greatly reduces the duration of the hot add operation.

BZ#1058417

When performing read operations on an XFS file system, failed buffer readahead can leave the buffer in the cache memory marked with an error. This could lead to incorrect detection of stale errors during completion of an I/O operation because most callers do not zero out the b_error field of the buffer on a subsequent read. To avoid this problem and ensure correct I/O error detection, the b_error field of the used buffer is now zeroed out before submitting an I/O operation on a file.

BZ#1060490

When transferring a large amount of data over the peer-to-peer (PPP) link, a rare race condition between the throttle() and unthrottle() functions in the tty driver could be triggered. As a consequence, the tty driver became unresponsive, remaining in the throttled state, which resulted in the traffic being stalled. Also, if the PPP link was heavily loaded, another race condition in the tty driver could has been triggered. This race allowed an unsafe update of the available buffer space, which could also result in the stalled traffic. A series of patches addressing both race conditions has been applied to the tty driver; if the first race is triggered, the driver loops and forces re-evaluation of the respective test condition, which ensures uninterrupted traffic flow in the described situation. The second race is now completely avoided due to a well-placed read lock, and the update of the available buffer space proceeds correctly.

BZ#1059990

Due to a bug in the SELinux socket receive hook, network traffic was not dropped upon receiving a peer:recv access control denial on some configurations. A broken labeled networking check in the SELinux socket receive hook has been corrected, and network traffic is now properly dropped in the described case.

BZ#1059382

Due to a bug in ext4 metadata allocation code, the number of metadata blocks needed to complete a file system operation could be calculated incorrectly. Consequently, when performing file system operations on a nearly full ext4 file system, unexpected allocation failures could occur at writeback time, leading to possible data loss and file system inconsistency. A series of patches has been applied, fixing metadata allocation estimation problems and introducing a reserved space concept that ensures correct allocation of metadata in specific situations, such as the aforementioned scenario.

BZ#1055363

Previously, certain SELinux functions did not correctly handle the TCP synchronize-acknowledgment (SYN-ACK) packets when processing IPv4 labeled traffic over an INET socket. The initial SYN-ACK packets were labeled incorrectly by SELinux, and as a result, the access control decision was made using the server socket's label instead of the new connection's label. In addition, SELinux was not properly inspecting outbound labeled IPsec traffic, which led to similar problems with incorrect access control decisions. A series of patches that addresses these problems has been applied to SELinux. The initial SYN-ACK packets are now labeled correctly and SELinux processes all SYN-ACK packets as expected.

BZ#1041143

A bug in the mlx4 driver could trigger a race between the "blue flame" feature's traffic flow and the stamping mechanism in the Tx ring flow when processing Work Queue Elements (WQEs) in the Tx ring. Consequently, the related queue pair (QP) of the mlx4 Ethernet card entered an error state and the traffic on the related Tx ring was blocked. A patch has been applied to the mlx4 driver so that the driver does not stamp the last completed WQE in the Tx ring, and thus avoids the aforementioned race.

BZ#1058419

Previously, the e752x_edac module incorrectly handled the pci_dev usage count, which could reach zero and deallocate a PCI device structure. As a consequence, a kernel panic could occur when the module was loaded multiple times on some systems. This update fixes the usage count that is triggered by loading and unloading of the module repeatedly, and a kernel panic no longer occurs.

BZ#1048098

Previously, task management commands in the lpfc driver had a fixed timeout value of 60 seconds, which could pose a problem for error handling. The lpfc driver has been upgraded to version 8.3.7.21.2p in order to include a fix of this problem. The timeout of the task management commands is now adjustable in range from 5 to 180 seconds, and by default, it is set to 60 seconds.

BZ#1046042

Inefficient usage of Big Kernel Locks (BKLs) in the ptrace() system call could lead to BKL contention on certain systems that widely utilize ptrace(), such as User-mode Linux (UML) systems, resulting in degraded performance on these systems. This update removes the relevant BKLs from the ptrace() system call, thus resolving any related performance issues.

BZ#1038122

An improper function call in a previous kernel patch backport caused the PID namespace nesting to malfunction. This could adversely affect the proper functioning of other components, such as the Linux Container (LXC) driver, that rely on nested PID namespace usage. A patch has been applied to correct this problem so that nested PID namespaces can be used as expected.

BZ#1056143

Previously, GFS2 marked files that were written to for in-core data flushing only if the file size was actually increased. When the gfs2_fsync() function was called on a file that was not marked for in-core data flushing, any metadata or journaled data was not synchronized to the disk. This could, under certain circumstances, cause writes to files that were open for synchronous I/O to return before the data was written to the disk, allowing the data to be lost during a crash. A patch has been applied to mark files correctly whenever metadata has been updated during a write, ensuring that all in-core data are written to the disk with synchronous I/O operations.

All kernel users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

7.103.4. RHBA-2013:1770 — kernel bug fix and enhancement update

Updated kernel packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.4 Extended Update Support.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Bug Fixes

BZ#962894

When extending memory, the hot-add operation could fail while the machine was under memory pressure, causing a kernel panic. A patch has been applied to improve the memory hot-add operation and this problem can now occur only in extremely rare occasions.

BZ#1030168

A bug in the netpoll transmit (Tx) code path that is used for netconsole logging could lead to various problems with bonding devices, for example, an invalid Tx queue index could have been used. To avoid these problems, an upstream patch has been backported to allow netpoll calling the external netdev_pick_tx() function from the netpoll_send_skb_on_dev() function.

BZ#1014968

The igb driver previously used a 16-bit mask when writing values of the flow control high-water mark to hardware registers on a network device. Consequently, the values were truncated on some network device, disrupting the flow control. A patch has been applied to the igb driver so that it now uses 32-bit mask as expected.

BZ#1006167

Previously, mounting a GFS2 file system in spectator mode on a cluster node was not possible if no other cluster node had already mounted this GFS2 file system. In such a case, a "file system consistency error" occurred and the GFS2 file system was withdrawn. A patch has been applied to allow the first cluster node mounting a GFS2 file system in spectator mode if all the file system journals are clean.

BZ#1006388

Due to a bug in the transmit path of the bonding driver, a buffer for the bonding device queue mapping could become corrupted. As a consequence, a kernel panic could occur or the system could become unresponsive in certain environments, such as is running a KVM guest in the Red Hat Enterprise Virtualization (RHEV) hypervisor with netconsole enabled and a bonding device over a network bridge configured. A patch has been applied to save the bonding device queue mapping buffer properly, and buffer corruption in this scenario is now prevented.

BZ#1006664

A bug in the kernel's super block code allowed a race between the get_active_super() and umount() functions that could lead to a use-after-free issue, resulting in a kernel oops. An upstream patch has been backported to fix this problem so that get_active_super() repeats attempts to obtain the active super block until it succeeds. The aforementioned race no longer occurs.

BZ#1008508

A kernel panic could occur during path failover on systems using multiple iSCSI, FC or SRP paths to connect an iSCSI initiator and an iSCSI target. This happened because a race condition in the SCSI driver allowed removing a SCSI device from the system before processing its run queue, which led to a NULL pointer dereference. The SCSI driver has been modified and the race is now avoided by holding a reference to a SCSI device run queue while it is active.

BZ#1009251

When a driver does not support namespace, the user must use the VLAN splinter feature from Open vSwitch to support VLANs and TCP traffic. However,when using the be2net driver and the VLAN splinter feature was enabled, the floating IP traffic could fail. This bug has been fixed and incompatibilities no longer occur, when using the VLAN splinter feature with the be2net driver.

BZ#1019614

When removing neigh entries, the list_del() function removed the neigh entry from the associated struct ipoib_path, while the ipoib_neigh_free() function removed the neigh entry from the device's neigh entry lookup table. Both of these operations were protected by a spinlock. However, the table was also protected by RCU kernel locking, and thus the spinlock was not held when performing read operations. Consequently, a race condition occurred, in which a thread could successfully look up a neigh entry that has already been deleted from the list of neighbor characters, but the previous deletion had marked the entry as "poisoned", and list_del() on the object caused a kernel panic. The list_del() function has been into ipoib_neigh_free(), so that deletion happens only once, after the entry has been successfully removed from the lookup table, thus fixing the bug.

BZ#1010451

If the arp_interval and arp_validate bonding options were not enabled on the configured bond device in the correct order, the bond device did not process ARP replies, which led to link failures and changes of the active slave device. A series of patches has been applied to modify an internal bond ARP hook based on the values of arp_validate and arp_interval. Therefore, the ARP hook is registered even if arp_interval is set after arp_validate has already been enabled, and ARP replies are processed as expected.

BZ#1018966

When GFS2 files were unlinked, sometimes they were not deleted completely. This could happen because when multiple nodes in a cluster accessed the same deleted file, the node responsible for freeing the "unlinked" blocks could not have been determined properly. Consequently, many deleted dinode blocks that should have been freed were often left in an "unlinked" state. With this update, the responsibility handover for deleting unlinked dinodes is accomplished through a mechanism known as the "iopen" glock. The "iopen" glocks are no longer cached by nodes after the point where it becomes impossible to free the dinode blocks. As a result, the dinode blocks for unlinked dinodes are now freed properly by the last process to close the file.

BZ#1017905

When the Audit subsystem was under heavy load, it could loop infinitely in the audit_log_start() function instead of failing over to the error recovery code. This could cause soft lockups in the kernel. With this update, the timeout condition in the audit_log_start() function has been modified to properly fail over when necessary.

BZ#1018965

Due to a race condition in the kernel's key management code, any process searching for a key in a keyring could dereference a NULL pointer while that key was instantiated as negative. This led to a kernel panic. A patch to fix this bug has been provided so that the kernel now handles the aforementioned situation properly without triggering the race.

BZ#1016108

The crypto_larval_lookup() function could return a larval, an in-between state when a cryptographic algorithm is being registered, even if it did not create one. This could cause a larval to be terminated twice, and result in a kernel panic. This occurred for example when the NFS service was running in FIPS mode, and attempted to use the MD5 hashing algorithm even though FIPS mode has this algorithm blacklisted. A condition has been added to the crypto_larval_lookup() function to check whether a larval was created before returning it.

BZ#1012049

Previously, the tcp_ioctl() function tried to take into account if a TCP socket has received a packet with a FIN flag in order to report the correct number of bytes in the receive queue. However, in certain cases, the reported number of bytes in the receive queue was incorrect. This bug has been fixed by using an improved way to detect if a TCP packet with a FIN flag has been received.

BZ#988807

Previously, on systems with RAID10 arrays defined, stack memory could become corrupted due to an insufficient amount of memory being allocated for a dynamically sized kernel data structure, leading to a kernel panic. This bug has been fixed and RAID10 arrays can now safely run without the risk of causing a kernel panic.

BZ#1009756

Due to the way the VFS code resolves dentry lookups, a race between multiple threads could have been triggered if the threads performed lookups on the same FUSE dentry subtree that contained an invalid (or stale) dentry or inode. As a consequence, the threads could fail with an ENOENT error instead of properly resolving a new dentry or inode. This update applies a series of patches to the FUSE code that addresses this problem and the aforementioned race can no longer occur.

BZ#1004661

Previously, the Hyper-V utility services negotiated the highest version of the Key-Value Pair (KVP) protocol that a Windows Server 2012 R2 host advertised but the host implemented a KVP protocol version that was not compatible with prior versions of the KVP protocol. Consequently, the IP injection functionality did not work on the latest Windows Server 2012 R2 host. This update explicitly specifies the KVP protocol version that the guest can support.

BZ#1012495

When a userspace process was reading the /proc/$PID/pagemap file, a memory leak could occur. An upstream patch has been provided to fix this bug, and memory usage before and after the mm_leak call is now the same.

BZ#1020994

Previously, when a CPU was brought offline, a race window occurred. During the race window, if an inter processor interrupt (IPI) was received, it got lost. As a consequence, the system became unresponsive. To fix this bug, a check has been added to the __cpu_disable() function, which executes the enqueued but not yet received IPIs before the CPU is marked offline.

BZ#1023350

Previously, when the user added an IPv6 route for local delivery, the route did not work and packets could not be sent. A patch has been applied to limit the neighbor entry creation only for input flow, thus fixing this bug. As a result, IPv6 routes for local delivery now work as expected.

BZ#1014687, BZ#1025736

The qla2xxx driver did not use any locking mechanism when passing information between its ISR and mailbox routines. Under certain conditions, this led to multiple mailbox command completions being signaled, which, in turn, led to a false mailbox timeout error for the subsequently issued mailbox command. This bug has been fixed and a mailbox timeout error no longer occurs in this scenario.

Enhancements

BZ#1011168

With this update, the missing values for the PG_buddy variable have been added to the kexec system call in order to increase dump performance relating to the buddy system for filtering free pages.

BZ#990483

Support for the fallocate method has been added to Filesystem in Userspace (FUSE). This method allows the caller to preallocate and deallocate blocks of a file.

Users of kernel are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. The system must be rebooted for this update to take effect.

7.103.5. RHSA-2013:1436 — Moderate: kernel security and bug fix update

Updated kernel packages that fix two security issues and several bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2013-4162, Moderate

A flaw was found in the way the Linux kernel's TCP/IP protocol suite implementation handled IPv6 sockets that used the UDP_CORK option. A local, unprivileged user could use this flaw to cause a denial of service.

CVE-2013-4299, Moderate

An information leak flaw was found in the way Linux kernel's device mapper subsystem, under certain conditions, interpreted data written to snapshot block devices. An attacker could use this flaw to read data from disk blocks in free space, which are normally inaccessible.

Red Hat would like to thank Hannes Frederic Sowa for reporting CVE-2013-4162; and Fujitsu for reporting CVE-2013-4299.

Bug Fixes

BZ#987261

Due to a bug in the NFS code, kernel size-192 and size-256 slab caches could leak memory. This could eventually result in an OOM issue when the most of available memory was used by the respective slab cache. A patch has been applied to fix this problem and the respective attributes in the NFS code are now freed properly.

BZ#987262

NFS previously allowed extending an NFS file write to cover a full page only if the file had not set a byte-range lock. However, extending the write to cover the entire page is sometimes desirable in order to avoid fragmentation inefficiencies. For example, a noticeable performance decrease was reported if a series of small non-contiguous writes was performed on the file. A patch has been applied to the NFS code that allows NFS extending a file write to a full page write if the whole file is locked for writing or if the client holds a write delegation.

BZ#988228

A change in the ipmi_si driver handling caused an extensively long delay while booting Red Hat Enterprise Linux 6.4 on SIG UV platforms. The driver was loaded as a kernel module on previous versions of Red Hat Enterprise Linux 6 while it is now built within the kernel. However, SIG UV does not use, and thus does not support the ipmi_si driver. A patch has been applied and the kernel now does not initialize the ipmi_si driver when booting on SIG UV.

BZ#988384

The GFS2 did not reserve journal space for a quota change block while growing the size of a file. Consequently, a fatal assertion causing a withdraw of the GFS2 file system could have been triggered when the free blocks were allocated from the secondary bitmap. With this update, GFS2 reserves additional blocks in the journal for the quota change so the file growing transaction can now complete successfully in this situation.

BZ#988708

A dentry leak occurred in the FUSE code when, after a negative lookup, a negative dentry was neither dropped nor was the reference counter of the dentry decremented. This triggered a BUG() macro when unmounting a FUSE subtree containing the dentry, resulting in a kernel panic. A series of patches related to this problem has been applied to the FUSE code and negative dentries are now properly dropped so that triggering the BUG() macro is now avoided.

BZ#991346

The fnic driver previously allowed I/O requests with the number of SGL descriptors greater than is supported by Cisco UCS Palo adapters. Consequently, the adapter returned any I/O request with more than 256 SGL descriptors with an error indicating invalid SGLs. A patch has been applied to limit the maximum number of supported SGLs in the fnic driver to 256 and the problem no longer occurs.

BZ#993544

An NFS server could terminate unexpectedly due to a NULL pointer dereference caused by a rare race condition in the lockd daemon. An applied patch fixes this problem by protecting the relevant code with spin locks, and thus avoiding the race in lockd.

BZ#993547

The kernel interface to ACPI had implemented error messaging incorrectly. The following error message was displayed when the system had a valid ACPI Error Record Serialization Table (ERST) and the pstore.backend kernel parameter had been used to disable use of ERST by the pstore interface:

```
ERST: Could not register with persistent store
```

However, the same message was also used to indicate errors precluding registration. A series of patches modifies the relevant ACPI code so that ACPI now properly distinguish between different cases and accordingly prints unique and informative messages.

BZ#994140

Due a bug in the memory mapping code, the fadvise64() system call sometimes did not flush all the relevant pages of the given file from cache memory. A patch addresses this problem by adding a test condition that verifies whether all the requested pages were flushed and retries with an attempt to empty the LRU pagevecs in the case of test failure.

BZ#994866

A previous patch to the CIFS code caused a regression of a problem where under certain conditions, a mount attempt of a CIFS DFS share fails with a "mount error(6): No such device or address" error message. This happened because the return code variable was not properly reset after a previous unsuccessful mount attempt. A backported patch has been applied to properly reset the variable and CIFS DFS shares can now be mounted as expected.

BZ#994867

Previously, systems running heavily-loaded NFS servers could experience poor performance of the NFS READDIR operations on large directories that were undergoing concurrent modifications, especially over higher latency connections. This happened because the NFS code performed certain dentry operations inefficiently and revalidated directory attributes too often. This update applies a series of patches that address the problem as follows; needed dentries can be accessed from dcache after the READDIR operation, and directory attributes are revalidated only at the beginning of the directory or if the cached attributes expire.

BZ#995334

A previous change in the bridge multicast code allowed sending general multicast queries in order to achieve faster convergence on startup. To prevent interference with multicast routers, send packets contained a zero source IP address. However, these packets interfered with certain multicast-aware switches, which resulted in the system being flooded with the IGMP membership queries with zero source IP address. A series of patches addresses this problem by disabling multicast queries by default and implementing multicast querier that allows to toggle up sending of general multicast queries if needed.

BZ#995458

When a slave device started up, the current_arp_slave parameter was unset but the active flags on the slave were not marked inactive. Consequently, more than one slave device with active flags in active-backup mode could be present on the system. A patch has been applied to fix this problem by marking the active flags inactive for a slave device before the current_arp_slave parameter is unset.

BZ#996014

An infinite loop bug in the NFSv4 code caused an NFSv4 mount process to hang on a busy loop of the LOOKUP_ROOT operation when attempting to mount an NFSv4 file system and the first iteration on this operation failed. A patch has been applied that allows to exit the LOOKUP_ROOT operation properly and a mount attempt now either succeeds or fails in this situation.

BZ#996424

An NFS client previously did not wait for completing of unfinished I/O operations before sending the LOCKU and RELEASE_LOCKOWNER operations to the NFS server in order to release byte range locks on files. Consequently, if the server processed the LOCKU and RELEASE_LOCKOWNER operations before some of the related READ operations, it released all locking states associated with the requested lock owner, and the READs returned the NFS4ERR_BAD_STATEID error code. This resulted in the "Lock reclaim failed!" error messages being generated in the system log and the NFS client had to recover from the error. A series of patches has been applied ensuring that an NFS client waits for all outstanding I/O operations to complete before releasing the locks.

BZ#997746

A previous patch to the bridge multicast code introduced a bug allowing reinitialization of an active timer for a multicast group whenever an IPv6 multicast query was received. A patch has been applied to the bridge multicast code so that a bridge multicast timer is no longer reinitialized when it is active.

BZ#997916

An use-after-free issue in the PPS (Pulse-per-second) driver could cause the kernel to crash when unregistering the PPS source. A patch has been applied to resolve this problem so the respective char device is now removed from the system prior to its deallocating. The patch also prevents deallocating a PPS device with open file descriptors.

BZ#999328

Previously, power-limit notification interrupts were enabled by default on the system. This could lead to degradation of system performance or even render the system unusable on certain platforms, such as Dell PowerEdge servers. A patch has been applied to disable power-limit notification interrupts by default and a new kernel command line parameter "int_pln_enable" has been added to allow users observing these events using the existing system counters. Power-limit notification messages are also no longer displayed on the console. The affected platforms no longer suffer from degraded system performance due to this problem.

BZ#1000314

A bug in the autofs4 mount expiration code could cause the autofs4 module to falsely report a busy tree of NFS mounts as "not in use". Consequently, automount attempted to unmount the tree and failed with a "failed to umount offset" error, leaving the mount tree to appear as empty directories. A patch has been applied to remove an incorrectly used autofs dentry mount check and the aforementioned problem no longer occurs.

BZ#1001954

An insufficiently designed calculation in the CPU accelerator could cause an arithmetic overflow in the set_cyc2ns_scale() function if the system uptime exceeded 208 days prior to using kexec to boot into a new kernel. This overflow led to a kernel panic on the systems using the Time Stamp Counter (TSC) clock source, primarily the systems using Intel Xeon E5 processors that do not reset TSC on soft power cycles. A patch has been applied to modify the calculation so that this arithmetic overflow and kernel panic can no longer occur under these circumstances.

BZ#1001963

Due to a bug in firmware, systems using the LSI MegaRAID controller failed to initialize this device in the kdump kernel if the "intel_iommu=on" and "iommu=pt"kernel parameters were specified in the first kernel. As a workaround until a firmware fix is available, a patch to the megaraid_sas driver has been applied so if the firmware is not in the ready state upon the first attempt to initialize the controller, the driver resets the controller and retries for firmware transition to the ready state.

BZ#1002184

Due to a bug in the SCTP code, a NULL pointer dereference could occur when freeing an SCTP association that was hashed, resulting in a kernel panic. A patch addresses this problem by trying to unhash SCTP associations before freeing them and the problem no longer occurs.

BZ#1003765

The RAID1 and RAD10 code previously called the raise_barrier() and lower_barrier() functions instead of the freeze_array() and unfreeze_array() functions that are safe being called from within the management thread. As a consequence, a deadlock situation could occur if an MD array contained a spare disk, rendering the respective kernel thread unresponsive. Furthermore, if a shutdown sequence was initiated after this problem had occurred, the shutdown sequence became unresponsive and any in-cache file system data that were not synchronized to the disk were lost. A patch correcting this problem has been applied and the RAID1 and RAID10 code now uses management-thread safe functions as expected.

BZ#1003931

A function in the RPC code responsible for verifying whether the cached credentials matches the current process did not perform the check correctly. The code checked only whether the groups in the current process credentials appear in the same order as in the cached credential but did not ensure that no other groups are present in the cached credentials. As a consequence, when accessing files in NFS mounts, a process with the same UID and GID as the original process but with a non-matching group list could have been granted an unauthorized access to a file, or under certain circumstances, the process could have been wrongly prevented from accessing the file. The incorrect test condition has been fixed and the problem can no longer occur.

BZ#1004657

The xen-netback and xen-netfront drivers cannot handle packets with size greater than 64 KB including headers. The xen-netfront driver previously did not account for any headers when determining the maximum size of GSO (Generic Segmentation Offload). Consequently, Xen DomU guest operations could have caused a network DoS issue on DomU when sending packets larger than 64 KB. This update adds a patch that corrects calculation of the GSO maximum size and the problem no longer occurs.

BZ#1006932

A bug in the real-time (RT) scheduler could cause a RT priority process to stop running due to an invalid attribute of the run queue. When a CPU became affected by this bug, the migration kernel thread stopped running on the CPU, and subsequently every other process that was migrated to the affected CPU by the system stopped running as well. A patch has been applied to the RT scheduler and RT priority processes are no longer affected this problem.

BZ#1006956

A patch included in kernel version 2.6.32-358.9.1.el6, to fix handling of revoked NFSv4 delegations, introduced a regression bug to the NFSv4 code. This regression in the NFSv4 exception and asynchronous error handling allowed, under certain circumstances, passing a NULL inode to an NFSv4 delegation-related function, which resulted in a kernel panic. The NFSv4 exception and asynchronous error handling has been fixed so that a NULL inode can no longer be passed in this situation.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

7.103.6. RHSA-2013:1173 — Important: kernel security and bug fix update

Updated kernel packages that fix several security issues and bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2013-2206, Important

A flaw was found in the way the Linux kernel's Stream Control Transmission Protocol (SCTP) implementation handled duplicate cookies. If a local user queried SCTP connection information at the same time a remote attacker has initialized a crafted SCTP connection to the system, it could trigger a NULL pointer dereference, causing the system to crash.

CVE-2013-2224, Important

It was found that the fix for CVE-2012-3552 released via RHSA-2012:1304 introduced an invalid free flaw in the Linux kernel's TCP/IP protocol suite implementation. A local, unprivileged user could use this flaw to corrupt kernel memory via crafted sendmsg() calls, allowing them to cause a denial of service or, potentially, escalate their privileges on the system.

CVE-2013-2146, Moderate

A flaw was found in the Linux kernel's Performance Events implementation. On systems with certain Intel processors, a local, unprivileged user could use this flaw to cause a denial of service by leveraging the perf subsystem to write into the reserved bits of the OFFCORE_RSP_0 and OFFCORE_RSP_1 model-specific registers.

CVE-2013-2232, Moderate

An invalid pointer dereference flaw was found in the Linux kernel'sTCP/IP protocol suite implementation. A local, unprivileged user could use this flaw to crash the system or, potentially, escalate their privileges on the system by using sendmsg() with an IPv6 socket connected to an IPv4 destination.

CVE-2012-6544, Low

Information leak flaws in the Linux kernel's Bluetooth implementation could allow a local, unprivileged user to leak kernel memory to user-space.

CVE-2013-2237, Low

An information leak flaw in the Linux kernel could allow a privileged, local user to leak kernel memory to user-space.

Bug Fixes

BZ#956054

The kernel could rarely terminate instead of creating a dump file when a multi-threaded process using FPU aborted. This happened because the kernel did not wait until all threads became inactive and attempted to dump the FPU state of active threads into memory which triggered a BUG_ON() routine. A patch addressing this problem has been applied and the kernel now waits for the threads to become inactive before dumping their FPU state into memory.

BZ#959930

Due to the way the CPU time was calculated, an integer multiplication overflow bug could occur after several days of running CPU bound processes that were using hundreds of kernel threads. As a consequence, the kernel stopped updating the CPU time and provided an incorrect CPU time instead. This could confuse users and lead to various application problems. This update applies a patch fixing this problem by decreasing the precision of calculations when the stime and rtime values become too large. Also, a bug allowing stime values to be sometimes erroneously calculated as utime values has been fixed.

BZ#963557

Due to several bugs in the ext4 code, data integrity system calls did not always properly persist data on the disk. Therefore, the unsynchronized data in the ext4 file system could have been lost after the system's unexpected termination. A series of patches has been applied to the ext4 code to address this problem, including a fix that ensures proper usage of data barriers in the code responsible for file synchronization. Data loss no longer occurs in the described situation.

BZ#974597

A previous patch that modified dcache and autofs code caused a regression. Due to this regression, unmounting a large number of expired automounts on a system under heavy NFS load caused soft lockups, rendering the system unresponsive. If a "soft lockup" watchdog was configured, the machine rebooted. To fix the regression, the erroneous patch has been reverted and the system now handle the aforementioned scenario properly without any soft lockups.

BZ#975576

A system could become unresponsive due to an attempt to shut down an XFS file system that was waiting for log I/O completion. A patch to the XFS code has been applied that allows for the shutdown method to be called from different contexts so XFS log items can be deleted properly even outside the AIL, which fixes this problem.

BZ#975578

XFS file systems were occasionally shut down with the "xfs_trans_ail_delete_bulk: attempting to delete a log item that is not in the AIL" error message. This happened because the EFI/EFD handling logic was incorrect and the EFI log item could have been freed before it was placed in the AIL and committed. A patch has been applied to the XFS code fixing the EFI/EFD handling logic and ensuring that the EFI log items are never freed before the EFD log items are processed. The aforementioned error no longer occurs on an XFS shutdown.

BZ#977668

A race condition between the read_swap_cache_async() and get_swap_page() functions in the memory management (mm) code could lead to a deadlock situation. The deadlock could occur only on systems that deployed swap partitions on devices supporting block DISCARD and TRIM operations if kernel preemption was disabled (the !CONFIG_PREEMPT parameter). If the read_swap_cache_async() function was given a SWAP_HAS_CACHE entry that did not have a page in the swap cache yet, a DISCARD operation was performed in the scan_swap_map() function. Consequently, completion of an I/O operation was scheduled on the same CPU's working queue the read_swap_cache_async() was running on. This caused the thread in read_swap_cache_async() to loop indefinitely around its "-EEXIST" case, rendering the system unresponsive. The problem has been fixed by adding an explicit cond_resched() call to read_swap_cache_async(), which allows other tasks to run on the affected CPU, and thus avoiding the deadlock.

BZ#977680, BZ#989923

A previous change in the port auto-selection code allowed sharing ports with no conflicts extending its usage. Consequently, when binding a socket with the SO_REUSEADDR socket option enabled, the bind(2) function could allocate an ephemeral port that was already used. A subsequent connection attempt failed in such a case with the EADDRNOTAVAIL error code. This update applies a patch that modifies the port auto-selection code so that bind(2) now selects a non-conflict port even with the SO_REUSEADDR option enabled.

BZ#979293

Cyclic adding and removing of the st kernel module could previously cause a system to become unresponsive. This was caused by a disk queue reference count bug in the SCSI tape driver. An upstream patch addressing this bug has been backported to the SCSI tape driver and the system now responds as expected in this situation.

BZ#979912

On KVM guests with the KVM clock (kvmclock) as a clock source and with some VCPUs pinned, certain VCPUs could experience significant sleep delays (elapsed time was greater 20 seconds). This resulted in unexpected delays by sleeping functions and inaccurate measurement for low latency events. The problem happened because a kvmclock update was isolated to a certain VCPU so the NTP frequency correction applied only to that single VCPU. This problem has been resolved by a patch allowing kvmclock updates to all VCPUs on the KVM guest. VCPU sleep time now does not exceed the expected amount and no longer causes the aforementioned problems.

BZ#981177

When using applications that intensively utilized memory mapping, customers experienced significant application latency, which led to serious performance degradation. A series of patches has been applied to fix the problem. Among other, the patches modifies the memory mapping code to allow block devices to require stable page writes, enforce stable page writes only if required by a backing device, and optionally snapshot page content to provide stable pages during write. As a result, application latency has been improved by a considerable amount and applications with high demand of memory mapping now perform as expected.

BZ#982116

The bnx2x driver could have previously reported an occasional MDC/MDIO timeout error along with the loss of the link connection. This could happen in environments using an older boot code because the MDIO clock was set in the beginning of each boot code sequence instead of per CL45 command. To avoid this problem, the bnx2x driver now sets the MDIO clock per CL45 command. Additionally, the MDIO clock is now implemented per EMAC register instead of per port number, which prevents ports from using different EMAC addresses for different PHY accesses. Also, a boot code or Management Firmware (MFW) upgrade is required to prevent the boot code (firmware) from taking over link ownership if the driver's pulse is delayed. The BCM57711 card requires boot code version 6.2.24 or later, and the BCM57712/578xx cards require MFW version 7.4.22 or later.

BZ#982472

If the Audit queue is too long, the kernel schedules the kauditd daemon to alleviate the load on the Audit queue. Previously, if the current Audit process had any pending signals in such a situation, it entered a busy-wait loop for the duration of an Audit backlog timeout because the wait_for_auditd() function was called as an interruptible task. This could lead to system lockup in non-preemptive uniprocessor systems. This update fixes the problem by setting wait_for_auditd() as uninterruptible.

BZ#982496

A possible race in the tty layer could result in a kernel panic after triggering the BUG_ON() macro. As a workaround, the BUG_ON() macro has been replaced by the WARN_ON() macro, which allows for avoiding the kernel panic and investigating the race problem further.

BZ#982571

A recent change in the memory mapping code introduced a new optional next-fit algorithm for allocating VMAs to map processed files to the address space. This change, however, broke behavior of a certain internal function which then always followed the next-fit VMA allocation scheme instead of the first-fit VMA allocation scheme. Consequently, when the first-fit VMA allocation scheme was in use, this bug caused linear address space fragmentation and could lead to early "-ENOMEM" failures for mmap() requests. This patch restores the original first-fit behavior to the function so the aforementioned problems no longer occur.

BZ#982697

When using certain HP hardware with UHCI HDC support and the uhci-hdc driver performed the auto-stop operation, the kernel emitted the "kernel: uhci_hcd 0000:01:00.4: Controller not stopped yet!" warning messages. This happened because HP's virtual UHCI host controller takes extremely long time to suspend (several hundred microseconds) even with no attached USB device and the driver was not adjusted to handle this situation. To avoid this problem, the uhci-hdc driver has been modified to not run the auto-stop operation until the controller is suspended.

BZ#982703

A previously released erratum, RHSA-2013:0911, included a patch that added support for memory configurations greater than 1 TB of RAM on AMD systems, and a patch that fixed a kernel panic preventing installation of Red Hat Enterprise Linux on such systems. However, these patches broke booting of Red Hat Enterprise Linux 6.4 on the SGI UV platform, and therefore they have been reverted with this update. Red Hat Enterprise Linux 6.4 now boots on SGI UV as expected.

BZ#982758

Due to a bug in descriptor handling, the ioat driver did not correctly process pending descriptors on systems with the Intel Xeon Processor E5 family. Consequently, the CPU was utilized excessively on these systems. A patch has been applied to the ioat driver so the driver now determines pending descriptors correctly and CPU usage is normal again for the described processor family.

BZ#990464

A bug in the network bridge code allowed an internal function to call code which was not atomic-safe while holding a spin lock. Consequently, a "BUG: scheduling while atomic" error has been triggered and a call trace logged by the kernel. This update applies a patch that orders the function properly so the function no longer holds a spin lock while calling code which is not atomic-safe. The aforementioned error with a call trace no longer occurs in this case.

BZ#990470

A race condition in the abort task and SPP device task management path of the isci driver could, under certain circumstances, cause the driver to fail cleaning up timed-out I/O requests that were pending on an SAS disk device. As a consequence, the kernel removed such a device from the system. A patch applied to the isci driver fixes this problem by sending the task management function request to the SAS drive anytime the abort function is entered and the task has not completed. The driver now cleans up timed-out I/O requests as expected in this situation.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

7.103.7. RHSA-2013:1051 — Moderate: kernel security and bug fix update

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

These packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2013-2128, Moderate

A flaw was found in the tcp_read_sock() function in the Linux kernel's IPv4 TCP/IP protocol suite implementation in the way socket buffers (skb) were handled. A local, unprivileged user could trigger this issue via a call to splice(), leading to a denial of service.

CVE-2012-6548, CVE-2013-2634, CVE-2013-2635, CVE-2013-3222, CVE-2013-3224, CVE-2013-3225, Low

Information leak flaws in the Linux kernel could allow a local, unprivileged user to leak kernel memory to user-space.

CVE-2013-0914, Low

An information leak was found in the Linux kernel's POSIX signals implementation. A local, unprivileged user could use this flaw to bypass the Address Space Layout Randomization (ASLR) security feature.

CVE-2013-1848, Low

A format string flaw was found in the ext3_msg() function in the Linux kernel's ext3 file system implementation. A local user who is able to mount an ext3 file system could use this flaw to cause a denial of service or, potentially, escalate their privileges.

CVE-2013-2852, Low

A format string flaw was found in the b43_do_request_fw() function in the Linux kernel's b43 driver implementation. A local user who is able to specify the "fwpostfix" b43 module parameter could use this flaw to cause a denial of service or, potentially, escalate their privileges.

CVE-2013-3301, Low

A NULL pointer dereference flaw was found in the Linux kernel's ftrace and function tracer implementations. A local user who has the CAP_SYS_ADMIN capability could use this flaw to cause a denial of service.

Red Hat would like to thank Kees Cook for reporting CVE-2013-2852.

Bug Fixes

BZ#924847

An error in backporting the block reservation feature from upstream resulted in a missing allocation of a reservation structure when an allocation is required during the rename system call. Renaming a file system object (for example, file or directory) requires a block allocation for the destination directory. If the destination directory had not had a reservation structure allocated, a NULL pointer dereference occurred, leading to a kernel panic. With this update, a reservation structure is allocated before the rename operation, and a kernel panic no longer occurs in this scenario. This patch also ensures that the inode's multi-block reservation is not deleted when a file is closed while changing the inode's size.

BZ#927308

When an inconsistency is detected in a GFS2 file system after an I/O operation, the kernel performs the withdraw operation on the local node. However, the kernel previously did not wait for an acknowledgement from the GFS control daemon (gfs_controld) before proceeding with the withdraw operation. Therefore, if a failure isolating the GFS2 file system from a data storage occurred, the kernel was not aware of this problem and an I/O operation to the shared block device may have been performed after the withdraw operation was logged as successful. This could lead to corruption of the file system or prevent the node from journal recovery. This patch modifies the GFS2 code so the withdraw operation no longer proceeds without the acknowledgement from gfs_controld, and the GFS2 file system can no longer become corrupted after performing the withdraw operation.

BZ#927317

The GFS2 discard code did not calculate the sector offset correctly for block devices with the sector size of 4 KB, which led to loss of data and metadata on these devices. A patch correcting this problem has been applied so the discard and FITRIM requests now work as expected for the block devices with the 4 KB sector size.

BZ#956296

The virtual file system (VFS) code had a race condition between the unlink and link system calls that allowed creating hard links to deleted (unlinked) files. This could, under certain circumstances, cause inode corruption that eventually resulted in a file system shutdown. The problem was observed in Red Hat Storage during rsync operations on replicated Gluster volumes that resulted in an XFS shutdown. A testing condition has been added to the VFS code, preventing hard links to deleted files from being created.

BZ#956979

The sunrpc code paths that wake up an RPC task are highly optimized for speed so the code avoids using any locking mechanism but requires precise operation ordering. Multiple bugs were found related to operation ordering, which resulted in a kernel crash involving either a BUG_ON() assertion or an incorrect use of a data structure in the sunrpc layer. These problems have been fixed by properly ordering operations related to the RPC_TASK_QUEUED and RPC_TASK_RUNNING bits in the wake-up code paths of the sunrpc layer.

BZ#958684

A previous update introduced a new failure mode to the blk_get_request() function returning the -ENODEV error code when a block device queue is being destroyed. However, the change did not include a NULL pointer check for all callers of the function. Consequently, the kernel could dereference a NULL pointer when removing a block device from the system, which resulted in a kernel panic. This update applies a patch that adds these missing NULL pointer checks. Also, some callers of the blk_get_request() function could previously return the -ENOMEM error code instead of -ENODEV, which would lead to incorrect call chain propagation. This update applies a patch ensuring that correct return codes are propagated.

BZ#962368

A rare race condition between the "devloss" timeout and discovery state machine could trigger a bug in the lpfc driver that nested two levels of spin locks in reverse order. The reverse order of spin locks led to a deadlock situation and the system became unresponsive. With this update, a patch addressing the deadlock problem has been applied and the system no longer hangs in this situation.

BZ#962370

When attempting to deploy a virtual machine on a hypervisor with multiple NICs and macvtap devices, a kernel panic could occur. This happened because the macvtap driver did not gracefully handle a situation when the macvlan_port.vlans list was empty and returned a NULL pointer. This update applies a series of patches which fix this problem using a read-copy-update (RCU) mechanism and by preventing the driver from returning a NULL pointer if the list is empty. The kernel no longer panics in this scenario.

BZ#962372

Certain CPUs contain on-chip virtual-machine control structure (VMCS) caches that are used to keep active VMCSs managed by the KVM module. These VMCSs contain runtime information of the guest machines operated by KVM. These CPUs require support of the VMCLEAR instruction that allows flushing the cache's content into memory. The kernel previously did not use the VMCLEAR instruction in Kdump. As a consequence, when dumping a core of the QEMU KVM host, the respective CPUs did not flush VMCSs to the memory and the guests' runtime information was not included in the core dump. This problem has been addressed by a series of patches that implement support of using the VMCLEAR instruction in Kdump. The kernel is now performs the VMCLEAR operation in Kdump if it is required by a CPU so the vmcore file of the QEMU KVM host contains all VMCSs information as expected.

BZ#963564

When a network interface (NIC) is running in promiscuous (PROMISC) mode, the NIC may receive and process VLAN tagged frames even though no VLAN is attached to the NIC. However, some network drivers, such as bnx2, igb, tg3, and e1000e did not handle processing of packets with VLAN tagged frames in PROMISC mode correctly if the frames had no VLAN group assigned. The drivers processed the packets with incorrect routines and various problems could occur; for example, a DHCPv6 server connected to a VLAN could assign an IPv6 address from the VLAN pool to a NIC with no VLAN interface. To handle the VLAN tagged frames without a VLAN group properly, the frames have to be processed by the VLAN code so the aforementioned drivers have been modified to restrain from performing a NULL value test of the packet's VLAN group field when the NIC is in PROMISC mode. This update also includes a patch fixing a bug where the bnx2x driver did not strip a VLAN header from the frame if no VLAN was configured on the NIC, and another patch that implements some register changes in order to enable receiving and transmitting of VLAN packets on a NIC even if no VLAN is registered with the card.

BZ#964046

Due to a bug in the NFSv4 nfsd code, a NULL pointer could have been dereferenced when nfsd was looking up a path to the NFSv4 recovery directory for the fsync operation, which resulted in a kernel panic. This update applies a patch that modifies the NFSv4 nfsd code to open a file descriptor for fsync in the NFSv4 recovery directory instead of looking up the path. The kernel no longer panics in this situation.

BZ#966432

When adding a virtual PCI device, such as virtio disk, virtio net, e1000 or rtl8139, to a KVM guest, the kacpid thread reprograms the hot plug parameters of all devices on the PCI bus to which the new device is being added. When reprogramming the hot plug parameters of a VGA or QXL graphics device, the graphics device emulation requests flushing of the guest's shadow page tables. Previously, if the guest had a huge and complex set of shadow page tables, the flushing operation took a significant amount of time and the guest could appear to be unresponsive for several minutes. This resulted in exceeding the threshold of the "soft lockup" watchdog and the "BUG: soft lockup" events were logged by both, the guest and host kernel. This update applies a series of patches that deal with this problem. The KVM's Memory Management Unit (MMU) now avoids creating multiple page table roots in connection with processors that support Extended Page Tables (EPT). This prevents the guest's shadow page tables from becoming too complex on machines with EPT support. MMU now also flushes only large memory mappings, which alleviates the situation on machines where the processor does not support EPT. Additionally, a free memory accounting race that could prevent KVM MMU from freeing memory pages has been fixed.

BZ#968557

A race condition could occur in the uhci-hcd kernel module if the IRQ line was shared with other devices. The race condition allowed the IRQ handler routine to be called before the data structures were fully initialized, which caused the system to become unresponsive. This update applies a patch that fixes the problem by adding a test condition to the IRQ handler routine; if the data structure initialization is still in progress, the handler routine finishes immediately.

BZ#969306

When setting up a bonding device, a certain flag was used to distinguish between TLB and ALB modes. However, usage of this flag in ALB mode allowed enslaving NICs before the bond was activated. This resulted in enslaved NICs not having unique MAC addresses as required, and consequent loss of "reply" packets sent to the slaves. This patch modifies the function responsible for the setup of the slave's MAC address so the flag is no longer needed to discriminate ALB mode from TLB and the flag was removed. The described problem no longer occur in this situation.

BZ#969326

When booting the normal kernel on certain servers, such as HP ProLiant DL980 G7, some interrupts may have been lost which resulted in the system being unresponsive or rarely even in data loss. This happened because the kernel did not set correct destination mode during the boot; the kernel booted in "logical cluster mode" that is default while this system supported only "x2apic physical mode". This update applies a series of patches addressing the problem. The underlying APIC code has been modified so the x2apic probing code now checks the Fixed ACPI Description Table (FADT) and installs the x2apic "physical" driver as expected. Also, the APIC code has been simplified and the code now uses probe routines to select destination APIC mode and install the correct APIC drivers.

BZ#972586

A bug in the OProfile tool led to a NULL pointer dereference while unloading the OProfile kernel module, which resulted in a kernel panic. The problem was triggered if the kernel was running with the nolapic parameter set and OProfile was configured to use the NMI timer interrupt. The problem has been fixed by correctly setting the NMI timer when initializing OProfile.

BZ#973198

Previously, when booting a Red Hat Enterprise Linux 6.4 system and the ACPI Static Resource Affinity Table (SRAT) had a hot-pluggable bit enabled, the kernel considered the SRAT table incorrect and NUMA was not configured. This led to a general protection fault and a kernel panic occurring on the system. The problem has been fixed by using an SMBIOS check in the code in order to avoid the SRAT code table consistency checks. NUMA is now configured as expected and the kernel no longer panics in this situation.

BZ#973555

A bug in the PCI driver allowed to use a pointer to the Virtual Function (VF) device entry that was already freed. Consequently, when hot-removing an I/O unit with enabled SR-IOV devices, a kernel panic occurred. This update modifies the PCI driver so a valid pointer to the Physical Function (PF) device entry is used and the kernel no longer panics in this situation.

BZ#975086

The kernel previously did not handle situation where the system needed to fall back from non-flat Advanced Programmable Interrupt Controller (APIC) mode to flat APIC mode. Consequently, a NULL pointer was dereferenced and a kernel panic occurred. This update adds the flat_probe() function to the APIC driver, which allows the kernel using flat APIC mode as a fall-back option. The kernel no longer panics in this situation.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

7.103.8. RHSA-2013:0911 — Important: kernel security, bug fix and enhancement update

Updated kernel packages that fix several security issues and bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2013-1935, Important

A flaw was found in the way KVM (Kernel-based Virtual Machine) initialized a guest's registered pv_eoi (paravirtualized end-of-interrupt) indication flag when entering the guest. An unprivileged guest user could potentially use this flaw to crash the host.

CVE-2013-1943, Important

A missing sanity check was found in the kvm_set_memory_region() function in KVM, allowing a user-space process to register memory regions pointing to the kernel address space. A local, unprivileged user could use this flaw to escalate their privileges.

CVE-2013-2017, Moderate

A double free flaw was found in the Linux kernel's Virtual Ethernet Tunnel driver (veth). A remote attacker could possibly use this flaw to crash a target system.

Red Hat would like to thank IBM for reporting the CVE-2013-1935 issue and Atzm WATANABE of Stratosphere Inc. for reporting the CVE-2013-2017 issue. The CVE-2013-1943 issue was discovered by Michael S. Tsirkin of Red Hat.

Bug Fixes

BZ#923096

Previously, the queue limits were not being retained as they should have been if a device did not contain any data or if a multipath device temporarily lost all its paths. This problem has been fixed by avoiding a call to the **`dm_calculate_queue_limits()`** function.

BZ#924823

A bug in the **`dm_btree_remove()`** function could cause leaf values to have incorrect reference counts. Removal of a shared block could result in space maps considering the block as no longer used. As a consequence, sending a discard request to a shared region of a thin device could corrupt its snapshot. The bug has been fixed to prevent corruption in this scenario.

BZ#927292

Prior to this update, if Large Receive Offload (LRO) was enabled, Broadcom, QLogic, and Intel card drivers did not fill in all the packet fields. Consequently, when the **`macvtap`** driver received a packet with a **`gso_type`** field that was not set, a kernel panic occurred. With this update, the **`ixgbe`**, **`qlcnic`**, and **`bnx2x`** drivers have been fixed to always set the **`gso_type`** field. Thus, kernel panic no longer occurs in the previously-described scenario.

BZ#927294

Reading a large number of files from a pNFS (parallel NFS) mount and canceling the running operation by pressing **`Ctrl`**+**`c`** caused a general protection fault in the XDR code, which could manifest itself as a kernel oops with an **`unable to handle kernel paging request`** message. This happened because decoding of the **`LAYOUTGET`** operation is done by a worker thread and the caller waits for the worker thread to complete. When the reading operation was canceled, the caller stopped waiting and freed the pages. So the pages no longer existed at the time the worker thread called the relevant function in the XDR code. The cleanup process of these pages has been moved to a different place in the code, which prevents the kernel oops from happening in this scenario.

BZ#961431

By default, the kernel uses a best-fit algorithm for allocating Virtual Memory Areas (VMAs) to map processed files to the address space. However, if an enormous number of small files (hundreds of thousands or millions) was being mapped, the address space became extremely fragmented, which resulted in significant CPU usage and performance degradation. This update introduces an optional next-fit policy which, if enabled, allows for mapping of a file to the first suitable unused area in the address space that follows after the previously allocated VMA.

BZ#960864

C-states for the Intel Family 6, Model 58 and 62, processors were not properly initialized in Red Hat Enterprise Linux 6. Consequently, these processors were unable to enter deep C-states. Also, C-state accounting was not functioning properly and power management tools, such as powertop or turbostat, thus displayed incorrect C-state transitions. This update applies a patch that ensures proper C-states initialization so the aforementioned processors can now enter deep core power states as expected. Note that this update does not correct C-state accounting which has been addressed by a separate patch.

BZ#960436

If an NFSv4 client was checking open permissions for a delegated OPEN operation during OPEN state recovery of an NFSv4 server, the NFSv4 state manager could enter a deadlock. This happened because the client was holding the NFSv4 sequence ID of the OPEN operation. This problem is resolved by releasing the sequence ID before the client starts checking open permissions.

BZ#960429

When using parallel NFS (pNFS), a kernel panic could occur when a process was killed while getting the file layout information during the open() system call. A patch has been applied to prevent this problem from occurring in this scenario.

BZ#960426

In the RPC code, when a network socket backed up due to high network traffic, a timer was set causing a retransmission, which in turn could cause even larger amount of network traffic to be generated. To prevent this problem, the RPC code now waits for the socket to empty instead of setting the timer.

BZ#960420

Previously, the fsync(2) system call incorrectly returned the EIO (Input/Output) error instead of the ENOSPC (No space left on device) error. This was caused by incorrect error handling in the page cache. This problem has been fixed and the correct error value is now returned.

BZ#960417

Previously, an NFS RPC task could enter a deadlock and become unresponsive if it was waiting for an NFSv4 state serialization lock to become available and the session slot was held by the NFSv4 server. This update fixes this problem along with the possible race condition in the pNFS return-on-close code. The NFSv4 client has also been modified to not accepting delegated OPEN operations if a delegation recall is in effect. The client now also reports NFSv4 servers that try to return a delegation when the client is using the CLAIM_DELEGATE_CUR open mode.

BZ#952613

When pNFS code was in use, a file locking process could enter a deadlock while trying to recover form a server reboot. This update introduces a new locking mechanism that avoids the deadlock situation in this scenario.

BZ#960412

Previously, when open(2) system calls were processed, the GETATTR routine did not check to see if valid attributes were also returned. As a result, the open() call succeeded with invalid attributes instead of failing in such a case. This update adds the missing check, and the open() call succeeds only when valid attributes are returned.

BZ#955504

The be2iscsi driver previously leaked memory in the driver's control path when mapping tasks.This update fixes the memory leak by freeing all resources related to a task when the task was completed. Also, the driver did not release a task after responding to the received NOP-IN acknowledgment with a valid Target Transfer Tag (TTT). Consequently, the driver run out of tasks available for the session and no more iscsi commands could be issued. A patch has been applied to fix this problem by releasing the task.

BZ#960415

Due to a missing structure, the NFSv4 error handler did not handle exceptions caused by revoking NFSv4 delegations. Consequently, the NFSv4 client received the EIO error message instead of the NFS4ERR_ADMIN_REVOKED error. This update modifies the NFSv4 code to no longer require the nfs4_state structure in order to revoke a delegation.

BZ#954298

Under rare circumstances, if a TCP retransmission was multiple times partially acknowledged and collapsed, the used Socked Buffer (SKB) could become corrupted due to an overflow caused by the transmission headroom. This resulted in a kernel panic. The problem was observed rarely when using an IP-over-InfiniBand (IPoIB) connection. This update applies a patch that verifies whether a transmission headroom exceeded the maximum size of the used SKB, and if so, the headroom is reallocated. It was also discovered that a TCP stack could retransmit misaligned SKBs if a malicious peer acknowledged sub MSS frame and output interface did not have a sequence generator (SG) enabled. This update introduces a new function that allows for copying of a SKB with a new head so the SKB remains aligned in this situation.

BZ#921964

In a case of a broken or malicious server, an index node (inode) of an incorrect type could be matched. This led to an NFS client NULL pointer dereference, and, consequently, to a kernel oops. To prevent this problem from occurring in this scenario, a check has been added to verify that the inode type is correct.

BZ#962482

When using more than 4 GB of RAM with an AMD processor, reserved regions and memory holes (E820 regions) can also be placed above the 4 GB range. For example, on configurations with more than 1 TB of RAM, AMD processors reserve the 1012 GB - 1024 GB range for the Hyper Transport (HT) feature. However, the Linux kernel does not correctly handle E820 regions that are located above the 4 GB range. Therefore, when installing Red Hat Enterprise Linux on a machine with an AMD processor and 1 TB of RAM, a kernel panic occurred and the installation failed. This update modifies the kernel to exclude E820 regions located above the 4 GB range from direct mapping. The kernel also no longer maps the whole memory on boot but only finds memory ranges that are necessary to be mapped. The system can now be successfully installed on the above-described configuration.

BZ#950529

This update reverts two previously-included **qla2xxx** patches. These patches changed the fibre channel target port discovery procedure, which resulted in some ports not being discovered in some corner cases. Reverting these two patches fixes the discovery issues.

BZ#928817

A previously-applied patch introduced a bug in the **ipoib_cm_destroy_tx()** function, which allowed a CM object to be moved between lists without any supported locking. Under a heavy system load, this could cause the system to crash. With this update, proper locking of the CM objects has been re-introduced to fix the race condition, and the system no longer crashes under a heavy load.

BZ#928683

A bug in the **do_filp_open()** function caused it to exit early if any write access was requested on a read-only file system. This prevented the opening of device nodes on a read-only file system. With this update, the **do_filp_open()** has been fixed to no longer exit if a write request is made on a read-only file system.

BZ#960433

An NFSv4 client could previously enter a deadlock situation with the state recovery thread during state recovery after a reboot of an NFSv4 server. This happened because the client did not release the NFSv4 sequence ID of an OPEN operation that was requested before the reboot. This problem is resolved by releasing the sequence ID before the client starts waiting for the server to recover.

Enhancement

BZ#952570

The kernel now supports memory configurations with more than 1 TB of RAM on AMD systems.

Users should upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement. The system must be rebooted for this update to take effect.

7.103.9. RHSA-2013:0744 — Important: kernel security and bug fix update

Updated kernel packages that fix several security issues and several bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2013-0913, Important

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the way the Intel i915 driver in the Linux kernel handled the allocation of the buffer used for relocation copies. A local user with console access could use this flaw to cause a denial of service or escalate their privileges.

CVE-2013-1773, Important

A buffer overflow flaw was found in the way UTF-8 characters were converted to UTF-16 in the utf8s_to_utf16s() function of the Linux kernel's FAT file system implementation. A local user able to mount a FAT file system with the "utf8=1" option could use this flaw to crash the system or, potentially, to escalate their privileges.

CVE-2013-1796, Important

A flaw was found in the way KVM handled guest time updates when the buffer the guest registered by writing to the MSR_KVM_SYSTEM_TIME machine state register (MSR) crossed a page boundary. A privileged guest user could use this flaw to crash the host or, potentially, escalate their privileges, allowing them to execute arbitrary code at the host kernel level.

CVE-2013-1797, Important

A potential use-after-free flaw was found in the way KVM handled guest time updates when the GPA (guest physical address) the guest registered by writing to the MSR_KVM_SYSTEM_TIME machine state register (MSR) fell into a movable or removable memory region of the hosting user-space process (by default, QEMU-KVM) on the host. If that memory region is deregistered from KVM using KVM_SET_USER_MEMORY_REGION and the allocated virtual memory reused, a privileged guest user could potentially use this flaw to escalate their privileges on the host.

CVE-2013-1798, Important

A flaw was found in the way KVM emulated IOAPIC (I/O Advanced Programmable Interrupt Controller). A missing validation check in the ioapic_read_indirect() function could allow a privileged guest user to crash the host, or read a substantial portion of host kernel memory.

CVE-2013-1792, Moderate

A race condition in install_user_keyrings(), leading to a NULL pointer dereference, was found in the key management facility. A local, unprivileged user could use this flaw to cause a denial of service.

CVE-2013-1826, Moderate

A NULL pointer dereference in the XFRM implementation could allow a local user who has the CAP_NET_ADMIN capability to cause a denial of service.

CVE-2013-1827, Moderate

A NULL pointer dereference in the Datagram Congestion Control Protocol (DCCP) implementation could allow a local user to cause a denial of service.

CVE-2012-6537, Low

Information leak flaws in the XFRM implementation could allow a local user who has the CAP_NET_ADMIN capability to leak kernel stack memory to user-space.

CVE-2012-6546, Low

Two information leak flaws in the Asynchronous Transfer Mode (ATM) subsystem could allow a local, unprivileged user to leak kernel stack memory to user-space.

CVE-2012-6547, Low

An information leak was found in the TUN/TAP device driver in the networking implementation. A local user with access to a TUN/TAP virtual interface could use this flaw to leak kernel stack memory to user-space.

CVE-2013-0349, Low

An information leak in the Bluetooth implementation could allow a local user who has the CAP_NET_ADMIN capability to leak kernel stack memory to user-space.

CVE-2013-1767, Low

A use-after-free flaw was found in the tmpfs implementation. A local user able to mount and unmount a tmpfs file system could use this flaw to cause a denial of service or, potentially, escalate their privileges.

CVE-2013-1774, Low

A NULL pointer dereference was found in the Linux kernel's USB Inside Out Edgeport Serial Driver implementation. An attacker with physical access to a system could use this flaw to cause a denial of service.

Red Hat would like to thank Andrew Honig of Google for reporting CVE-2013-1796, CVE-2013-1797, and CVE-2013-1798. CVE-2013-1792 was discovered by Mateusz Guzik of Red Hat EMEA GSS SEG Team.

Bug Fixes

BZ#909156

When running the Hyper-V hypervisor, the host expects guest virtual machines to report free memory and the memory used for memory ballooning, including the pages that were ballooned out. However, the memory ballooning code did not handle reporting correctly, and the pages that were ballooned out were not included in the report. Consequently, after the memory was ballooned out from the guest, the Hyper-V Manager reported an incorrect value of the demanded memory and a memory status. This update provides a patch that adjusts the memory ballooning code to include the ballooned-out pages and to determine the demanded memory correctly.

BZ#911267

The Intel 5520 and 5500 chipsets do not properly handle remapping of MSI and MSI-X interrupts. If the interrupt remapping feature is enabled on the system with such a chipset, various problems and service disruption could occur (for example, a NIC could stop receiving frames), and the "kernel: do_IRQ: 7.71 No irq handler for vector (irq -1)" error message appears in the system logs. As a workaround to this problem, it has been recommended to disable the interrupt remapping feature in the BIOS on such systems, and many vendors have updated their BIOS to disable interrupt remapping by default. However, the problem is still being reported by users without proper BIOS level with this feature properly turned off. Therefore, this update modifies the kernel to check if the interrupt remapping feature is enabled on these systems and to provide users with a warning message advising them on turning off the feature and updating the BIOS.

BZ#911475

If a logical volume was created on devices with thin provisioning enabled, the mkfs.ext4 command took a long time to complete, and the following message was recorded in the system log:

```
kernel: blk: request botched
```

This was caused by discard request merging that was not completely functional in the block and SCSI layers. This functionality has been temporarily disabled to prevent such problems from occurring.

BZ#915579

Timeout errors could occur on an NFS client with heavy read workloads; for example when using the rsync and ldconfig utilities. Both, client-side and server-side causes were found for the problem. On the client side, problems that could prevent the client reconnecting lost TCP connections; this was fixed prior to this update. On the server side, TCP memory pressure on the server forced the send buffer size to be lower than the size required to send a single Remote Procedure Call (RPC), which consequently caused the server to be unable to reply to the client. A series of patches addressing the server-side problem has been applied. This update provides the last of those patches that removes the redundant xprt->shutdown bit field from the sunrpc code. Setting this bit field could lead to a race causing the aforementioned problem. Timeout errors no longer occur on NFS clients that are under heavy read workload.

BZ#915583

Previously, running commands such as "ls", "find" or "move" on a MultiVersion File System (MVFS) could cause a kernel panic. This happened because the d_validate() function, which is used for dentry validation, called the kmem_ptr_validate() function to validate a pointer to a parent dentry. The pointer could have been freed anytime so the kmem_ptr_validate() function could not guarantee the pointer to be dereferenced, which could lead to a NULL pointer derefence. This update modifies d_validate() to verify the parent-child relationship by traversing the parent dentry's list of child dentries, which solves this problem. The kernel no longer panics in the described scenario.

BZ#916957

A previous patch introduced the use of the page_descs length field to describe the size of a fuse request. That patch incorrectly handled a code path that does not exist in the upstream fuse code, which resulted in a data corruption when using loop devices over FUSE. This patch fixes this problem by setting the fuse request size before submitting the request.

BZ#917690

When the state of the netfilter module was out-of-sync, a TCP connection was recorded in the conntrack table although the TCP connection did not exist between two hosts. If a host re-established this connection with the same source, port, destination port, source address and destination address, the host sent a TCP SYN packet and the peer sent back acknowledgment for this SYN package. However, because netfilter was out-of-sync, netfilter dropped this acknowledgment, and deleted the connection item from the conntrack table, which consequently caused the host to retransmit the SYN packet. A patch has been applied to improve this handling; if an unexpected SYN packet appears, the TCP options are annotated. Acknowledgment for the SYN packet serves as a confirmation of the connection tracking being out-of-sync, then a new connection record is created using the information annotated previously to avoid the retransmission delay.

BZ#920266

The NFS code implements the "silly rename" operation to handle an open file that is held by a process while another process attempts to remove it. The "silly rename" operation works according to the "delete on last close" semantics so the inode of the file is not released until the last process that opens the file closes it. A previous update of the NFS code broke the mechanics that prevented an NFS client from deleting a silly-renamed dentry. This affected the "delete on last close" semantics and silly-renamed files could be deleted by any process while the files were open for I/O by another process. As a consequence, the process reading the file failed with the "ESTALE" error code. This update modifies the way how the NFS code handles dentries of silly-renamed files and silly-renamed files can not be deleted until the last process that has the file open for I/O closes it.

BZ#920268

The NFSv4 code uses byte range locks to simulate the flock() function, which is used to apply or remove an exclusive advisory lock on an open file. However, using the NFSv4 byte range locks precludes a possibility to open a file with read-only permissions and subsequently to apply an exclusive advisory lock on the file. A previous patch broke a mechanism used to verify the mode of the open file. As a consequence, the system became unresponsive and the system logs filled with a "kernel: nfs4_reclaim_open_state: Lock reclaim failed!" error message if the file was open with read-only permissions and an attempt to apply an exclusive advisory lock was made. This update modifies the NFSv4 code to check the mode of the open file before attempting to apply the exclusive advisory lock. The "-EBADF" error code is returned if the type of the lock does not match the file mode.

BZ#921145

Due to a bug in the tty driver, an ioctl call could return the "-EINTR" error code when the "read" command was interrupted by a signal, such as SIGCHLD. As a consequence, the subsequent"read" command caused the Bash shell to abort with a "double free or corruption (out)" error message. An applied patch corrects the tty driver to use the "-ERESTARTSYS" error code so the system call is restarted if needed. Bash no longer crashes in this scenario.

BZ#921150

Previously, the NFS Lock Manager (NLM) did not resend blocking lock requests after NFSv3 server reboot recovery. As a consequence, when an application was running on a NFSv3 mount and requested a blocking lock, the application received an -ENOLCK error. This patch ensures that NLM always resend blocking lock requests after the grace period has expired.

BZ#921535

Virtual LAN (VLAN) support of the eHEA ethernet adapter did not work as expected. A "device ethX has buggy VLAN hw accel" message could have been reported when running the "dmesg" command. This was because a backported upstream patch removed the vlan_rx_register() function. This update adds the function back, and eHEA VLAN support works as expected. This update also addresses a possible kernel panic, which could occur due to a NULL pointer dereference when processing received VLAN packets. The patch adds a test condition verifying whether a VLAN group is set by the network stack, which prevents a possible NULL pointer to be dereferenced, and the kernel no longer crashes in this situation.

BZ#921958

When the Active Item List (AIL) becomes empty, the xfsaild daemon is moved to a task sleep state that depends on the timeout value returned by the xfsaild_push() function. The latest changes modified xfsaild_push() to return a 10-ms value when the AIL is empty, which sets xfsaild into the uninterruptible sleep state (D state) and artificially increased system load average. This update applies a patch that fixes this problem by setting the timeout value to the allowed maximum, 50 ms. This moves xfsaild to the interruptible sleep state (S state), avoiding the impact on load average.

BZ#921961

When running a high thread workload of small-sized files on an XFS file system, sometimes, the system could become unresponsive or a kernel panic could occur. This occurred because the xfsaild daemon had a subtle code path that led to lock recursion on the xfsaild lock when a buffer in the AIL was already locked and an attempt was made to force the log to unlock it. This patch removes the dangerous code path and queues the log force to be invoked from a safe locking context with respect to xfsaild. This patch also fixes the race condition between buffer locking and buffer pinned state that exposed the original problem by rechecking the state of the buffer after a lock failure. The system no longer hangs and the kernel no longer panics in this scenario.

BZ#921963

The kernel's implementation of RTAS (RunTime Abstraction Services) previously allowed the stop_topology_update() function to be called from an interrupt context during live partition migration on PowerPC and IMB System p machines. As a consequence, the system became unresponsive.

This update fixes the problem by calling stop_topology_update() earlier in the migration process, and the system no longer hangs in this situation.

BZ#922154

A previous kernel update broke queue pair (qp) hash list deletion in the qp_remove() function. This could cause a general protection fault in the InfiniBand stack or QLogic InfiniBand driver. A patch has been applied to restore the former behavior so the general protection fault no longer occurs.

BZ#923098

Due to a bug in the CIFS mount code, it was not possible to mount Distributed File System (DFS) shares in Red Hat Enterprise Linux 6.4. This update applies a series of patches that address this problem and modifies the CIFS mount code so that DFS shares can now be mounted as expected.

BZ#923204

When the Red Hat Enterprise Linux 6 kernel runs as a virtual machine, it performs boot-time detection of the hypervisor in order to enable hypervisor-specific optimizations. Red Hat Enterprise Linux 6.4 introduces detection and optimization for the Microsoft Hyper-V hypervisor. Previously Hyper-V was detected first, however, because some Xen hypervisors can attempt to emulate Hyper-V, this could lead to a boot failure when that emulation was not exact. A patch has been applied to ensure that the attempt to detect Xen is always done before Hyper-V, resolving this issue.

BZ#927309

When using the congestion window lock functionality of the ip utility, the system could become unresponsive. This happened because the tcp_slow_start() function could enter an infinite loop if the congestion window was locked using route metrics. A set of patches has been applied to comply with the upstream kernel, ensuring the problem no longer occurs in this scenario.

BZ#928686

Previously, the tty driver allowed a race condition to occur in the tty buffer code. If the tty buffer was requested by multiple users of the same tty device in the same time frame, the same tty's buffer structure was used and the buffer could exceed the reserved size. This resulted in a buffer overflow problem and a subsequent memory corruption issue, which caused the kernel to panic. This update fixes the problem by implementing a locking mechanism around the tty buffer structure using spin locks. The described race can no longer occur so the kernel can no longer crash due to a tty buffer overflow.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

7.103.10. RHSA-2013:0630 — Important: kernel security and bug fix update

Updated kernel packages that fix two security issues and several bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2013-0228, Important

A flaw was found in the way the xen_iret() function in the Linux kernel used the DS (the CPU's Data Segment) register. A local, unprivileged user in a 32-bit para-virtualized guest could use this flaw to crash the guest or, potentially, escalate their privileges.

CVE-2013-0268, Important

A flaw was found in the way file permission checks for the "/dev/cpu/[x]/msr" files were performed in restricted root environments (for example, using a capability-based security model). A local user with the ability to write to these files could use this flaw to escalate their privileges to kernel level, for example, by writing to the SYSENTER_EIP_MSR register.

The CVE-2013-0228 issue was discovered by Andrew Jones of Red Hat.

Bug Fixes

BZ#908398

Truncating files on a GFS2 file system could fail with an "unable to handle kernel NULL pointer dereference" error. This was because of a missing reservation structure that caused the truncate code to reference an incorrect pointer. To prevent this, a patch has been applied to allocate a block reservation structure before truncating a file.

BZ#908733

Previously, when using parallel network file system (pNFS) and data was written to the appropriate storage device, the LAYOUTCOMMIT requests being sent to the metadata server could fail internally. The metadata server was not provided with the modified layout based on the written data, and these changes were not visible to the NFS client. This happened because the encoding functions for the LAYOUTCOMMIT and LAYOUTRETURN operations were defined as void, and returned thus an arbitrary status. This update corrects these encoding functions to return 0 on success as expected. The changes on the storage device are now propagated to the metadata server and can be observed as expected.

BZ#908737

Previously, init scripts were unable to set the MAC address of the master interface properly because it was overwritten by the first slave MAC address. To avoid this problem, this update re-introduces the check for an unassigned MAC address before setting the MAC address of the first slave interface as the MAC address of the master interface.

BZ#908739

During device discovery, the system creates a temporary SCSI device with the LUN ID 0 if the LUN 0 is not mapped on the system. Previously, this led to a NULL pointer dereference because inquiry data was not allocated for the temporary LUN 0 device, which resulted in a kernel panic. This update adds a NULL pointer test in the underlying SCSI code, and the kernel no longer panics in this scenario.

BZ#908744

Previously on system boot, devices with associated Reserved Memory Region Reporting (RMRR) information had lost their RMRR information after they were removed from the static identity (SI) domain. Consequently, a system unexpectedly terminated in an endless loop due to unexpected NMIs triggered by DMA errors. This problem was observed on HP ProLiant Generation 7 (G7) and 8 (G8) systems. This update prevents non-USB devices that have RMRR information associated with them from being placed into the SI domain during system boot. HP ProLiant G7 and G8 systems that contain devices with the RMRR information now boot as expected.

BZ#908794

When counting CPU time, the utime and stime values are scaled based on rtime. Prior to this update, the utime value was multiplied with the rtime value, but the integer multiplication overflow could happen, and the resulting value could be then truncated to 64 bits. As a consequence, utime values visible in the user space were stall even if an application consumed a lot of CPU time. With this update, the multiplication is performed on stime instead of utime. This significantly reduces the chances of an overflow on most workloads because the stime value, unlike the utime value, cannot grow fast.

BZ#909159

When using transparent proxy (TProxy) over IPv6, the kernel previously created neighbor entries for local interfaces and peers that were not reachable directly. This update corrects this problem and the kernel no longer creates invalid neighbor entries.

BZ#909813

Due to a bug in the superblock code, a NULL pointer could be dereferenced when handling a kernel paging request. Consequently, the request failed and a kernel oops occurred. This update corrects this problem and kernel page requests are processed as expected.

BZ#909814

Sometimes, the irqbalance tool could not get the CPU NUMA node information due to missing symlinks for CPU devices in sysfs. This update adds the NUMA node symlinks for CPU devices in sysfs, which is also useful when using irqbalance to build a CPU topology.

BZ#909815

A previous kernel patch introduced a bug by assigning a different value to the IFLA_EXT_MASK Netlink attribute than found in the upstream kernels. This could have caused various problems; for example, a binary compiled against the upstream kernel headers could have failed or behaved unexpectedly on Red Hat Enterprise Linux 6.4 and later kernels. This update realigns IFLA_EXT_MASK in the enumeration correctly by synchronizing the IFLA_* enumeration with the upstream. This ensures that binaries compiled against Red Hat Enterprise Linux 6.4 kernel headers will function as expected. Backwards compatibility is guaranteed.

BZ#909816

Broadcom 5719 NIC could previously sometimes drop received jumbo frame packets due to cyclic redundancy check (CRC) errors. This update modifies the tg3 driver so that CRC errors no longer occur and Broadcom 5719 NICs process jumbo frame packets as expected.

BZ#909818

Previously, the VLAN code incorrectly cleared the timestamping interrupt bit for network devices using the igb driver. Consequently, timestamping failed on the igb network devices with Precision Time Protocol (PTP) support. This update modifies the igb driver to preserve the interrupt bit if interrupts are disabled.

BZ#910370

The NFSv4.1 client could stop responding while recovering from a server reboot on an NFSv4.1 or pNFS mount with delegations disabled. This could happen due to insufficient locking in the NFS code and several related bugs in the NFS and RPC scheduler code which could trigger a deadlock situation. This update applies a series of patches which prevent possible deadlock situations from occurring. The NFSv4.1 client now recovers and continue with workload as expected in the described situation.

BZ#910373

Previously, race conditions could sometimes occur in interrupt handling on the Emulex BladeEngine 2 (BE2) controllers, causing the network adapter to become unresponsive. This update provides a series of patches for the be2net driver, which prevents the race from occurring. The network cards using BE2 chipsets no longer hang due to incorrectly handled interrupt events.

BZ#910998

A previous patch to the mlx4 driver enabled an internal loopback to allow communication between functions on the same host. However, this change introduced a regression that caused virtual switch (vSwitch) bridge devices using Mellanox Ethernet adapter as the uplink to become inoperative in native (non-SRIOV) mode under certain circumstances. To fix this problem, the destination MAC address is written to Tx descriptors of transmitted packets only in SRIOV or eSwitch mode, or during the device self-test. Uplink traffic works as expected in the described setup.

BZ#911000

Previously, the kernel did not support a storage discard granularity that was not a power of two. Consequently, if the underlying storage reported such a granularity, the kernel issued discard requests incorrectly, which resulted in I/O errors. This update modifies the kernel to correct calculation of the storage discard granularity and the kernel now process discard requests correctly even for storage devices with the discard granularity that is not power of two.

BZ#911655

Previously, a kernel panic could occur on machines using the SCSI sd driver with Data Integrity Field (DIF) type 2 protection. This was because the scsi_register_driver() function registered a prep_fn() function that might have needed to use the sd_cdp_pool variable for the DIF functionality. However, the variable had not yet been initialized at this point. The underlying code has been updated so that the driver is registered last, which prevents a kernel panic from occurring in this scenario.

BZ#911663

Previously, the mlx4 driver set the number of requested MSI-X vectors to 2 under multi-function mode on mlx4 cards. However, the default setting of the mlx4 firmware allows for a higher number of requested MSI-X vectors (4 of them with the current firmware). This update modifies the mlx4 driver so that it uses these default firmware settings, which improves performance of mlx4 cards.

All users should upgrade to these updated packages, which contain backported patches to correct these issues and fix the bugs. The system must be rebooted for this update to take effect.

7.103.11. RHSA-2013:0496 — Important: Red Hat Enterprise Linux 6 kernel security, bug fix, and enhancement update

Updated kernel packages that fix two security issues, address several hundred bugs and add numerous enhancements are now available as part of the ongoing support and maintenance of Red Hat Enterprise Linux version 6. This is the fourth regular update.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2012-4508, Important

A race condition was found in the way asynchronous I/O and fallocate() interacted when using the ext4 file system. A local, unprivileged user could use this flaw to expose random data from an extent whose data blocks have not yet been written, and thus contain data from a deleted file.

CVE-2013-0311, Important

A flaw was found in the way the vhost kernel module handled descriptors that spanned multiple regions. A privileged guest user in a KVM guest could use this flaw to crash the host or, potentially, escalate their privileges on the host.

CVE-2012-4542, Moderate

It was found that the default SCSI command filter does not accommodate commands that overlap across device classes. A privileged guest user could potentially use this flaw to write arbitrary data to a LUN that is passed-through as read-only.

CVE-2013-0190, Moderate

A flaw was found in the way the xen_failsafe_callback() function in the Linux kernel handled the failed iret (interrupt return) instruction notification from the Xen hypervisor. An unprivileged user in a 32-bit para-virtualized guest could use this flaw to crash the guest.

CVE-2013-0309, Moderate

A flaw was found in the way pmd_present() interacted with PROT_NONE memory ranges when transparent hugepages were in use. A local, unprivileged user could use this flaw to crash the system.

CVE-2013-0310, Moderate

A flaw was found in the way CIPSO (Common IP Security Option) IP options were validated when set from user mode. A local user able to set CIPSO IP options on the socket could use this flaw to crash the system.

Red Hat would like to thank Theodore Ts'o for reporting CVE-2012-4508, and Andrew Cooper of Citrix for reporting CVE-2013-0190. Upstream acknowledges Dmitry Monakhov as the original reporter of CVE-2012-4508. The CVE-2012-4542 issue was discovered by Paolo Bonzini of Red Hat.

Bug Fixes

BZ#807385

Suspending a system (mode S3) running on a HP Z1 All-in-one Workstation with an internal Embedded DisplayPort (eDP) panel and an external DisplayPort (DP) monitor, and, consequently, waking up the system caused the backlight of the eDP panel to not be re-enabled. To fix this issue, the code that handles suspending in the i915 module has been modified to write the BLC_PWM_CPU_CTL parameter using the I915_WRITE function after writing the BLC_PWM_CPU_CTL2 parameter.

BZ#891839

Prior to this update, when a VLAN device was set up on a qlge interface, running the TCP Stream Performance test using the netperf utility to test TCP/IPv6 traffic caused the kernel to produce warning messages that impacted the overall performance. This was due to an unsupported feature (NETIF_F_IPV6_CSUM) which was enabled via the NETIF_F_TSO6 flag. This update removes the NETIF_F_TSO6 flag from qlge code and TCP/IPv6 traffic performance is no longer impacted.

BZ#876912

The isci driver copied the result of a "Register Device to Host" frame into the wrong buffer causing the SATA DOWNLOAD MICROCODE command to fail, preventing the download of hard drive firmware. This bug in the frame handler routine caused a timeout, resulting in a reset. With this update, the underlying source code has been modified to address this issue, and the isci driver successfully completes SATA DOWNLOAD MICROCODE commands as expected.

BZ#813677

In the xHCI code, due to a descriptor that incorrectly pointed at the USB 3.0 register instead of USB 2.0 registers, kernel panic could occur when more USB 2.0 registers were available than USB 3.0 registers. This update fixes the descriptor to point at the USB 2.0 registers, and kernel panic no longer occurs in the aforementioned case.

BZ#879509

When the "perf script --gen-script" command was called with a perf.data file which contained no tracepoint events, the command terminated unexpectedly with a segmentation fault due to a NULL "pevent" pointer. With this update, the underlying source code has been modified to address this issue, and the aforementioned command no longer crashes.

BZ#885030

Running the mq_notify/5-1 test case from the Open POSIX test suite resulted in corrupted memory, later followed by various kernel crash/BUG messages. This update addresses the mq_send/receive memory corruption issue in the inter-process communication code, and the aforementioned test case no longer fails.

BZ#841983

Bond masters and slaves now have separate VLAN groups. As such, if a slave device incurred a network event that resulted in a failover, the VLAN device could process this event erroneously. With this update, when a VLAN is attached to a master device, it ignores events generated by slave devices so that the VLANs do not go down until the bond master does.

BZ#836748

Previously in the kernel, when the leap second hrtimer was started, it was possible that the kernel livelocked on the xtime_lock variable. This update fixes the problem by using a mixture of separate subsystem locks (timekeeping and ntp) and removing the xtime_lock variable, thus avoiding the livelock scenarios that could occur in the kernel.

BZ#836803

After the leap second was inserted, applications calling system calls that used futexes consumed almost 100% of available CPU time. This occurred because the kernel's timekeeping structure update did not properly update these futexes. The futexes repeatedly expired, re-armed, and then expired immediately again. This update fixes the problem by properly updating the futex expiration times by calling the clock_was_set_delayed() function, an interrupt-safe method of the clock_was_set() function.

BZ#822691

When the Fibre Channel (FC) layer sets a device to "running", the layer also scans for other new devices. Previously, there was a race condition between these two operations. Consequently, for certain targets, thousands of invalid devices were created by the SCSI layer and the udev service. This update ensures that the FC layer always sets a device to "online" before scanning for others, thus fixing this bug.

BZ#845135

Certain disk device arrays report a medium error without returning any data. This was not being handled correctly in cases where low level device drivers were not setting the optional residual field, however, most modern low level drivers do set it. This update correctly handles cases where low level drivers do not set the residual field in the upper level sd driver, avoiding the potential data corruption.

BZ#890454

This update reverts a previously-applied patch that caused the qla2xxx driver to not be able to load on an IBM POWER 7 7895-81X system. This patch has also been isolated as the cause of Dynamic Logical Partitioning (DLPAR) memory remove failures on 2 adapters.

BZ#841149

Previous update changed the /proc/stat code to use the get_cpu_idle_time_us() and get_cpu_iowait_time_us() macros if dynamic ticks are enabled in the kernel. This could lead to problems on IBM System z architecture that defines the arch_idle_time() macro. For example, executing the "vmstat" command could fail with "Floating point exception" followed by a core dump. The underlying source code has been modified so that the arch_idle_time() macro is used for idle and iowait times, which prevents the mentioned problem.

BZ#809792

The Stream Control Transmission Protocol (SCTP) process became unresponsive inside the sctp_wait_for_sndbuf() function when the sender exhausted the send buffer and waited indefinitely to be woken up. This was because twice the amount of data was accounted for during a packet transmission, once when constructing the packet and the second time when transmitting it. Thus, the available memory resources were used up too early, causing a deadlock. With this update, only a single byte is reserved to ensure the socket stays alive for the life time of the packet, and the SCTP process no longer hangs.

BZ#852847

If there are no active threads using a semaphore, blocked threads should be unblocked. Previously, the R/W semaphore code looked for a semaphore counter as a whole to reach zero - which is incorrect because at least one thread is usually queued on the semaphore and the counter is marked to reflect this. As a consequence, the system could become unresponsive when an application used direct I/O on the XFS file system. With this update, only the count of active semaphores is checked, thus preventing the hang in this scenario.

BZ#861164

When performing PCI device assignment on AMD systems, a virtual machine using the assigned device could not be able to boot, as the device had failed the assignment, leaving the device in an unusable state. This was due to an improper range check that omitted the last PCI device in a PCI subsystem or tree. The check has been fixed to include the full range of PCI devices in a PCI subsystem or tree. This bug fix avoids boot failures of a virtual machine when the last device in a PCI subsystem is assigned to a virtual machine on an AMD host system.

BZ#859533

The mlx4 driver must program the mlx4 card so that it is able to resolve which MAC addresses to listen to, including multicast addresses. Therefore, the mlx4 card keeps a list of trusted MAC addresses. The driver used to perform updates to this list on the card by emptying the entire list and then programming in all of the addresses. Thus, whenever a user added or removed a multicast address or put the card into or out of promiscuous mode, the card's entire address list was re-written. This introduced a race condition, which resulted in a packet loss if a packet came in on an address the card should be listening to, but had not yet been reprogrammed to listen to. With this update, the driver no longer rewrites the entire list of trusted MAC addresses on the card but maintains a list of addresses that are currently programmed into the card. On address addition, only the new address is added to the end of the list, and on removal, only the to-be-removed address is removed from the list. The mlx4 card no longer experiences the described race condition and packets are no longer dropped in this scenario.

BZ#858850

Filesystem in Userspace (FUSE) did not implement scatter-gather direct I/O optimally. Consequently, the kernel had to process an extensive number of FUSE requests, which had a negative impact on system performance. This update applies a set of patches which improves internal request management for other features, such as readahead. FUSE direct I/O overhead has been significantly reduced to minimize negative effects on system performance.

BZ#865637

A previous kernel update introduced a bug that caused RAID0 and linear arrays larger than 4 TB to be truncated to 4 TB when using 0.90 metadata. The underlying source code has been modified so that 0.90 RAID0 and linear arrays larger than 4 TB are no longer truncated in the md RAID layer.

BZ#865682

A larger command descriptor block (CDB) is allocated for devices using Data Integrity Field (DIF) type 2 protection. The CDB was being freed in the sd_done() function, which resulted in a kernel panic if the command had to be retried in certain error recovery cases. With this update, the larger CDB is now freed in the sd_unprep_fn() function instead. This prevents the kernel panic from occurring.

BZ#857518

Previously, a use-after-free bug in the usbhid code caused a NULL pointer dereference. Consequent kernel memory corruption resulted in a kernel panic and could cause data loss. This update adds a NULL check to avoid these problems.

BZ#856325

A race condition could occur between page table sharing and virtual memory area (VMA) teardown. As a consequence, multiple "bad pmd" message warnings were displayed and "kernel BUG at mm/filemap.c:129" was reported while shutting down applications that share memory segments backed by huge pages. With this update, the VM_MAYSHARE flag is explicitly cleaned during the unmap_hugepage_range() call under the i_mmap_lock. This makes VMA ineligible for sharing and avoids the race condition. After using shared segments backed by huge pages, applications like databases and caches shut down correctly, with no crash.

BZ#855984

When I/O is issued through blk_execute_rq(), the blk_execute_rq_nowait() routine is called to perform various tasks. At first, the routine checks for a dead queue. Previously, however, if a dead queue was detected, the blk_execute_rq_nowait() function did not invoke the done() callback function. This resulted in blk_execute_rq() being unresponsive when waiting for completion, which had never been issued. To avoid such hangs, the rq->end_io pointer is initialized to the done() callback before the queue state is verified.

BZ#855759

The Stream Control Transmission Protocol (SCTP) ipv6 source address selection logic did not take the preferred source address into consideration. With this update, the source address is chosen from the routing table by taking this aspect into consideration. This brings the SCTP source address selection on par with IPv4.

BZ#855139

Under certain circumstances, a system crash could result in data loss on XFS file systems. If files were created immediately before the file system was left to idle for a long period of time and then the system crashed, those files could appear as zero-length once the file system was remounted. This occurred even if a sync or fsync was run on the files. This was because XFS was not correctly idling the journal, and therefore it incorrectly replayed the inode allocation transactions upon mounting after the system crash, which zeroed the file size. This problem has been fixed by re-instating the periodic journal idling logic to ensure that all metadata is flushed within 30 seconds of modification, and the journal is updated to prevent incorrect recovery operations from occurring.

BZ#854376

Mellanox hardware keeps a separate list of Ethernet hardware addresses it listens to depending on whether the Ethernet hardware address is unicast or multicast. Previously, the mlx4 driver was incorrectly adding multicast addresses to the unicast list. This caused unstable behavior in terms of whether or not the hardware would have actually listened to the addresses requested. This update fixes the problem by always putting multicast addresses on the multicast list and vice versa.

BZ#854140

Previously, the kernel had no way to distinguish between a device I/O failure due to a transport problem and a failure as a result of command timeout expiration. I/O errors always resulted in a device being set offline and the device had to be brought online manually even though the I/O failure occured due to a transport problem. With this update, the SCSI driver has been modified and a new SDEV_TRANSPORT_OFFLINE state has been added to help distinguish transport problems from another I/O failure causes. Transport errors are now handled differently and storage devices can now recover from these failures without user intervention.

BZ#854053

In a previous release of Red Hat Enterprise Linux, the new Mellanox packet steering architecture had been intentionally left out of the Red Hat kernel. With Red Hat Enterprise Linux 6.4, the new Mellanox packet steering architecture was merged into Red Hat Mellanox driver. One merge detail was missing, and as a result, the multicast promiscuous flag on an interface was not checked during an interface reset to see if the flag was on prior to the reset and should be re-enabled after the reset. This update fixes the problem, so if an adapter is reset and the multicast promiscuous flag was set prior to the reset, the flag is now still set after the reset.

BZ#854052

On dual port Mellanox hardware, the mlx4 driver was adding promiscuous mode to the correct port, but when attempting to remove promiscuous mode from a port, it always tried to remove it from port one. It was therefore impossible to remove promiscuous mode from the second port, and promiscuous mode was incorrectly removed from port one even if it was not intended. With this update, the driver now properly attempts to remove promiscuous mode from port two when needed.

BZ#853007

The kernel provided by the Red Hat Enterprise Linux 6.3 release included an unintentional kernel ABI (kABI) breakage with regards to the "contig_page_data" symbol. Unfortunately, this breakage did not cause the checksums to change. As a result, drivers using this symbol could silently corrupt memory on the kernel. This update reverts the previous behavior.

BZ#852148

In case of a regular CPU hot plug event, the kernel does not keep the original cpuset configuration and can reallocate running tasks to active CPUs. Previously, the kernel treated switching between suspend and resume modes as a regular CPU hot plug event, which could have a significant negative impact on system performance in certain environments such as SMP KVM virtualization. When resuming an SMP KVM guest from suspend mode, the libvirtd daemon and all its child processes were pinned to a single CPU (the boot CPU) so that all VMs used only the single CPU. This update applies a set of patches which ensure that the kernel does not modify cpusets during suspend and resume operations. The system is now resumed in the exact state before suspending without any performance decrease.

BZ#851118

Prior to this update, it was not possible to set IPv6 source addresses in routes as it was possible with IPv4. With this update, users can select the preferred source address for a specific IPv6 route with the "src" option of the "ip -6 route" command.

BZ#849702

Previously, when a server attempted to shut down a socket, the svc_tcp_sendto() function set the XPT_CLOSE variable if the entire reply failed to be transmitted. However, before XPT_CLOSE could be acted upon, other threads could send further replies before the socket was really shut down. Consequently, data corruption could occur in the RPC record marker. With this update, send operations on a closed socket are stopped immediately, thus preventing this bug.

BZ#849188

The usb_device_read() routine used the bus->root_hub pointer to determine whether or not the root hub was registered. However, this test was invalid because the pointer was set before the root hub was registered and remained set even after the root hub was unregistered and deallocated. As a result, the usb_device_read() routine accessed freed memory, causing a kernel panic; for example, on USB device removal. With this update, the hcs->rh_registered flag - which is set and cleared at the appropriate times - is used in the test, and the kernel panic no longer occurs in this scenario.

BZ#894344

BE family hardware could falsely indicate an unrecoverable error (UE) on certain platforms and stop further access to be2net-based network interface cards (NICs). A patch has been applied to disable the code that stops further access to hardware for BE family network interface cards (NICs). For a real UE, it is not necessary as the corresponding hardware block is not accessible in this situation.

BZ#847838

Previously, a race condition existed whereby device open could race with device removal (for example when hot-removing a storage device), potentially leading to a kernel panic. This was due a use-after-free error in the block device open patch, which has been corrected by not referencing the "disk" pointer after it has been passed to the module_put() function.

BZ#869750

The hugetlbfs file system implementation was missing a proper lock protection of enqueued huge pages at the gather_surplus_pages() function. Consequently, the hstate.hugepages_freelist list became corrupted, which caused a kernel panic. This update adjusts the code so that the used spinlock protection now assures atomicity and safety of enqueued huge pages when handling hstate.hugepages_freelist. The kernel no longer panics in this scenario.

BZ#847310

An unnecessary check for the RXCW.CW bit could cause the Intel e1000e NIC (Network Interface Controller) to not work properly. The check has been removed so that the Intel e1000e NIC now works as expected.

BZ#846585

If a mirror or redirection action is configured to cause packets to go to another device, the classifier holds a reference count. However, it was previously assuming that the administrator cleaned up all redirections before removing. Packets were therefore dropped if the mirrored device was not present, and connectivity to the host could be lost. To prevent such problems, a notifier and cleanup are now run during the unregister action. Packets are not dropped if the a mirrored device is not present.

BZ#846419

Previously, the MultiTech MT9234MU USB serial device was not supported by version 0.9 of the it_usb_3410_5052 kernel module. With this update, the MultiTech MT9234MU USB serial device is supported by this version.

BZ#846024

Previously, the I/O watchdog feature was disabled when Intel Enhanced Host Controller Interface (EHCI) devices were detected. This could cause incorrect detection of USB devices upon addition or removal. Also, in some cases, even though such devices were detected properly, they were non-functional. The I/O watchdog feature can now be enabled on the kernel command line, which improves hardware detection on underlying systems.

BZ#845347

A kernel panic could occur when using the be2net driver. This was because the Bottom Half (BF) was enabled even if the Interrupt ReQuest (IRQ) was already disabled. With this update, the BF is disabled in callers of the be_process_mcc() function and the kernel no longer crashes in this scenario. Note that, in certain cases, it is possible to experience the network card being unresponsive after installing this update. A future update will correct this problem.

BZ#844814

This issue affects O_DSYNC performance on GFS2 when only data (and not metadata such as file size) has been dirtied as the result of a write system call. Prior to this patch, O_DSYNC writes were behaving in the same way as O_SYNC for all cases. After this patch, O_DSYNC writes will only write back data, if the inode's metadata is not dirty. This gives a considerable performance improvement for this specific case. Note that the issue does not affect data integrity. The same issue also applies to the pairing of write and fdatasync calls.

BZ#844531

Previously, a cgroup or its hierarchy could only be modified under the cgroup_mutex master lock. This introduced a locking dependency on cred_guard_mutex from cgroup_mutex and completed a circular dependency, which involved cgroup_mutex, namespace_sem and workqueue, and led to a deadlock. As a consequence, many processes were unresponsive, and the system could be eventually unusable. This update introduces a new mutex, cgroup_root_mutex, which protects cgroup root modifications and is now used by mount options readers instead of the master lock. This breaks the circular dependency and avoids the deadlock.

BZ#843771

On architectures with the 64-bit cputime_t type, it was possible to trigger the "divide by zero" error, namely, on long-lived processes. A patch has been applied to address this problem, and the "divide by zero" error no longer occurs under these circumstances.

BZ#843541

The kernel allows high priority real time tasks, such as tasks scheduled with the SCHED_FIFO policy, to be throttled. Previously, the CPU stop tasks were scheduled as high priority real time tasks and could be thus throttled accordingly. However, the replenishment timer, which is responsible for clearing a throttle flag on tasks, could be pending on the just disabled CPU. This could lead to a situation that the throttled tasks were never scheduled to run. Consequently, if any of such tasks was needed to complete the CPU disabling, the system became unresponsive. This update introduces a new scheduler class, which gives a task the highest possible system priority and such a task cannot be throttled. The stop-task scheduling class is now used for the CPU stop tasks, and the system shutdown completes as expected in the scenario described.

BZ#843163

The previous implementation of socket buffers (SKBs) allocation for a NIC was node-aware, that is, memory was allocated on the node closest to the NIC. This increased performance of the system because all DMA transfer was handled locally. This was a good solution for networks with a lower frame transmitting rate where CPUs of the local node handled all the traffic of the single NIC well. However, when using 10Gb Ethernet devices, CPUs of one node usually do not handle all the traffic of a single NIC efficiently enough. Therefore, system performance was poor even though the DMA transfer was handled by the node local to the NIC. This update modifies the kernel to allow SKBs to be allocated on a node that runs applications receiving the traffic. This ensures that the NIC's traffic is handled by as many CPUs as needed, and since SKBs are accessed very frequently after allocation, the kernel can now operate much more efficiently even though the DMA can be transferred cross-node.

BZ#872813

Bug 768304 introduced a deadlock on the super block umount mutex. Consequently, when two processes attempted to mount an NFS file system at the same time they would block. This was because a backport mistake with one of the patches of bug 768304, which resulted in an imbalance between the mutex aquires and releases. Rather than just fix the imbalance, an upstream patch that the problem patch depended on was identified and backported so that the kernel code then matched the upstream code. The deadlock no longer occurs in this scenario.

BZ#842881

A kernel oops could occur due to a NULL pointer dereference upon USB device removal. The NULL pointer dereference has been fixed and the kernel no longer crashes in this scenario.

BZ#842435

When an NFSv4 client received a read delegation, a race between the OPEN and DELEGRETURN operation could occur. If the DELEGRETURN operation was processed first, the NFSv4 client treated the delegation returned by the following OPEN as a new delegation. Also, the NFSv4 client did not correctly handle errors caused by requests that used a bad or revoked delegation state ID. As a result, applications running on the client could receive spurious EIO errors. This update applies a series of patches that fix the NFSv4 code so an NFSv4 client recovers correctly in the described situations instead of returning errors to applications.

BZ#842312

Due to a missing return statement, the nfs_attr_use_mounted_on_file() function returned a wrong value. As a consequence, redundant ESTALE errors could potentially be returned. This update adds the proper return statement to nfs_attr_use_mounted_on_file(), thus preventing this bug. Note that this bug only affects NFSv4 file systems.

BZ#841987

Previously, soft interrupt requests (IRQs) under the bond_alb_xmit() function were locked even when the function contained soft IRQs that were disabled. This could cause a system to become unresponsive or terminate unexpectedly. With this update, such IRQs are no longer disabled, and the system no longer hangs or crashes in this scenario.

BZ#873949

Previously, the IP over Infiniband (IPoIB) driver maintained state information about neighbors on the network by attaching it to the core network's neighbor structure. However, due to a race condition between the freeing of the core network neighbor struct and the freeing of the IPoIB network struct, a use after free condition could happen, resulting in either a kernel oops or 4 or 8 bytes of kernel memory being zeroed when it was not supposed to be. These patches decouple the IPoIB neighbor struct from the core networking stack's neighbor struct so that there is no race between the freeing of one and the freeing of the other.

BZ#874322

Previously, XFS could, under certain circumstances, incorrectly read metadata from the journal during XFS log recovery. As a consequence, XFS log recovery terminated with an error message and prevented the file system from being mounted. This problem could result in a loss of data if the user forcibly "zeroed" the log to allow the file system to be mounted. This update ensures that metadata is read correctly from the log so that journal recovery completes successfully and the file system mounts as expected.

BZ#748827

If a dirty GFS2 inode was being deleted but was in use by another node, its metadata was not written out before GFS2 checked for dirty buffers in the gfs2_ail_flush() function. GFS2 was relying on the inode_go_sync() function to write out the metadata when the other node tried to free the file. However, this never happened because GFS2 failed the error check. With this update, the inode is written out before calling the gfs2_ail_flush() function. If a process has the PF_MEMALLOC flag set, it does not start a new transaction to update the access time when it writes out the inode. The inode is marked as dirty to make sure that the access time is updated later unless the inode is being freed.

BZ#839973

A USB Human Interface Device (HID) can be disconnected at any time. If this happened right before or while the hiddev_ioctl() call was in progress, hiddev_ioctl() attempted to access the invalid hiddev->hid pointer. When the HID device was disconnected, the hiddev_disconnect() function called the hid_device_release() function, which frees the hid_device structure type, but did not set the hiddev->hid pointer to NULL. If the deallocated memory region was re-used by the kernel, a kernel panic or memory corruption could occur. The hiddev->exist flag is now checked while holding the existancelock and hid_device is used only if such a device exists. As a result, the kernel no longer crashes in this scenario.

BZ#839311

The CONFIG_CFG80211_WEXT configuration option previously defined in the KConfig of the ipw2200 driver was removed with a recent update. This led to a build failure of the driver. The driver no longer depends on the CONFIG_CFG80211_WEXT option, so it can build successfully.

BZ#875036

The mmap_rnd() function is expected to return a value in the [0x00000000 .. 0x000FF000] range on 32-bit x86 systems. This behavior is used to randomize the base load address of shared libraries by a bug fix resolving the CVE-2012-1568 issue. However, due to a signedness bug, the mmap_rnd() function could return values outside of the intended scope. Consequently, the shared libraries base address could be less than one megabyte. This could cause binaries that use the MAP_FIXED mappings in the first megabyte of the process address space (typically, programs using vm86 functionality) to work incorrectly. This update modifies the mmap_rnd() function to no longer cast values returned by the get_random_int() function to the long data type. The aforementioned binaries now work correctly in this scenario.

BZ#837607

Due to an error in the dm-mirror driver, when using LVM mirrors on disks with discard support (typically SSD disks), repairing such disks caused the system to terminate unexpectedly. The error in the driver has been fixed and repairing disks with discard support is now successful.

BZ#837230

During the update of the be2net driver between the Red Hat Enterprise Linux 6.1 and 6.2, the NETIF_F_GRO flag was incorrectly removed, and the GRO (Generic Receive Offload) feature was therefore disabled by default. In OpenVZ kernels based on Red Hat Enterprise Linux 6.2, this led to a significant traffic decrease. To prevent this problem, the NETIF_F_GRO flag has been included in the underlying source code.

BZ#875091

Previously, the HP Smart Array driver (hpsa) used the target reset functionality. However, HP Smart Array logical drives do not support the target reset functionality. Therefore, if the target reset failed, the logical drive was taken offline with a file system error. The hpsa driver has been updated to use the LUN reset functionality instead of target reset, which is supported by these drives.

BZ#765665

A possible race between the n_tty_read() and reset_buffer_flags() functions could result in a NULL pointer dereference in the n_tty_read() function under certain circumstances. As a consequence, a kernel panic could have been triggered when interrupting a current task on a serial console. This update modifies the tty driver to use a spin lock to prevent functions from a parallel access to variables. A NULL pointer dereference causing a kernel panic can no longer occur in this scenario.

BZ#769045

Traffic to the NFS server could trigger a kernel oops in the svc_tcp_clear_pages() function. The source code has been modified, and the kernel oops no longer occurs in this scenario.

BZ#836164

Previously, reference counting was imbalanced in the slave add and remove paths for bonding. If a network interface controller (NIC) did not support the NETIF_F_HW_VLAN_FILTER flag, the bond_add_vlans_on_slave() and bond_del_vlans_on_slave() functions did not work properly, which could lead to a kernel panic if the VLAN module was removed while running. The underlying source code for adding and removing a slave and a VLAN has been revised and now also contains a common path, so that kernel crashes no kernel no longer occur in the described scenario.

BZ#834764

The bonding method for adding VLAN Identifiers (VIDs) did not always add the VID to a slave VLAN group. When the NETIF_F_HW_VLAN_FILTER flag was not set on a slave, the bonding module could not add new VIDs to it. This could cause networking problems and the system to be unreachable even if NIC messages did not indicate any problems. This update changes the bond VID add path to always add a new VID to the slaves (if the VID does not exist). This ensures that networking problems no longer occur in this scenario.

BZ#783322

Previously, after a crash, preparing to switch to the kdump kernel could in rare cases race with IRQ migration, causing a deadlock of the ioapic_lock variable. As a consequence, kdump became unresponsive. The race condition has been fixed, and switching to kdump no longer causes hangs in this scenario.

BZ#834038

Previously, futex operations on read-only (RO) memory maps did not work correctly. This broke workloads that had one or more reader processes performing the FUTEX_WAIT operation on a futex within a read-only shared file mapping and a writer process that had a writable mapping performing the FUTEX_WAKE operation. With this update, the FUTEX_WAKE operation is performed with a RO MAP_PRIVATE mapping, and is successfully awaken if another process updates the region of the underlying mapped file.

BZ#833098

When a device was registered to a bus, a race condition could occur between the device being added to the list of devices of the bus and binding the device to a driver. As a result, the device could already be bound to a driver which led to a warning and incorrect reference counting, and consequently to a kernel panic on device removal. To avoid the race condition, this update adds a check to identify an already bound device.

BZ#832135

Sometimes, the crypto allocation code could become unresponsive for 60 seconds or multiples thereof due to an incorrect notification mechanism. This could cause applications, like openswan, to become unresponsive. The notification mechanism has been improved to avoid such hangs.

BZ#832009

When a device is added to the system at runtime, the AMD IOMMU driver initializes the necessary data structures to handle translation for it. Previously, however, the per-device dma_ops structure types were not changed to point to the AMD IOMMU driver, so mapping was not performed and direct memory access (DMA) ended with the IO_PAGE_FAULT message. This consequently led to networking problems. With this update, the structure types point correctly to the AMD IOMMU driver, and networking works as expected when the AMD IOMMU driver is used.

BZ#830716

It is possible to receive data on multiple transports. Previously, however, data could be selectively acknowledged (SACKed) on a transport that had never received any data. This was against the SHOULD requirement in section 6.4 of the RFC 2960 standard. To comply with this standard, bundling of SACK operations is restricted to only those transports which have moved the ctsn of the association forward since the last sack. As a result, only outbound SACKs on a transport that has received a chunk since the last SACK are bundled.

BZ#830209

On ext4 file systems, when fallocate() failed to allocate blocks due to the ENOSPC condition (no space left on device) for a file larger than 4 GB, the size of the file became corrupted and, consequently, caused file system corruption. This was due to a missing cast operator in the "ext4_fallocate()" function. With this update, the underlying source code has been modified to address this issue, and file system corruption no longer occurs.

BZ#829739

Previously, on Fibre Channel hosts using the QLogic QLA2xxx driver, users could encounter error messages and long I/O outages during fabric faults. This was because the number of outstanding requests was hard-coded. With this update, the number of outstanding requests the driver keeps track of is based on the available resources instead of being hard-coded, which avoids the aforementioned problems.

BZ#829211

Previously introduced firmware files required for new Realtek chipsets contained an invalid prefix ("rtl_nic_") in the file names, for example "/lib/firmware/rtl_nic/rtl_nic_rtl8168d-1.fw". This update corrects these file names. For example, the aforementioned file is now correctly named "/lib/firmware/rtl_nic/rtl8168d-1.fw".

BZ#829149

Due to insufficient handling of a dead Input/Output Controller (IOC), the mpt2sas driver could fail Enhanced I/O Error Handling (EEH) recovery for certain PCI bus failures on 64-bit IBM PowerPC machines. With this update, when a dead IOC is detected, EEH recovery routine has more time to resolve the failure and the controller in a non-operational state is removed.

BZ#828271

USB Request Blocks (URBs) coming from user space were not allowed to have transfer buffers larger than an arbitrary maximum. This could lead to various problems; for example, attempting to redirect certain USB mass-storage devices could fail. To avoid such problems, programs are now allowed to submit URBs of any size; if there is not sufficient contiguous memory available, the submission fails with an ENOMEM error. In addition, to prevent programs from submitting a lot of small URBs and so using all the DMA-able kernel memory, this update also replaces the old limits on individual transfer buffers with a single global limit of 16MB on the total amount of memory in use by USB file system (usbfs).

BZ#828065

A race condition could occur due to incorrect locking scheme in the code for software RAID. Consequently, this could cause the mkfs utility to become unresponsive when creating an ext4 file system on software RAID5. This update introduces a locking scheme in the handle_stripe() function, which ensures that the race condition no longer occurs.

BZ#826375

Previously, using the e1000e driver could lead to a kernel panic. This was caused by a NULL pointer dereference that occurred if the adapter was being closed and reset simultaneously. The source code of the driver has been modified to address this problem, and kernel no longer crashes in this scenario.

BZ#878204

When a new rpc_task is created, the code takes a reference to rpc_cred and sets the task->tk_cred pointer to it. After the call completes, the resources held by the rpc_task are freed. Previously, however, after the rpc_cred was released, the pointer to it was not zeroed out. This led to an rpc_cred reference count underflow, and consequently to a kernel panic. With this update, the pointer to rpc_cred is correctly zeroed out, which prevents a kernel panic from occurring in this scenario.

BZ#823822

When removing a bonding module, the bonding driver uses code separate from the net device operations to clean up the VLAN code. Recent changes to the kernel introduced a bug which caused a kernel panic if the vlan module was removed after the bonding module had been removed. To fix this problem, the VLAN group removal operations found in the bonding kill_vid path are now duplicated in alternate paths which are used when removing a bonding module.

BZ#823371

When TCP segment offloading (TSO) or jumbo packets are used on the Broadcom BCM5719 network interface controller (NIC) with multiple TX rings, small packets can be starved for resources by the simple round-robin hardware scheduling of these TX rings, thus causing lower network performance. To ensure reasonable network performance for all NICs, multiple TX rings are now disabled by default.

BZ#822651

Previously, the default minimum entitled capacity of a virtual processor was 10%. This update changes the PowerPC architecture vector to support a lower minimum virtual processor capacity of 1%.

BZ#821374

On PowerPC architecture, the "top" utility displayed incorrect values for the CPU idle time, delays and workload. This was caused by a previous update that used jiffies for the I/O wait and idle time, but the change did not take into account that jiffies and CPU time are represented by different units. These differences are now taken into account, and the "top" utility displays correct values on PowerPC architecture.

BZ#818172

A bug in the writeback livelock avoidance scheme could result in some dirty data not being written to disk during a sync operation. In particular, this could occasionally occur at unmount time, when previously written file data was not synced, and was unavailable after the file system was remounted. Patches have been applied to address this issue, and all dirty file data is now synced to disk at unmount time.

BZ#807704

Previously, the TCP socket bound to NFS server contained a stale skb_hints socket buffer. Consequently, kernel could terminate unexpectedly. A patch has been provided to address this issue and skb_hints is now properly cleared from the socket, thus preventing this bug.

BZ#814877

Previously, bnx2x devices did not disable links with a large number of RX errors and overruns, and such links could still be detected as active. This prevented the bonding driver from failing over to a working link. This update restores remote-fault detection, which periodically checks for remote faults on the MAC layer. In case the physical link appears to be up but an error occurs, the link is disabled. Once the error is cleared, the link is brought up again.

BZ#813137

Various race conditions that led to indefinite log reservation hangs due to xfsaild "idle" mode occurred in XFS file system. This could lead to certain tasks being unresponsive; for example, the cp utility could become unresponsive on heavy workload. This update improves the Active Item List (AIL) pushing logic in xfsaild. Also, the log reservation algorithm and interactions with xfsaild have been improved. As a result, the aforementioned problems no longer occur in this scenario.

BZ#811255

The Out of Memory (OOM) killer killed processes outside of a memory cgroup when one or more processes inside that memory cgroup exceeded the "memory.limit_in_bytes" value. This was because when a copy-on-write fault happened on a Transparent Huge Page (THP), the 2 MB THP caused the cgroup to exceed the memory.limit_in_bytes value but the individual 4 KB page was not exceeded. With this update, the 2 MB THP is correctly split into 4 KB pages when the memory.limit_in_bytes value is exceeded. The OOM kill is delivered within the memory cgroup; tasks outside the memory cgroups are no longer killed by the OOM killer.

BZ#812904

This update blacklists the ADMA428M revision of the 2GB ATA Flash Disk device. This is due to data corruption occurring on the said device when the Ultra-DMA 66 transfer mode is used. When the "libata.force=5:pio0,6:pio0" kernel parameter is set, the aforementioned device works as expected.

BZ#814044

With certain switch peers and firmware, excessive link flaps could occur due to the way DCBX (Data Center Bridging Exchange) was handled. To prevent link flaps, changes were made to examine the capabilities in more detail and only initialize hardware if the capabilities have changed.

BZ#865115

If an abort request times out to the virtual Fibre Channel adapter, the ibmvfc driver initiates a reset of the adapter. Previously, however, the ibmvfc driver incorrectly returned success to the eh_abort handler and then sent a response to the same command, which led to a kernel oops on IBM System p machines. This update ensures that both the abort request and the request being aborted are completed prior to exiting the en_abort handler, and the kernel oops no longer occurs in this scenario.

BZ#855906

A kernel panic occurred when the size of a block device was changed and an I/O operation was issued at the same time. This was because the direct and non-direct I/O code was written with the assumption that the block size would not change. This update introduces a new read-write lock, bd_block_size_semaphore. The lock is taken for read during I/O operations and for write when changing the block size of a device. As a result, block size cannot be changed while I/O is being submitted. This prevents the kernel from crashing in the described scenario.

BZ#883643

The bonding driver previously did not honor the maximum Generic Segmentation Offload (GSO) length of packets and segments requested by the underlying network interface. This caused the firmware of the underlying NIC, such as be2net, to become unresponsive. This update modifies the bonding driver to set up the lowest gso_max_size and gso_max_segs values of network devices while attaching and detaching the devices as slaves. The network drivers no longer hangs and network traffic now proceeds as expected in setups using a bonding interface.

BZ#855131

In Fibre Channel fabrics with large zones, the automatic port rescan on incoming Extended Link Service (ELS) frames and any adapter recovery could cause high traffic, in particular if many Linux instances shared a host bus adapter (HBA), which is common on IBM System z architecture. This could lead to various failures; for example, names server requests, port or adapter recovery could fail. With this update, ports are re-scanned only when setting an adapter online or on manual user-triggered writes to the sysfs attribute "port_rescan".

BZ#824964

A deadlock sometimes occurred between the dlm_controld daemon closing a lowcomms connection through the configfs file system and the dlm_send process looking up the address for a new connection in configfs. With this update, the node addresses are saved within the lowcomms code so that the lowcomms work queue does not need to use configfs to get a node address.

BZ#827031

On Intel systems with Pause Loop Exiting (PLE), or AMD systems with Pause Filtering (PF), it was possible for larger multi-CPU KVM guests to experience slowdowns and soft lock-ups. Due to a boundary condition in kvm_vcpu_on_spin, all the VCPUs could try to yield to VCPU0, causing contention on the run queue lock of the physical CPU where the guest's VCPU0 is running. This update eliminates the boundary condition in kvm_vcpu_on_spin.

BZ#796352

On Red Hat Enterprise Linux 6, mounting an NFS export from a Windows 2012 server failed due to the fact that the Windows server contains support for the minor version 1 (v4.1) of the NFS version 4 protocol only, along with support for versions 2 and 3. The lack of the minor version 0 (v4.0) support caused Red Hat Enterprise Linux 6 clients to fail instead of rolling back to version 3 as expected. This update fixes this bug and mounting an NFS export works as expected.

BZ#832575

Previously, the size of the multicast IGMP (Internet Group Management Protocol) snooping hash table for a bridge was limited to 256 entries even though the maximum is 512. This was due to the hash table size being incorrectly compared to the maximum hash table size, hash_max, and the following message could have been produced by the kernel:

```
Multicast hash table maximum reached, disabling snooping: vnet1, 512
```

With this update, the hash table value is correctly compared to the hash_max value, and the error message no longer occurs under these circumstances.

BZ#834185

The xmit packet size was previously 64K, exceeding the hardware capability of the be2net card because the size did not account for the Ethernet header. The adapter was therefore unable to process xmit requests exceeding this size, produced error messages and could become unresponsive. To prevent these problems, GSO (Generic Segmentation Offload) maximum size has been reduced to account for the Ethernet header.

BZ#835797

Signed-unsigned values comparison could under certain circumstances lead to a superfluous reshed_task() routine to be called, causing several unnecessary cycles in the scheduler. This problem has been fixed, preventing the unnecessary cycles in the scheduler.

BZ#838025

When using virtualization with the netconsole module configured over the main system bridge, guests could not be added to the bridge, because TAP interfaces did not support netpoll. This update adds support of netpoll to the TUN/TAP interfaces so that bridge devices in virtualization setups can use netconsole.

BZ#838640

In the ext4 file system, splitting an unwritten extent while using Direct I/O could fail to mark the modified extent as dirty, resulting in multiple extents claiming to map the same block. This could lead to the kernel or fsck reporting errors due to multiply claimed blocks being detected in certain inodes. In the ext4_split_unwritten_extents() function used for Direct I/O, the buffer which contains the modified extent is now properly marked as dirty in all cases. Errors due to multiply claimed blocks in inodes should no longer occur for applications using Direct I/O.

BZ#839266

When the netconsole module was configured over bridge and the "service network restart" command was executed, a deadlock could occur, resulting in a kernel panic. This was caused by recursive rtnl locking by both bridge and netconsole code during network interface unregistration. With this update, the rtnl lock usage is fixed, and the kernel no longer crashes in this scenario.

BZ#756044

Migrating virtual machines from Intel hosts that supported the VMX "Unrestricted Guest" feature to older hosts without this feature could result in kvm returning the "unhandled exit 80000021" error for guests in real mode. The underlying source code has been modified so that migration completes successfully on hosts where "Unrestricted Guest" is disabled or not supported.

BZ#843849

The kernel contains a rule to blacklist direct memory access (DMA) modes for "2GB ATA Flash Disk" devices. However, this device ID string did not contain a space at the beginning of the name. Due to this, the rule failed to match the device and failed to disable DMA modes. With this update, the string correctly reads " 2GB ATA Flash Disk", and the rule can be matched as expected.

Enhancements

NOTE

For more information on the most important of the Red Hat Enterprise Linux 6.4 kernel enhancements, refer to the *Kernel* chapter in the Red Hat Enterprise Linux 6.4 Release Notes or Chapter 2, *Device Drivers*.

For a summary of added or updated **procfs** entries, **sysfs** default values, boot parameters, kernel configuration options, or any noticeable behavior changes, refer to Chapter 1, *Important Changes to External Kernel Parameters*.

BZ#872799

The INET socket interface has been modified to send a warning message when the ip_options structure is allocated directly by a third-party module using the kmalloc() function.

BZ#823010

The z90crypt device driver has been updated to support the new Crypto Express 4 (CEX4) adapter card.

BZ#586028

This update adds the ability to use InfiniBand's Queue Pair (QP) interface under KVM. The QP interface can be exported to a KVM guest.

BZ#795598

With this update, it possible to adjust the TCP initial receive window, using the "initrwnd" iproute setting, on a per-route basis.

BZ#831623

A new "route_localnet" interface option has been added, which enables routing of addresses within the 127.0.0.0/8 block.

BZ#847998

With this update, a warning message is logged when a storage device reports a certain SCSI Unit Attention code.

Users should upgrade to these updated packages, which contain backported patches to correct these issues, fix these bugs, and add these enhancement. The system must be rebooted for this update to take effect.

7.103.12. RHSA-2013:0830 — Important: kernel security update

Updated kernel packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix

CVE-2013-2094, Important

It was found that the Red Hat Enterprise Linux 6.1 kernel update (RHSA-2011:0542) introduced an integer conversion issue in the Linux kernel's Performance Events implementation. This led to a user-supplied index into the perf_swevent_enabled array not being validated properly, resulting in out-of-bounds kernel memory access. A local, unprivileged user could use this flaw to escalate their privileges.

A public exploit that affects Red Hat Enterprise Linux 6 is available.

Refer to Red Hat Knowledge Solution 373743 for further information and mitigation instructions for users who are unable to immediately apply this update.

Users should upgrade to these updated packages, which contain a backported patch to correct this issue. The system must be rebooted for this update to take effect.

7.103.13. RHSA-2013:0567 — Important: kernel security update

Updated kernel packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix

CVE-2013-0871, Important

A race condition was found in the way the Linux kernel's ptrace implementation handled PTRACE_SETREGS requests when the debuggee was woken due to a SIGKILL signal instead of being stopped. A local, unprivileged user could use this flaw to escalate their privileges.

Users should upgrade to these updated packages, which contain a backported patch to correct this issue. The system must be rebooted for this update to take effect.

7.103.14. RHBA-2013:0093 — kernel bug fix update

Updated kernel packages that fix several bugs are now available for Red Hat Enterprise Linux 6.4 Extended Update Support.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Bug Fixes

BZ#1012275

A bug in the kernel's memory management code allowed the callback routine to call the **`find_vma()`** function without acquiring the memory map semaphore when reading from the **`/proc/<pid>/pagemap`** file. This could trigger a kernel panic or lead to another system failure. A set of patches has been applied to address this problem so that memory map semaphore is now held when walking through the memory page map. Moreover, this update fix a bug that allowed exceeding of the page mid-level directory (PMD) boundary between memory pages, which could cause various problems. The memory management code now handles reading of memory page map as expected.

BZ#1021813

As a result of a recent fix preventing a deadlock upon an attempt to cover an active **`XFS`** log, the behavior of the **`xfs_log_need_covered()`** function has changed. However, **`xfs_log_need_covered()`** is also called to ensure that the **`XFS`** log tail is correctly updated as a part of the **`XFS`** journal sync operation. As a consequence, when shutting down an **`XFS`** file system, the sync operation failed and some files might have been lost. A patch has been applied to ensure that the tail of the XFS log is updated by logging a dummy record to the **`XFS`** journal. The sync operation completes successfully and files are properly written to the disk in this situation.

BZ#1026622

When the Wacom Intuous 4 tablet was attached to the system using GNOME, and writing to the LED control occurred before the input device was opened, a bug that set the tablet to an incorrect mode could have been triggered. Consequently, after hot plugging the tablet or logging into the system, the Wacom Intuous 4 tablet could stop functioning correctly and was no longer detected by the Wacom control panel. A patch has been applied to fix this problem by correctly marking get requests as input requests in the **`wacom_get_report()`** function. The Wacom Intuous 4 tablets now work as expected in the described scenario.

BZ#1028171

A change introduced in an earlier kernel version caused the **`d_mountpoint()`** function to return a different value than before, although the semantics of the function stayed the same. Consequently, certain third-party kernel modules, such as the Veritas file system (**`VxFS`**) module, could stop working properly. A patch has been applied, ensuring that the **`d_mountpoint()`** function returns expected values.

BZ#1029091

The stripe_width is the stripe device length divided by the number of stripes. However, previously, the stripe_width was not being calculated properly. As a consequence, device topologies that had previously worked correctly with the stripe target were no longer considered valid. In particular, there was a higher risk of encountering this problem if one of the stripe devices had a 4K logical block size. As a result, the following error message could be displayed:

```
device-mapper: table: 253:4: len=21845 not aligned to h/w logical block
size 4096 of dm-1
```

This update fixes the stripe_width calculation error, and device topologies work as expected in this scenario.

BZ#1029425

The kernel's thread helper previously used larvals of the request threads without holding a reference count. This could result in a NULL pointer dereference and a subsequent kernel panic if the helper thread completed after the larval had been destroyed upon the request thread exiting. With this update, the helper thread holds a reference count on the request threads larvals so that a NULL pointer dereference is now avoided.

BZ#1029731

When printing information about SCSI devices on systems with a very large number (more than about 1600) of SCSI devices, intermittent page allocation errors occurred, and the **`cat /proc/scsi/scsi`** command failed with an ENOMEM error. This was caused by the show routine that iterated over all SCSI devices and attempted to dump information about all of them into the buffer at the same time. This update modifies the SCSI driver to define its own seq_file operations to iterate over the SCSI devices. As a result, each **`show()`** operation only dumps approximately 180 bytes into the buffer at a time, and the error no longer occurs.

BZ#1029860

Under high memory pressure, the **`shrink_zone()`** function could complete an iteration without reclaiming or even scanning any pages, in which case it should give up. The latter was detected by comparing the sc->nr_scanned pointer against a snapshot taken at the start of **`shrink_zone()`**, instead of at the start of the iteration. This meant **`shrink_zone()`** could enter an indefinite loop if it scanned some pages in one iteration, but failed on subsequent iterations due to memory pressure. A patch has been applied to fix this bug, preventing the indefinite loop.

BZ#1029904

Due to a bug in the SELinux Makefile, a kernel compilation could fail when the **`-j`** option was specified to perform the compilation with multiple parallel jobs. This happened because SELinux expected the existence of an automatically generated file, **`flask.h`**, prior to the compiling of some dependent files. The Makefile has been corrected and the **`flask.h`** dependency now applies to all objects from the **`selinux-y`** list. The parallel compilation of the kernel now succeeds as expected.

BZ#1030169

A previous change in the NFSv4 code resulted in breaking the sync NFSv4 mount option. A patch has been applied that restores functionality of the sync mount option.

BZ#1032160

When performing I/O operations on a heavily-fragmented **`GFS2`** file system, significant performance degradation could occur. This was caused by the allocation strategy that GFS2 used to search for an ideal contiguous chunk of free blocks in all the available resource groups. A series of patches has been applied that improves performance of GFS2 file systems in case of heavy fragmentation. GFS2 now allocates the biggest extent found in the resource groups if it fulfills the minimum requirements. GFS2 has also reduced the amount of bitmap searching in case of multi-block reservations by keeping track of the smallest extent for which the multi-block reservation would fail in the given resource groups. This improves GFS2 performance by avoiding unnecessary resource groups free block searches that would fail. Additionally, this patch series fixes a bug in the GFS2 block allocation code where a multi-block reservation was not properly removed from the resource groups' reservation tree when it was disqualified, which eventually triggered a BUG_ON() macro due to an incorrect count of reserved blocks.

BZ#1032165

An earlier patch to the kernel added the dynamic queue depth throttling functionality to the QLogic's qla2xxx driver that allowed the driver to adjust queue depth for attached SCSI devices. However, the kernel might have crashed when having this functionality enabled in certain environments, such as on systems with EMC PowerPath Multipathing installed that were under heavy I/O load. To resolve this problem, the dynamic queue depth throttling functionality has been removed from the qla2xxx driver.

BZ#1032248

As a result of a recent fix preventing a deadlock upon an attempt to cover an active **`XFS`** log, the behavior of the **`xfs_log_need_covered()`** function has changed. However, **`xfs_log_need_covered()`** is also called to ensure that the XFS log tail is correctly updated as a part of the XFS journal sync operation. As a consequence, when shutting down an XFS file system, the sync operation failed and some files might have been lost. A patch has been applied to ensure that the tail of the XFS log is updated by logging a dummy record to the XFS journal. The sync operation completes successfully and files are properly written to the disk in this situation.

BZ#1032394

Due to a bug in the mlx4 driver, Mellanox Ethernet cards were brought down unexpectedly while adjusting their Transmission (Tx) or Reception (Rx) ring. A patch has been applied so that the mlx4 driver now properly verifies the state of the Ethernet card when the coalescing of the Tx or Rx ring is being set, which resolves this problem.

BZ#1036775

During the probe operations on the Broadcom 5717 and later devices, the tg3 driver was incorrectly switching the devices to a low-power mode. Consequently, some ports on the certain device slots were not recognized. With this update, the tg3 driver no longer resumes a low-power mode when probing the aforementioned devices.

BZ#1038934

Certain storage device or storage environment failures could cause all SCSI commands and task management functions that were sent to a SCSI target to time out, without any other indication of an error. As a consequence, the Linux SCSI error handling code stopped issuing any I/O operations on the entire host bus adapter (HBA) until the recovery operations completed. Additionally, when using DM Multipath, I/O operations did not fail over to a working path in this situation. To resolve this problem, a new **`sysfs`** parameter, ***`eh_deadline`***, has been added to the SCSI host object. This parameter allows to set the maximum amount of time for which the SCSI error handling attempts to perform error recovery before resetting the entire HBA adapter. This timeout is disabled by default. The default value of this timeout can be reset for all SCSI HBA adapters on the system using the ***`eh_deadline`*** parameter. The described scenario no longer occurs if ***`eh_deadline`*** is properly used.

BZ#1040825

Due to several bugs in the IPv6 code, a soft lockup could occur when the number of cached IPv6 destination entries reached the garbage collector treshold on a high-traffic router. A series of patches has been applied to address this problem. These patches ensure that the route probing is performed asynchronously to prevent a dead lock with garbage collection. Also, the garbage collector is now run asynchronously, preventing CPUs that concurrently requested the garbage collector from waiting until all other CPUs finish the garbage collection. As a result, soft lockups no longer occur in the described situation.

BZ#1042733

The RPC client always retransmitted zero-copy of the page data if it timed out before the first RPC transmission completed. However, such a retransmission could cause data corruption if using the O_DIRECT buffer and the first RPC call completed while the respective TCP socket still held a reference to the pages. To prevent the data corruption, retransmission of the RPC call is, in this situation, performed using the **`sendmsg()`** function. The **`sendmsg()`** function retransmits an authentic reproduction of the first RPC transmission because the TCP socket holds the full copy of the page data.

Users of kernel are advised to upgrade to these updated packages, which fix these bugs. The system must be rebooted for this update to take effect.

7.104. KEXEC-TOOLS

7.104.1. RHBA-2013:0281 — kexec-tools bug fix and enhancement update

Updated kexec-tools packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The kexec fastboot mechanism allows booting a Linux kernel from the context of an already running kernel. The kexec-tools package provides the **`/sbin/kexec`** binary and ancillary utilities that form the user-space component of the kernel's kexec feature.

Bug Fixes

BZ#628610

When starting the kdump service, kdump always verifies the following vendor model attributes on the present block devices: "/sys/block/vda/device/model", "/sys/block/vda/device/rev" and "/sys/block/vda/device/type". However, the virtio block devices do not provide these attributes to sysfs so if such a device was tested, the following error messages were displayed:

```
cat: /sys/block/vda/device/model: No such file or directory
cat: /sys/block/vda/device/type: No such file or directory
```

This update modifies the underlying code to restrain kdump from printing these error messages if a block device does not provide the aforementioned sysfs attributes.

BZ#770000

Previously, if memory ballooning was enabled in the first kernel, the virtio balloon driver was included in the kdump kernel, which led to extensive memory consumption. Consequently, kdump failed due to an out of memory (OOM) error and the vmcore file could not be saved. With this update, the virtio_balloon kernel module is no longer loaded in the second kernel so that an OOM failure no longer prevents kdump from capturing vmcore.

BZ#788253

Previously, the microde.ko module was included and loaded in the kdump kernel, however, related firmware was not included in the kdump initrd. As a consequence, the kdump kernel waited for 60-

second timeout to expire before loading the next module. This update modifies kdump to exclude the microcode driver from the second kernel so that the kdump kernel no longer waits unnecessarily and loads kernel modules as expected.

BZ#813354

The kdump.conf(5) man page previously did not document what file system types are supported by kdump. The user could therefore attempt to specify an unsupported file-system-type option, such as "auto", in the kdump.conf file. This would result in a failure to start the kdump service while the user expected success. With this update, all supported file system types are clearly listed in the kdump.conf(5) man page.

BZ#816467

When configuring kdump to dump a core file to a remote target over SSH without requiring a password, the "service kdump propagate" command has to be executed to generate and propagate SSH keys to the target system. This action required SELinux to be switched from enforcing mode to permissive mode and back. Previously, kdump init script used an incorrect test condition to determine SELinux mode so that SELinux mode could not be switched as required. Consequently, if SELinux was in enforcing mode, SSH keys could not be generated and kdump failed to start. This update removes the code used to switch between permissive and enforcing modes, which is no longer required because with Red Hat Enterprise Linux 6.3 SELinux added a policy allowing applications to access the ssh-keygen utility to generate SSH keys. SSH keys can now be generated and propagated as expected, and kdump no longer fails to start in this scenario.

BZ#818645

When dumping a core file on IBM System z architecture using the line mode terminals, kdump displays its progress on these terminals. However, these terminals do not support cursor positioning so that formatting of the kdump output was incorrect and the output was hard to read. With this update, a new environment variable, TERM, has been introduced to correct this problem. If "TERM=dumb" is set, the makedumpfile utility produces an easily-readable output on the line mode terminals.

BZ#820474

Previously, kdump expected that the generic ATA driver was always loaded as the ata_generic.ko kernel module and the mkdumprd utility thus added the module explicitly. However, the ata_generic.ko module does not exist on the IBM System z architecture and this assumption caused the kdump service to fail to start if the SCSI device was specified as a dump target on these machines. With this update, mkdumprd has been modified to load the ata_generic module only when required by the specific hardware. The kdump service now starts as expected on IBM System z architecture with SCSI device specified as a dump target.

BZ#821376

Previously, kdump always called the hwclock command to set the correct time zone. However, the Real Time Clock (RTC) interface, which is required by hwclock, is not available on IBM System z architecture. Therefore, running kdump on these machines resulted in the following error messages being emitted:

```
hwclock: can't open '/dev/misc/rtc': No such file or directory
```

With this update, kdump has been modified to no longer call the hwclock command when running on IBM System z, and the aforementioned error messages no longer occur.

BZ#825640

When dumping a core file to a remote target using SSH, kdump sends random seeds from the /dev/mem device to the /dev/random device to generate sufficient entropy required to establish successful SSH connection. However, when dumping a core file on the IBM System z with the CONFIG_STRICT_DEVMEM configuration option enabled, reading the /dev/mem was denied and the dump attempt failed with the following error:

```
dd: /dev/mem: Operation not permitted
```

With this update, kdump has been modified to reuse the /etc/random_seed file instead of reading /dev/mem. Dumping no longer fails and the core file can now be successfully dumped to a remote target using SSH.

BZ#842476

When booting to the kdump kernel and the local file system specified as the dump target was unmounted, the kernel module required for the respective file-system driver would not have to be included in dumprd. Consequently, kdump could not mount the dump device and failed to capture vmcore. With this update, mkdumprd has been modified to always install the required file system module when dumping a core file to the local file system. The vmcore file can be successfully captured in this scenario.

BZ#859824

When dumping a core file to a remote target using a bonded interface and the target was connected by other than the bond0 interface, kdump failed to dump the core file. This happened because a bonding driver in the kdump kernel creates only one bonding interface named bond0 by default. This update modifies kdump to use the correct bonding interface in the kdump init script so that a core file can be dumped as expected in this scenario.

BZ#870957

When dumping a core file to a SCSI device over Fibre Channel Protol (FCP) on IBM System z, the zFCP device has to be configured and set online before adding WWPN and SCSI LUN to the system. Previously, the mkdumprd utility parsed the zfcp.conf file incorrectly so that the zFCP device could not be set up and the kdump kernel became unresponsive during the boot. Consequently, kdump failed to dump a core file to the target SCSI device. With this update, mkdumprd has been modified to parse the zfcp.conf file correctly and kdump can now successfully dump a core file to the SCSI target on IBM System z. Also, mkdumprd previously always tried to set online Direct Access Storage Devices (DASD) on IBM System z. This resulted in the "hush: can't open '/sys/bus/ccw/devices//online': No such file or directory" error messages to be emitted when booting the kdump kernel in a SCSI-only environment. This update modifies mkdumprd to skip entries from the dasd.conf file if the Linux on IMB System z runs without DASD devices. The aforementioned error messages no longer occur during the kdump kernel boot in the SCSI-only environment on IBM System z.

BZ#872086

Previously, the kexec utility incorrectly recognized the Xen DomU (HVM) guest as the Xen Dom0 management domain. Consequently, the kernel terminated unexpectedly and the kdump utility generated the vmcore dump file with no NT_PRSTATUS notes. The crash also led to a NULL pointer dereference. With this update, kexec collects positions and sizes of NT_PRSTATUS from /sys/devices/system/cpu/cpuN/crash_notes on Xen DomU and from /proc/iomem on Xen Dom0. As a result, the crashes no longer occur.

BZ#874832

Due to recent changes, LVM assumes that the udev utility is always present on the system and creates correct device nodes and links. However, the kdump initramfs image does not contain udev so that LVM was unable to create disk devices and kdump failed. With this update, the mkdumprd utility modifies the lvm.conf configuration file to inform LVM that initramfs does not contain functional udev. If the lvm.conf file does not exist, mkdumprd creates it. The LVM now creates the devices correctly and kdump works as expected.

BZ#876891

Previously, the mlx4_core kernel module was loaded in the kdump kernel on systems using Mellanox ConnectX InfiniBand adapter cards. However, the mlx4_core module requires an extensive amount of memory, which caused these systems to run into an OOM situation and kdump failed. With this update, the second kernel no longer loads the mlx4_core module so that the OOM situation no longer occurs and kdump captures the vmcore file successfully in this scenario.

BZ#880040

Due to recent changes, the libdevmapper library assumes that the udev utility is always present on the system and creates correct device nodes for mulitpath devices. However, the kdump initramfs image does not contain udev therefore LVM was unable to create disk devices and kdump failed. With this update, the mkdumprd utility sets the DM_DISABLE_UDEV environment variable to 1 to inform libdevmapper that the initramfs image does not contain functional udev. The LVM now creates the devices correctly and kdump can successfully dump a core file to a multipath device.

BZ#892703

When setting up a network in the kdump kernel, the mkdumprd code incorrectly renamed network bridges along with NIC names in the network configuration files. This caused the kdump network setup to fail and the vmcore file could not be captured on the remote target. This update modifies kdump to substitute names of network devices correctly so that the network can be set up and vmcore dumped on the remote target as expected.

Enhancements

BZ#822146

With this update, the mkdumprd utility has been modified to support multipath storage devices as dump targets, which includes the ability to activate multiple NICs in the second kernel.

BZ#850623

This update modifies kdump to always extract the dmesg output from the captured vmcore dump file, and save the output in a separate text file before dumping the core file.

BZ#878200

The /usr/share/doc/kexec-tools-2.0.0/kexec-kdump-howto.txt file has been modified to provide a comprehensive list of supported, unsupported, and unknown dump targets under the “Dump Target support status” section.

Users of kexec-tools are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.105. KRB5

7.105.1. RHBA-2013:0319 — krb5 bug fix update

Updated krb5 packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third-party, the Key Distribution Center (KDC).

NOTE

The krb5 packages have been upgraded to upstream version 1.10.3, which provides a number of bug fixes over the previous version, including better support of cross-domain trust functionality in other packages. (BZ#823926)

Bug Fixes

BZ#771687

Older versions of the libsmbclient package incorrectly depended on the krb5_locate_kdc() function, which is no longer supported. Consequently, applications which used older versions of libsmbclient became incompatible after the Kerberos library update. With this update, an explicit conflict with older versions of libsmbclient has been added. As a result, an incompatible combination cannot be installed.

BZ#773496

Previously, when the krb5-auth-dialog application was used and the prompter was left hanging for a long period of time, a large clock skew was mistakenly recorded. This clock drift was applied in the next kinit session. Consequently, the klist function reported an incorrect expiration time. This bug has been fixed, and the spurious time offset no longer occurs in the described scenario.

BZ#834718

Previously, when a list of trusted roots of a PKINIT client included the KDC's certificates, certain KDC implementations omitted such anchors from the list of certificates in the signed data structure. Consequently, the client failed to verify the KDC's signature on the signed data. With this update, a backported fix has been included to allow the client to use its own copies of relevant certificates. As a result, the verification no longer fails in the aforementioned scenario.

BZ#837855

Prior to this update, attempts to use the kinit command with a keytab file often failed when the keytab file did not contain the Advanced Encryption Standard (AES) keys, but the client's libraries and the KDC both supported AES. The strongest supported encryption type (AES) was chosen by default, even though it was not present in keytab. Consequently, a mismatch error occurred. The bug has been fixed, and keytabs containing any of the supported encryption types are now correctly processed.

BZ#838548

Previously, the krb5 package did not handle the timeout variable properly. In certain cases, the timeout variable became a negative number. Consequently, the client entered a loop while checking for responses. With this update, the client logic has been modified and the described error no longer occurs.

BZ#839017

Prior to this update, the passwd utility failed when used by an Identity Management client. Consequently, an error occurred with the following message:

```
token manipulation error
```

The bug has been fixed, and the passwd utility now works with Identity Management as expected.

BZ#845125, BZ#846472

Due to a previous update to a locally-applied patch, files created by the libkrb5 library were given correct SELinux labels. However, each flushing of the replay cache caused the file context configuration to be reloaded to ensure that the correct label is applied to the newly-created replacement replay cache file. This resulted in large performance degradation in applications which accept authentication and use replay caches. With this update, the context configuration is only loaded when the context configuration file has been modified and the configuration is now freed only when the library is unloaded or the calling application exits, thus greatly lowering the impact of this problem.

All users of krb5 are advised to upgrade to these updated packages, which fix these bugs.

7.106. KSH

7.106.1. RHBA-2013:0430 — ksh bug fix and enhancement update

Updated ksh packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language which is also compatible with sh, the original Bourne Shell.

Bug Fixes

BZ#827512

Originally, ksh buffered output of a subshell, flushing it when the subshell completed. This slowed certain processes that waited for a particular output, because they had to wait for the subshell to complete. Moreover, it made it difficult to determine the order of events. The new version of ksh flushes output of the subshell every time the subshell executes a new command. Thanks to this change, processes waiting for the subshell output receive their data after every subshell command and the order of events is preserved.

BZ#846663

Previously, the sfprints() function was unsafe to be called during the shell initialization, which could corrupt the memory. Consequently, assigning a right-aligned variable to a smaller size could result in inappropriate output format. With this update, the sfprints() call is no longer used in the described scenario, which fixes the format of the output.

BZ#846678

Due to a bug in the typeset command, when executed with the -Z option, output was being formatted to an incorrect width. As a result, exporting a right-aligned variable of a smaller size than the predefined field size caused it to not be prepended with the "0" character. A patch has been provided and the typeset command now works as expected in the aforementioned scenario.

Enhancement

BZ#869155

With this update, ksh has been enhanced to support logging of the shell output.

Users of ksh are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.107. LEDMON

7.107.1. RHBA-2013:0479 — ledmon bug fix and enhancement update

Updated ledmon packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The ledmon and ledctl are user space applications designed to control LEDs associated with each slot in an enclosure or a drive bay. There are two types of system: 2-LED system (Activity LED, Status LED) and 3-LED system (Activity LED, Locate LED, Fail LED). User must have root privileges to use this application.

NOTE

The ledmon package has been upgraded to upstream version 0.72., which provides a number of bug fixes and enhancements over the previous version. (BZ#817974)

Users of ledmon are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.108. LIBBURN

7.108.1. RHBA-2012:1273 — libburn bug fix update

Updated libburn packages that fix one bug are now available for Red Hat Enterprise Linux 6.

problem description Libburn is an open-source library for reading, mastering and writing optical discs. For now this means only CD-R and CD-RW.

BZ#822906

Prior to this update, libburn library contained the "burn_write_close_track" command, which was redundant and not fully supported by all burning drives. As a consequence, the burning process CD-R or CD-RW could log errors while closing a track after the burning process, even if the data was written correctly. This update removes this redundant call.

All users of gfs-kmod are advised to upgrade to these updated packages, which fix this bug.

7.109. LIBCGROUP

7.109.1. RHBA-2013:0452 — libcgroup bug fix and enhancement update

Updated libcgroup packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The libcgroup packages provide tools and libraries to control and monitor control groups.

Bug Fixes

BZ#773544

Previously, the cgrulesengd daemon ignored the "--sticky" option of the cgexec command and, as a consequence, moved a process to another cgroup when the process called the setuid() or setgid() functions even if the process had to be stuck to the current cgroup. This bug is now fixed and the cgrulesengd daemon now checks whether the process is "sticky" or not when the process calls setuid or setgid.

BZ#819137

Previously, the lscgroup command dropped the first character of a path unless prefixed with a slash, which led to lscgroup generating invalid paths. This bug is now fixed and the generated paths are now correct.

BZ#849757

Previously, adding a cgroup after the cgrulesengd daemon had started did not work. As a consequence, if a directory was created after cgrulesengd was already started, any /etc/cgrules.conf configuration for that directory would not be processed. With this update, a routine has been added to scan the cgrules.conf file and move matching running tasks in the /proc/pid/ directory into configured cgroups. This new routine is called at init time and also after inotify events on cgroups. With this update, a routine has been added to scan the cgrules.conf file and move matching running tasks into configured cgroups.

BZ#869990

Previously, the cgconfig service was not working properly with read-only file systems. As a consequence, cgconfig was not able to start with the default configuration on a Red Hat Enterprise Virtualization Hypervisor system. This update adds a check for the read-only file systems to the cgconfig service and it now works as expected with the default configuration on Red Hat Enterprise Virtualization Hypervisor systems.

Enhancement

BZ#738737

This update improves the logging facility and error messages generated by libcgroup.

Users of libcgroup are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.110. LIBDBI

7.110.1. RHBA-2013:0326 — libdbi bug fix update

Updated libdbi packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The libdbi packages provide implementation of a database-independent abstraction layer in the C language. This framework allows programmers to write one generic set of code that works with multiple databases and multiple simultaneous database connections.

Bug Fix

BZ#733413

Previously, when processing query results, the last row of a query result was not freed due to an off-by-one logic error. This resulted in a memory leak that could become significant after processing a large number of query results. This update corrects an incorrect test condition in the underlying source code and memory leaks no longer occur in this scenario.

All users of libdbi are advised to upgrade to these updated packages, which fix this bug.

7.111. LIBDVDREAD

7.111.1. RHBA-2012:1247 — libdvdread bug fix update

Updated libdvdread packages that fix one bug is now available for Red Hat Enterprise Linux 6.

The libdvdread packages contain a simple foundation to read DVD video disks. This provides the functionality that is required to access many DVDs.

Bug Fix

BZ#842016

Prior to this update, the dvd_stat_t structure was not public. As a consequence, source code that required such structures could not be compiled. This update makes the dvd_stat_t structure public, to allow compiling code with of this type.

All users of libdvdread are advised to upgrade to these updated packages, which fix this bug.

7.112. LIBGUESTFS

7.112.1. RHBA-2013:0324 — libguestfs bug fix and enhancement update

Updated libguestfs packages that fix numerous bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libguestfs packages contain a library, which is used for accessing and modifying guest disk images.

Bug Fixes

BZ#801640

Previously, when using the **`resize2fs -M`** command and an error due to lack of free space occurred, the returned error message was incorrect and could confuse the user. With this update, a proper error message is returned instead.

BZ#822626

Due to a bug in the source code, an error occurred when using the **`virt-ls --checksum`** command and the following error message was returned:

```
libguestfs: error: checksum: path: parameter cannot be NULL
```

The underlying source code has been modified and **`virt-ls --checksum`** now works as expected.

BZ#830369

Due to the **`guestfs_inspect_get_hostname()`** function, the **`libguestfs`**-based commands did not work properly when an empty **/etc/HOSTNAME** file was created on a Linux guest. This update applies a patch to fix this bug and the **libguestfs** based commands now work in the described scenario.

BZ#836573

Previously, the **libguestfs** library did not handle the **/dev/disk/by-id/*** paths. Consequently, it was impossible to examine a guest using commands with such a path and an error message was returned. With this update, a patch has been applied to fix this bug and the **libguestfs** library no longer returns error in this situation.

BZ#837691

Previously, under certain conditions, writing to disks in the **qcow2** format could cause silent data loss. The underlying source code has been modified to prevent this behavior and writing to disks in the **qcow2** format now works as expected.

BZ#838609

Due to a race condition between the **guestmount** and the **fusermount** tools, unmouting and then immediately using a disk image was not safe and could cause data loss or memory corruption. This update adds the new **--pid-file** option for **guestmount** to avoid the race condition between these tools and attempts to use disk images immediately after unmounting can no longer cause data loss or memory corruption.

BZ#852396

Previously, the **libguestfs** library limited the total size of downloaded hive files from a Windows Registry to 100 MB. Consequently, an attempt to inspect systems with large amount of hive files caused **libguestfs** to return an error message. With this update, the limit was increased to 300 MB and **libguestfs** can now inspect a larger Widows Registry properly.

BZ#853763

Previously, using the **file** utility to detect the format of a disk image could produce different output for different versions of this utility. The underlying source code has been modified and output is now the same for all versions of the **file** utility.

BZ#858126

Due to a bug in the underlying source code, the **virt-inspector** tool failed to work with certain Windows guests. This update applies a patch to fix this bug and **virt-inspector** now supports all Windows guests as expected.

BZ#858648

Due to recent changes in the iptables packages, the **libguestfs** library could not be installed with the new version of the **iptables** tool. The underlying source code has been modified to fix this bug and the installation of **libguestfs** works as expected.

BZ#872454

Previously, the **libguestfs** library detected the Red Hat Enterprise Linux 5.1 guests as NetBSD guests. This update applies a patch to fix this bug and **libguestfs** now detects Red Hat Enterprise Linux 5.1 guest correctly.

BZ#880805

The **`virt-df`** command with **`-a`** or **`-d`** arguments works correctly only with a single guest. An attempt to use this command with multiple arguments, such as **`virt-df -a RHEL-Server-5.9-32-pv.raw -a opensuse.img`**, caused the disk image names to be displayed incorrectly. With this update, the plus sign ("+") is displayed for each additional disk, so that the user can easily recognize them. In addition, the correct usage of the **`virt-df`** command has been described in the **`virt-df(1)`** man page.

Enhancements

BZ#830135

This enhancement improves the **`libguestfs`** library to support mount-local APIs.

BZ#836501

With this update, the dependency on the fuse packages has been added to **`libguestfs`** dependencies.

All users of libguestfs are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.113. LIBHBAAPI

7.113.1. RHEA-2013:0416 — libhbaapi enhancement update

Updated libhbaapi packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The libhbaapi library is the Host Bus Adapter (HBA) API library for Fibre Channel and Storage Area Network (SAN) resources. It contains a unified API that programmers can use to access, query, observe, and modify SAN and Fibre Channel services.

Enhancement

BZ#862386

This update converts libhbaapi code to a merged upstream repository at Open-FCoE.org. Consequently, the libhbaapi packages are no longer compiled from different sources, thus making maintenance and further development easier.

Users of libhbaapi are not required to upgrade to these updated packages as the change introduced by them is purely formal and does not affect functionality.

7.114. LIBHBALINUX

7.114.1. RHBA-2013:0415 — libhbalinux bug fix and enhancement update

Updated libhbalinux packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libhbalinux package contains the Host Bus Adapter API (HBAAPI) vendor library which uses standard kernel interfaces to obtain information about Fiber Channel Host Buses (FC HBA) in the system.

> **NOTE**
>
> The libhbalinux packages have been upgraded to upstream version 1.0.14, which provides a number of bug fixes and enhancements over the previous version. (BZ#819936)

All users of libhbalinux are advised to upgrade to these updated libhbalinux packages, which fix these bugs and add these enhancements.

7.115. LIBICAL

7.115.1. RHBA-2013:0471 — libical bug fix update

Updated libical packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The libical packages provide a reference implementation of the iCalendar data type and serialization format used in dozens of calendaring and scheduling products.

Bug Fix

BZ#664332

The libical packages can be configured to abort when parsing improperly formatted iCalendar data, primarily useful for testing and debugging. In Red Hat Enterprise Linux this behavior is disabled, but some parts of the libical source code were improperly checking for this option. Consequently, the library aborted even if configured not to do so. The underlying source code has been modified and libical no longer aborts in the described scenario.

All users of libical are advised to upgrade to these updated packages, which fix this bug.

7.116. LIBICA

7.116.1. RHEA-2013:0399 — libica enhancement update

Updated libica packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The libica library contains a set of functions and utilities for accessing the IBM eServer Cryptographic Accelerator (ICA) hardware on IBM System z.

Enhancement

BZ#738835

The libica library has been modified to allow usage of new algorithms that support the Message Security Assist Extension 4 instructions in the Central Processor Assist for Cryptographic Function (CPACF) feature. For the DES and 3DES block ciphers, the new feature supports the following modes of operation:

- Cipher Block Chaining with Ciphertext Stealing (CBC-CS)

- Cipher-based Message Authentication Code (CMAC)

For the AES block cipher, this feature supports the following modes of operation:

- Cipher Block Chaining with Ciphertext Stealing (CBC-CS)
- Counter with Cipher Block Chaining Message Authentication Code (CCM)
- Galois/Counter (GCM)

With this acceleration of complex cryptographic algorithms, performance of IBM System z machines significantly improves.

All users of libica are advised to upgrade to these updated packages, which add this enhancement.

7.117. LIBLDB

7.117.1. RHBA-2013:0372 — libldb bug fix and enhancement update

Updated libldb packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libldb packages provide an extensible library that implements an LDAP-like API to access remote LDAP servers, or use local TDB databases.

NOTE

The libldb packages have been upgraded to upstream version 1.1.13, which provides a number of bug fixes and enhancements over the previous version. One of the most significant changes is that the source code of libldb is no longer a part of the samba4 packages but has been extracted to a separate SRPM package. This resolves the problem caused by recent changes in the Samba build system, which made the libldb library impossible to build as a shared library from the Samba tarball. (BZ#859229)

Bug Fix

BZ#873422

Recent changes in the Samba compiling script caused libldb to expose internal functions and symbols in the public interface. This could lead to various linking and building problems if these internal symbols were used directly out of the libldb code. This update corrects the compiling script so that internal symbols of libldb are no longer exported and visible in the libldb public interface.

All users of libldb are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.118. LIBQB

7.118.1. RHBA-2013:0323 — libqb bug fix and enhancement update

Updated libqb packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libqb packages provide a library with the primary purpose of providing high performance client server reusable features, such as high performance logging, tracing, inter-process communication, and polling.

NOTE

The libqb packages have been upgraded to upstream version 0.14.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#845275)

Bug Fix

BZ#869446

Previously, a timeout argument given to the qb_ipcc_recv() API function was not passed to poll() while waiting for a reply. Consequently, this function could consume nearly 100% CPU resources and affect the pacemaker utility. This bug has been fixed by passing the timeout value to poll() in qb_ipcc_recv(). As a result, the timeout period is honored as expected and pacemaker works correctly in such a case.

All libqb users are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.118.2. RHBA-2013:1431 — libqb bug fix and enhancement update

Updated libqb packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libqb packages provide a library with the primary purpose of providing high performance client server reusable features, such as high performance logging, tracing, inter-process communication, and polling.

NOTE

The libqb packages have been upgraded to upstream version 0.16.0, which provides a number of bug fixes and enhancements over the previous version. One of the notable changes fixes a bug in the qb_log_from_external_source() function, that caused the Pacemaker's policy engine to terminate unexpectedly. The engine now works as expected. (BZ#1001491)

Users of libqb are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.119. LIBSEMANAGE

7.119.1. RHBA-2013:0465 — libsemanage bug fix update

Updated libsemanage packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The libsemanage library provides an API for the manipulation of SELinux binary policies. It is used by checkpolicy (the policy compiler) and similar tools, as well as by programs such as load_policy, which must perform specific transformations on binary policies (for example, customizing policy boolean settings).

Bug Fixes

BZ#798332

Previously, the "usepasswd" parameter was not available in the /etc/selinux/semanage.conf file. This update adds the missing "usepasswd" parameter to this file.

BZ#829378

When a custom SELinux policy module was loaded with an error, an error message that was not very informative was returned. This update fixes the error message to be more helpful for users.

All users of libsemanage are advised to upgrade to these updated packages, which fix these bugs.

7.120. LIBSOUP

7.120.1. RHBA-2013:0313 — libsoup bug fix update

Updated libsoup packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The libsoup packages provide an HTTP client and server library for GNOME.

Bug Fixes

BZ#657622

Prior to this update, the clock-applet did not handle canceled requests during a DNS lookup correctly and accessed already freed memory. As a consequence, the weather view of the clock-applet could, under certain circumstances, abort with a segmentation fault when updating the weather if the hostname of the weather server needed more than 30 seconds, for example due to network problems. This update modifies the underlying code to allow requests that take too long to be canceled.

BZ#746587

Prior to this update, the weather view of the clock-applet tried to connect to the weather server indefinitely as fast as it could if the weather server (or an HTTP proxy) closed the connection without responding. This update modifies the underlying code to retry a request only if the server unexpectedly closes a previously-used connection, not a new connection. Now, libsoup returns a "Connection terminated unexpectedly" error, so the clock-applet does not update the weather display, and tries again later.

All users of libsoup are advised to upgrade to these updated packages, which fix these bugs.

7.121. LIBSSH2

7.121.1. RHBA-2013:0329 — libssh2 bug fix and enhancement update

Updated libssh2 packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libssh2 packages provide a library that implements the SSH2 protocol.

NOTE

The libssh2 packages have been upgraded to upstream version 1.4.2, which provides a number of bug fixes and enhancements over the previous version, including fixes for memory leaks, missing error handling, and incompatibilities in the SSH2 protocol implementation. (BZ#749873)

Bug Fixes

BZ#741919

With this update, several stability patches have been added to libssh2. As a result, memory leaks, buffer overruns, and null pointer problems are avoided when managing a large number of nodes.

BZ#801428

Previously, an insufficient data type was used for certain bit shift operations in the libssh2 code. This behavior caused the curl utility to terminate unexpectedly when downloading files larger than 2 GB over the SSH File Transfer Protocol (SFTP). With this update, the underlying code has been modified to use the correct data type and curl now works as expected in the described scenario.

BZ#804145

Under certain circumstances, libssh2 failed to resume an interrupted key exchange when sending a large amount of data over SSH. Moreover, further data was erroneously sent, which caused the remote site to close the connection immediately. With this update, libssh2 has been modified to properly resume the interrupted key exchange before sending any further data. As a result, the connection remains open and the data transfer proceeds as expected.

BZ#804150

Previously, the function for writing to a channel in libssh2 incorrectly handled error states, which, under certain circumstances, resulted in an infinite loop. The function has been fixed and the error handling now works properly.

BZ#806862, BZ#873785

Previously, the window size adjustment in libssh2 did not work properly, which resulted in unclosed connections when transferring huge files over SCP or SFTP, extensive memory consumption or both. The window-adjusting code has been fixed and works now properly for blocks of arbitrary size.

BZ#826511

Previously, libssh2 incorrectly returned the LIBSSH2_ERROR_EAGAIN error code when operating in blocking mode. The error code is used by libssh2 internally to initiate a blocking operation on a socket. The error code was, however, not properly cleared on success and leaked through the public API of libssh2. An upstream patch has been applied to clear the error code prior to initiating the blocking operation, and libssh2 no longer returns LIBSSH2_ERROR_EAGAIN when operating in blocking mode.

All users of libssh2 are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. After installing these updated packages, all running applications using libssh2 have to be restarted for this update to take effect.

7.122. LIBTALLOC

7.122.1. RHBA-2013:0352 — libtalloc bug fix update

Updated libtalloc packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The libtalloc packages provide a library that implements a hierarchical memory allocator with destructors.

NOTE

The libtalloc packages have been upgraded to upstream version 2.0.7, which provides a number of bug fixes over the previous version. (BZ#766335)

All libtalloc users are advised to upgrade to these updated packages, which fix these bugs.

7.123. LIBTDB

7.123.1. RHBA-2013:0353 — libtdb bug fix and enhancement update

Updated libtdb packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6

The libtdb packages provide a library that implements the Trivial Database (TDB). TDB is a simple hashed database that uses internal locking to allow multiple simultaneous writers and readers.

NOTE

The libtdb packages have been upgraded to upstream version 1.2.10, which provides a number of bug fixes and enhancements over the previous version. These updated libtdb packages are compliant with requirements of Samba 4. (BZ#766334)

All users of libtdb are advised to upgrade to these updated packages, which fix these bugs and adds these enhancements.

7.124. LIBTEVENT

7.124.1. RHBA-2013:0354 — libtevent bug fix and enhancement update

Updated libtevent packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libtevent packages provide Tevent, an event system based on the talloc memory management library. Tevent supports many event types, including timers, signals, and the classic file descriptor events. Tevent also provides helpers to deal with asynchronous code represented by the tevent_req (Tevent Request) functions.

NOTE

The libtevent packages have been upgraded to upstream version 0.9.17, which provides a number of bug fixes and enhancements over the previous version. These updated libtevent packages are compliant with requirements of Samba 4. (BZ#766336)

All users of libtevent are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.125. LIBUSB1

7.125.1. RHBA-2013:0310 — libusb1 bug fix update

Updated libusb1 packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The libusb1 packages provide a library to communicate with USB devices from userspace.

Bug Fixes

BZ#820205

Prior to this update, the usbredir network protocol caused a conflict with the libusb library. As a consequence, SPICE USB-redirection failed with the following errors in the virt-viewer tool: usbredirhost error: submitting bulk transfer on ep 02: -1" when trying to redirect one USB device to two guests simultaneously. This update modifies the underlying code to send the error message "Device is busy" and fail after the second attempt.

BZ#830751

Prior to this update, USB Request Blocks (URBs) from the user space were not allowed to have transfer buffers larger than an arbitrary maximum. As a consequence, attempting to redirect certain USB mass-storage devices could fail. This update modifies the underlying code to allow programs to submit URBs of any size. If there is not sufficient memory available, the submission fails with an ENOMEM error. In addition, this update also replaces the old limits on individual transfer buffers with a single global limit of 16MB on the total amount of memory in use by the USB file system (usbfs) to prevent programs from submitting a lot of small URBs and so using all the DMA-able kernel memory.

All users of libusb1 are advised to upgrade to these updated packages, which fix these bugs.

7.126. LIBVIRT-CIM

7.126.1. RHBA-2013:0449 — libvirt-cim bug fix update

Updated libvirt-cim packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The libvirt-cim package contains a Common Information Model (CIM) provider based on Common Manageability Programming Interface (CMPI). It supports most libvirt virtualization features and allows management of multiple libvirt-based platforms.

Bug Fixes

BZ#805892

If the sblim-sfcb package was installed on the system, rebuilding the libvirt-cim package failed with an error due to an incomplete substitution in the Makefile. The substitution has been corrected and rebuilding libvirt-cim now works as expected.

BZ#864096

When upgrading the libvirt-cim package to a newer version after libvirt-cim had registered its classes with a cim-server, the %preun code unregistered the classes leaving the system without libvirt-cim classes being registered. Now the libvirt-cim package only unregisters the libvirt-cim classes on uninstall.

Users of libvirt-cim are advised to upgrade to these updated packages, which fix these bugs.

7.127. LIBVIRT-JAVA

7.127.1. RHBA-2013:0325 — libvirt-java bug fix and enhancement update

Updated libvirt-java packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The libvirt-java packages provide Java bindings to use libvirt, which is the virtualization API to manage and interact with virtualization capabilities.

NOTE

The libvirt-java packages have been upgraded to upstream version 0.4.9, which provides a number of bug fixes and enhancements over the previous version. (BZ#838046)

Bug Fix

BZ#836920

Due to a failing Java Native Access (JNA) conversion, the "setSchedulerParameters()" method for domains did not process input parameters properly. With this update, the conversion process has been modified. As a result, setSchedulerParameters() now works as expected.

All users of libvirt-java are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.128. LIBVIRT

7.128.1. RHBA-2013:0664 — libvirt bug fix and enhancement update

Updated libvirt packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remote management of virtualized systems.

Bug Fixes

BZ#908836

The AMD family 15h processors CPU architecture consists of "modules", which are represented both as separate cores and separate threads. Management applications needed to choose between one of the approaches, and libvirt did not provide enough information to do this. Management applications were not able to represent the modules in an AMD family 15h processors core according to their needs. The capabilities XML output now contains more information about the processor topology, so that the management applications can extract the information they need.

BZ#913624

When auto-port and port were not specified, but the tlsPort attribute was set to "-1", the tlsPort parameter specified in the QEMU command line was set to "1" instead of a valid port. Consequently, QEMU failed, because it was unable to bind a socket on the port. This update replaces the current QEMU driver code for managing port reservations with the new virPortAllocator APIs, and QEMU is able to bind a socket on the port.

BZ#915344

Previously, libvirtd was unable to execute an s3/s4 operation for a Microsoft Windows guest which ran the guest agent service. Consequently, this resulted in a "domain s4 fail" error message, due to the domain being destroyed. With this update, the guest is destroyed successfully and the libvirtd service no longer crashes.

BZ#915347

When a VM was saved into a compressed file and decompression of that file failed while libvirt was trying to resume the VM, libvirt removed the VM from the list of running VMs, but did not remove the corresponding QEMU process. With this update, the QEMU process is killed in such cases. Moreover, non-fatal decompression errors are now ignored and a VM can be successfully resumed if such an error occurs.

BZ#915348

Python bindings for libvirt contained incorrect implementation of getDomain() and getConnect() methods in virDomainSnapshot class. Consequently, the Python client terminated unexpectedly with a segmentation fault. Python bindings now provide proper domain() and connect() accessors that fetch Python objects stored internally within virDomainSnapshot instance and crashes no longer occur.

BZ#915349

Previously, libvirt added a cache of storage file backing chains, rather than rediscovering the backing chain details on every operation. This cache was then used to decide which files to label for sVirt, but when libvirt switched over to use the cache, the code only populated when cgroups were in use. On setups that did not use cgroups, due to the lack of backing chain cache information, sVirt was unable to properly label backing chain files, which caused a regression observed by guests being prevented from running. Now, populating the cache was moved earlier, to be independent of cgroups, the cache results in more efficient sVirt operations, and now works whether or not cgroups are in effect.

BZ#915353

Occasionally, when users ran multiple virsh create/destroy loops, a race condition could have occurred and libvirtd terminated unexpectedly with a segmentation fault. False error messages regarding the domain having already been destroyed to the caller also occurred. With this update, the outlined script is run and completes without libvirtd crashing.

BZ#915354

Previously, libvirt followed relative backing chains differently than QEMU. This resulted in missing sVirt permissions when libvirt could not follow the chain. With this update, relative backing files are now treated identically in libvirt and QEMU, and VDSM use of relative backing files functions properly.

BZ#915363

Previously, libvirt reported raw QEMU errors when snapshots failed, and the error message provided was confusing. With this update, libvirt now gives a clear error message when QEMU is not capable of snapshots, which enables more informative handling of the situation.

BZ#917063

Previously, libvirt was not tolerant of missing unpriv_sgio support in running kernel even though it was not necessary. After upgrading the host system to Red Hat Enterprise Linux 6.4, users were unable to start domains using shareable block disk devices unless they rebooted the host into the new kernel. The check for unpriv_sgio support is only performed when it is really needed, and libvirt is now able to start all domains that do not strictly require unpriv_sgio support regardless of host kernel support for it.

BZ#918754

When asked to create a logical volume with zero allocation, libvirt ran lvcreate to create a volume with no extends, which is not permitted. Creation of logical volumes with zero allocation failed and libvirt returned an error message that did not mention the real error. Now, rather than asking for no extends, libvirt tries to create the volume with a minimal number of extends. The code is also fixed to provide the real error message should the volume creation process fail. Logical volumes with zero allocation can now be successfully created using libvirt.

BZ#919504

Previously, when users started the guest with a sharable block CD-Rom, libvirtd failed unexpectedly due to accessing memory that was already freed. This update addresses the aforementioned issue, and libvirtd no longer crashes in the described scenario.

BZ#922095

Various memory leaks in libvirtd were discovered when users ran Coverity and Valgrind leak detection tools. This update addresses these issues, and libvirtd no longer leaks memory in the described scenario.

Enhancement

BZ#915352

This update adds support for ram_size settings to the QXL device. When using multiple heads in one PCI device, the device needed more RAM assigned. Now, the memory of the RAM bar size is set larger than the default size and libvirt can drive multi-head QXL.

Users of libvirt are advised to upgrade to these updated packages, which fix these bugs and add this enhancement. After installing the updated packages, libvirtd will be restarted automatically.

7.128.2. RHSA-2013:0276 — Moderate: libvirt bug fix, and enhancement update

Updated libvirt packages that fix one security issue, multiple bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The libvirt packages provide the **`libvirt`** library which is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, **`libvirt`** provides tools for remote management of virtualized systems.

NOTE

The libvirt packages have been upgraded to upstream version 0.10.2, which provides a number of bug fixes and enhancements over the previous version, such as support for **`Open vSwitch`**, a new API for detailed CPU statistics, improved support of LXC method including the **`sVirt`** technology, improvements of the **`virsh edit`** command, improved APIs for listing various objects and support for pinning and tuning emulator threads. (BZ#836934)

Security Fixes

CVE-2012-3411

It was discovered that libvirt made certain invalid assumptions about dnsmasq's command line options when setting up DNS masquerading for virtual machines, resulting in dnsmasq incorrectly processing network packets from network interfaces that were intended to be prohibited. This update includes the changes necessary to call dnsmasq with a new command line option, which was introduced to dnsmasq via RHSA-2013:0277.

In order for libvirt to be able to make use of the new command line option (--bind-dynamic), updated dnsmasq packages need to be installed. Refer to RHSA-2013:0277 for additional information.

Bug Fixes

BZ#794523

The **`libvirt`** library was issuing the **`PAUSED`** event before the QEMU processor emulator really paused. Consequently, a domain could be reported as paused before it was actually paused, which could confuse a management application using the **`libvirt`** library. With this update, the **`PAUSED`** event is started after QEMU is stopped on a monitor and the management application is no longer confused by **`libvirt`**.

BZ#797279, BZ#808980, BZ#869557

The fixed limit for the maximum size of an RPC message that could be sent between the **`libvirtd`** daemon and a client, such as the **`virsh`** utility, was 65536 bytes. However, this limit was not always sufficient and messages that were longer than that could be dropped, leaving a client unable to fetch important data. With this update, the buffer for incoming messages has been made dynamic and both sides, a client and **`libvirtd`**, now allocate as much memory as is needed for a given message, thus allowing to send much bigger messages.

BZ#807996

Previously, repeatedly migrating a guest between two machines while using the tunnelled migration could cause the **`libvirtd`** daemon to lock up unexpectedly. The bug in the code for locking remote drivers has been fixed and repeated tunnelled migrations of domains now work as expected.

BZ#814664

Previously, multiple **`libvirt`** API calls were needed to determine the full list of guests on a host controlled by the **`libvirt`** library. Consequently, a race condition could occur when a guest changed its state between two calls that were needed to enumerate started and stopped guests. This behavior caused the guest to disappear from both of the lists, because the time of enumeration was not considered to be a part of the lists. This update adds a new API function allowing to gather the guest list in one call while the driver is locked. This guarantees that no guest changes its state before the list is gathered so that guests no longer disappear in the described scenario.

BZ#818467

Previously, **`libvirt`** did not report many useful error messages that were returned by external programs such as QEMU and only reported a command failure. Consequently, certain problems, whose cause or resolution could be trivial to discover by looking at the error output, were difficult to diagnose. With this update, if any external command run by **`libvirt`** exits with a failure, its standard error output is added to the system log as a **`libvirt`** error. As a result, problems are now easier to diagnose, because better information is available.

BZ#823716

Closing a file descriptor multiple times could, under certain circumstances, lead to a failure to execute the **qemu-kvm** binary. As a consequence, a guest failed to start. A patch has been applied to address this issue, so that the guest now starts successfully.

BZ#825095

Prior to this update, **`libvirt`** used an unsuitable detection procedure to detect NUMA and processor topology of a system. Consequently, topology of some advanced multi-processor systems was detected incorrectly and management applications could not utilize the full potential of the system. Now, the detection has been improved and the topology is properly recognized even on modern systems.

BZ#825820

Previously, the **`libvirt`** library had hooks for calling a user-written script when a guest was started or stopped, but had no hook to call a script for each guest when the **`libvirtd`** daemon itself was restarted. Consequently, certain custom setups that required extra operations not directly provided by **`libvirt`** could fail when **`libvirtd`** was restarted. For example, packet forwarding rules installed to redirect incoming connections to a particular guest could be overridden by **`libvirt`**'s “refresh” of its own iptables packet forwarding rules, breaking the connection forwarding that had been set up. This update improves **`libvirt`** with a new “reconnect” hook; the QEMU hook script is called with a type of “reconnect” for every active guest each time **`libvirtd`** is restarted. Users can now write scripts to recognize the “reconnect” event, and for example reload the user-supplied iptables forwarding rules when this event occurs. As a result, incoming connections continue to be forwarded correctly, even when **`libvirtd`** is restarted.

BZ#828729

On certain NUMA architectures, **`libvirt`** failed to process and expose the NUMA topology, sometimes leading to performance degradation. With this update, **`libvirt`** can parse and expose the NUMA topology on such machines and makes the correct CPU placement, thus avoiding performance degradation.

BZ#831877

The **`virsh undefine`** command supports deleting volumes associated with a domain. When using this command, the volumes are passed as additional arguments and if the user adds any trailing string after the basic command, the string is interpreted as a volume to be deleted. Previously, the volumes were checked after the guest was deleted, which could lead to user's errors. With this update, the check of the volume arguments is performed before the deleting process so that errors can be reported sensibly. As a result, the command with an incorrect argument fails before it attempts to delete a guest and the host system stays in a sane state.

BZ#832081

Due to several bugs in the implementation of keep-alive messages that are used for the detection of broken connections or non-functional peers, these connections and peers could be incorrectly considered broken or non-functional and thus the keep-alive messages were disabled by default in Red Hat Enterprise Linux 6.3. The implementation of the keep-alive messages has been fixed and this feature is now enabled by default.

BZ#834927

Previously, a reversed condition in a check which is used during registering callbacks prevented multiple callbacks from being registered. This update applies a patch to fix this condition and multiple callbacks can be registered successfully now.

BZ#836135

The **`SPICE`** server needs certain time at the end of the migration process to transfer an internal state to a destination guest. Previously, the **`libvirt`** library could kill the source QEMU and the **`SPICE`** server before the internal state was transmitted. This behavior caused the destination client to be unresponsive. With this update, **`libvirt`** waits until the end of **`SPICE`** migration. As a result, the **`SPICE`** server no longer becomes unresponsive in this situation.

BZ#837659

When using the **`sanlock`** daemon for locking resources used by a domain, if such a resource was read-only, the locking attempt failed. Consequently, it was impossible to start a domain with a CD-ROM drive. This bug has been fixed and **`sanlock`** can now be properly used with read-only devices.

BZ#839661

Previously, the **`libvirt`** library did not support the S4 (Suspend-to-Disk) event on QEMU domains. Consequently, management applications could not register whether a guest was suspended to disk or powered off. With this update, support for S4 event has been added and management applications can now request receiving S4 events.

BZ#842208

Due to an installation of the **`vdsm`** daemon, the **`libvirt`** library was reconfigured and under certain conditions, **`libvirt`** was searching for a non-existing option when used outside of **`vdsm`**. Consequently, using the **`virsh`** utility on such a machine caused the system to terminate with a segmentation fault. The underlying source code has been modified to fix this bug and users can now use **`virsh`** on machines configured by **`vdsm`** as expected.

BZ#844266

Previously, a condition in a check, which is used for checking if modification of a domain XML in a saved file was successful or not, was inverted. Consequently, the **`virsh`** utility reported that this check failed even if it was successful and vice versa. This update applies a patch to fix this bug and success and failure of this check are reported correctly now.

BZ#844408

Disk hot plug is a two-part action: the **`qemuMonitorAddDrive()`** call is followed by the **`qemuMonitorAddDevice()`** call. When the first part succeeded but the second one failed, **`libvirt`** failed to roll back the first part and the device remained in use even though the disk hot plug failed. With this update, the rollback for the drive addition is properly performed in the described scenario and disk hot plug now works as expected.

BZ#845448

Previously the **`SIGINT`** signal was not blocked when the **`virDomainGetBlockJobInfo()`** function was performed. Consequently, an attempt to abort a process initialized by a command with the **`--`**

wait option specified using the CTRL+C shortcut did not work properly. This update applies a patch to block **SIGINT** during **virDomainGetBlockJobInfo()** and aborting processes using the CTRL+C shortcut now works as expected.

BZ#845635

Previously, an unspecified error with a meaningless error code was returned when a guest agent became unresponsive. Consequently, management applications could not recognize why the guest agent hung; whether the guest agent was not configured or was unusable. This update introduces a new **VIR_ERR_AGENT_UNRESPONSIVE** error code and fixes the error message. As a result, management applications now can recognize why the guest agent hangs.

BZ#846639

Due to a bug in the **libvirt** code, two mutually exclusive cases could occur. In the first case, a guest operating system could fail do detect that it was being suspended because the suspend routine is handled by hypervisor. In the second case, the cooperation of the guest operating system was required, for example during synchronization of the time after the resume routine. Consequently, it was possible to successfully call the suspend routine on a domain with the **pmsuspended** status and **libvirt** returned success on operation, which in fact failed. This update adds an additional check to prevent **libvirt** from suspending a domain with the **pmsuspended** status.

BZ#851397

Due to recent changes in port allocation, SPICE ports and SPICE TLS ports were the same. Consequently, QEMU domains started with both options configured to use the same port and SPICE TLS ports could not allocate one port twice. With this update, the port allocation has been fixed and the QEMU domains now work as expected in this situation.

BZ#853567

A virtual guest can have a network interface that is connected to an SR-IOV (Single Root I/O Virtualization) device's virtual function (VF) using the **macvtap** driver in passthrough mode, and from there is connected to an **802.1Qbh**-capable switch. Previously, when shutting down the guest, **libvirt** erroneously set SR-IOV device's physical function (PF) instead of VF and the PF offline rather than setting the VF offline. Here is an example of the type of an interface that could be affected:

```
<interface type='direct'>
  <source dev='eth7' mode='passthrough'/>
  <virtualport type='802.1Qbh'>
   <parameters profileid='test'/>
  </virtualport>
</interface>
```

Consequently, if PF was being used by the host for its own network connectivity, the host networking would be adversely affected, possibly completely disabled, whenever the guest was shut down, or when the guest's network device was detached. The underlying source code has been modified to fix this bug and the PF associated with the VF used by the **macvtap** driver now continues to work in the described scenario.

BZ#856247

Red Hat Enterprise Linux 6.3 implemented the **block copy** feature before the upstream version of QEMU. Since then, several improvements were made to the upstream version of this feature. Consequently, previous versions of the **libvirt** library were unable to fully manage the **block**

copy feature in current release of QEMU. With this update, the **block copy** feature has been updated to upstream versions of QEMU and **libvirt**. As a result, **libvirt** is able to manage all versions of the **block copy** feature.

BZ#856864

Previously, **libvirt** put the default USB controller into the XML configuration file during the live migration to Red Hat Enterprise Linux 6.1 hosts. These hosts did not support USB controllers in the XML file. Consequently, live migration to these hosts failed. This update prevents **libvirt** from including the default USB controller in the XML configuration file during live migration and live migration works properly in the described scenario.

BZ#856950

When a QEMU process is being destroyed by **libvirt**, a clean-up operation frees some internal structures and locks. However, since users can destroy QEMU processes at the same time, **libvirt** holds the QEMU driver mutex to protect the list of domains and their states, among other things. Previously, a function tried to lock up the QEMU driver mutex when it was already locked, creating a deadlock. The code has been modified to always check if the mutex is free before attempting to lock it up, thus fixing this bug.

BZ#858204

When the **host_uuid** option was present in the **libvirtd.conf** file, the **augeas libvirt** lens was unable to parse the file. This bug has been fixed and the **augeas libvirt** lens now parses **libvirtd.conf** as expected in the described scenario.

BZ#862515

Previously, handling of duplicate MAC addresses differed between live attach or detach, and persistent attach or detach of network devices. Consequently, the persistent attach-interface of a device with a MAC address that matches an existing device could fail, even though the live attach-interface of such a device succeed. This behavior was inconsistent, and sometimes led to an incorrect device being detached from the guest. With this update, **libvirt** has been modified to allow duplicate MAC addresses in all cases and to check a unique PCI address in order to distinguish between multiple devices with the same MAC address.

BZ#863115

Previously, **libvirt** called the **qemu-kvm -help** command every time it started a guest to learn what features were available for use in QEMU. On a machine with a number of guests, this behavior caused noticeable delays in starting all of the guests. This update modifies **libvirt** to store information cache about QEMU until the QEMU time stamp is changed. As a result, **libvirt** is faster when starting a machine with various guests.

BZ#865670

Previously, the **ESX 5.1** server was not fully tested. Consequently, connecting to **ESX 5.1** caused a warning to be returned. The **ESX 5.1** server has been properly tested and connecting to this server now works as expected.

BZ#866369

Under certain circumstances, the **iohelper** process failed to write data to disk while saving a domain and kernel did not report an out-of-space error (**ENOSPC**). With this update, **libvirt** calls the **fdatasync()** function in the described scenario to force the data to be written to disk or catch a write error. As a result, if a write error occurs, it is now properly caught and reported.

BZ#866388

Certain operations in **`libvirt`** can be done only when a domain is paused to prevent data corruption. However, if a resuming operation failed, the management application was not notified since no event was sent. This update introduces the **`VIR_DOMAIN_EVENT_SUSPENDED_API_ERROR`** event and management applications can now keep closer track of domain states and act accordingly.

BZ#866999

When **`libvirt`** could not find a suitable CPU model for a host CPU, it failed to provide the CPU topology in host capabilities even though the topology was detected correctly. Consequently, applications that work with the host CPU topology but not with the CPU model could not see the topology in host capabilities. With this update, the host capabilities XML description contains the host CPU topology even if the host CPU model is unknown.

BZ#869096

Previously, **`libvirt`** supported the **`emulatorpin`** option to set the CPU affinity for a QEMU domain process. However, this behavior overrode the CPU affinity set by the **`vcpu placement="auto"`** setting when creating a cgroup hierarchy for the domain process. This CPU affinity is set with the advisory nodeset from the **`numad`** daemon. With this update, **`libvirt`** does not allow **`emulatorpin`** option to change the CPU affinity of a domain process if the **`vcpu placement`** setting is set to **`auto`**. As a result, the **`numad`** daemon is supported as expected.

BZ#873792

The **`libvirt`** library allows users to cancel an ongoing migration. Previously, if an attempt to cancel the migration was made in the migration preparation phase, QEMU missed the request and the migration was not canceled. With this update, the **`virDomainAbortJob()`** function sets a flag when a cancel request is made and this flag is checked before the main phase of the migration starts. As a result, a migration can now be properly canceled even in the preparation phase.

BZ#874050

Certain AMD processors contain modules which are reported by the kernel as both threads and cores. Previously, the **`libvirt`** processor topology detection code was not able to detect these modules. Consequently, **`libvirt`** reported the actual number of processors twice. This bug has been fixed by reporting a topology that adds up to the total number of processors reported in the system. However, the actual topology has to be checked in the output of the **`virCapabilities()`** function. Additionally, documentation for the fallback output has been provided.

> **NOTE**
>
> Note that users should be instructed to use the capability output for topology detection purposes due to performance reasons. The NUMA topology has the important impact performance-wise but the physical topology can differ from that.

BZ#879780

Due to changes in the **`virStorageBackendLogicalCreateVol()`** function, the setting of the volume type was removed. Consequently, logical volumes were treated as files without any format and **`libvirt`** was unable to clone them. This update provides a patch to set the volume type and **`libvirt`** clones logical volumes as expected.

BZ#880919

When a saved file could not be opened, the **virFileWrapperFdCatchError()** function was called with a **NULL** argument. Consequently, the **libvirtd** daemon terminated unexpectedly due to a NULL pointer dereference. With this update, the **virFileWrapperFdCatchError()** function is called only when the file is open and instead of crashing, the daemon now reports an error.

BZ#884650

Whenever the **virDomainGetXMLDesc()** function was executed on an unresponsive domain, the call also became unresponsive. With this update, QEMU sends the **BALLOON_CHANGE** event when memory usage on a domain changes so that **virDomainGetXMLDesc()** no longer has to query an unresponsive domain. As a result, **virDomainGetXMLDesc()** calls no longer hang in the described scenario.

Enhancements

BZ#638512

This update adds support for external live snapshots of disks and RAM.

BZ#693884

Previously, **libvirt** could apply packet filters, among others the anti-spoofing filter, to guest network connections using the nwfilter subsystem. However, these filter rules required manually entering the IP address of a guest into the guest configuration. This process was not effective when guests were acquired their IP addresses via the **DHCP** protocol; the network needed a manually added **static host** entry for each guest and the guest's network interface definition needed that same IP address to be added to its filters. This enhancement improves **libvirt** to automatically learn IP and MAC addresses used by a guest network connection by monitoring the connection's **DHCP** and **ARP** traffic in order to setup host-based guest-specific packet filtering rules that block traffic with incorrect IP or MAC addresses from the guests. With this new feature, nwfilter packet filters can be written to use automatically detected IP and MAC addresses, which simplifies the process of provisioning a guest.

BZ#724893

When the guest CPU definition is not supported due to the user's special configuration, an error message is returned. This enhancement improves this error message to contain flags that indicate precisely which options of the user's configuration are not supported.

BZ#771424

The *Resident Set Size* (RSS) limits control how much RAM can a process use. If a process leaks memory, the limits do not let the process influence other processes within the system. With this update, the RSS limits of a QEMU process are set by default according to how much RAM and video RAM is configured for the domain.

BZ#772088

Previously, the **libvirt** library could create block snapshots, but could not clean them up. For a long-running guest, creating a large number of snapshots led to performance issues as the QEMU process emulator had to traverse longer chains of backing images. This enhancement improves the **libvirt** library to control the feature of the QEMU process emulator which is responsible for committing the changes in a snapshot image back into the backing file and the backing chain is now kept at a more manageable length.

BZ#772290

Previously, the automatically allocated ports for the **SPICE** and **VNC** protocols started on the port number 5900. With this update, the starting port for **SPICE** and **VNC** is configurable by users.

BZ#789327

The QEMU guest and the media of CD_ROM or Floppy could be suspended or resumed inside the guest directly instead of using the **libvirt** API. This enhancement improves the **libvirt** library to support three new events of the **QEMU Monitor Protocol** (QMP): the **SUSPEND**, **WAKEUP**, and **DEVICE_TRAY_MOVED** event. These events let a management application know that the guest status or the tray status has been changed:

- when the **SUSPEND** event is emitted, the domain status is changed to **pmsuspended**;
- when the **WAKEUP** event is emitted, the domain status is changed to **running**;
- when the **DEVICE_TRAY_MOVED** event is emitted for a disk device, the current tray status for the disk is reflected to the **libvirt** XML file, so that management applications do not start the guest with the medium inserted while the medium has been previously ejected inside the guest.

BZ#804749

The QEMU process emulator now supports **TSC-Deadline timer** mode for guests that are running on the Intel 64 architecture. This enhancement improves the **libvirt** library with this feature's flag to stay synchronized with QEMU.

BZ#805071

Previously, it was impossible to move a guest's network connection to a different network without stopping the guest. In order to change the connection, the network needed to be completely detached from the guest and then re-attached after changing the configuration to specify the new connection. With this update, it is now possible to change a guest's interface definition to specify a different type of interface, and to change the network or bridge name or both, all without stopping or pausing the guest or detaching its network device. From the point of view of the guest, the network remains available during the entire transition; if the move requires a new IP address, that can be handled by changing the configuration on the guest, or by requesting that it renews its **DHCP** lease.

BZ#805243

When connecting to the **libvirt** library, certain form of authentication could be required and if so, interactive prompts were presented to the user. However, in certain cases, the interactive prompts cannot be used, for example when automating background processes. This enhancement improves **libvirt** to use the **auth.conf** file located in the **$HOME/.libvirt/** directory to supply authentication credentials for connections. As a result, these credentials are pre-populated, thus avoiding the interactive prompts.

BZ#805654

This enhancement improves **libvirt** to support connection of virtual guest network devices to Open vSwitch bridges, which provides a more fully-featured replacement for the standard Linux Host Bridge. Among other features, Open vSwitch bridges allow setting more connections to a single bridge, transparent VLAN tagging, and better management using the Open Flow standard. As a result, **libvirt** is now able to use an already existing Open vSwitch bridge, either directly in the interface definition of a guest, or as a bridge in a **libvirt** network. Management of the bridge must be handled outside the scope of **libvirt**, but guest network devices can be attached and detached, and VLAN tags and interface IDs can be assigned on a per-port basis.

BZ#818996

Certain users prefer to run minimal configurations for server systems and do not need graphical or USB support. This enhancement provides a new feature that allows users to disable USB and graphic controllers in guest machines.

BZ#820808, BZ#826325

With this enhancement, the **`virsh dump`** command is now supported for domains with passthrough devices. As a result, these domains can be dumped with an additional **`--memory-only`** option.

BZ#822064

The **`libvirt`** library has already supported pinning and limiting QEMU threads associated with virtual CPUs, but other threads, such as the I/O thread, could not be pinned and limited separately. This enhancement improves **`libvirt`** to support pinning and limiting of both CPU threads and other emulator threads separately.

BZ#822589

This enhancement improves the **`libvirt`** library to be able to configure *Discretionary Access Control* (DAC) for each domain, so that certain domains can access different resources.

BZ#822601

Previously, only the “system instance” of the **`libvirtd`** daemon, that is the one that is running as the root user, could set up a guest network connection using a tap device and host bridge. A “session instance”, that is the one that is running as a non-root user, was only able to use QEMU's limited “user mode” networking. User mode network connection have several limitations; for example, they do not allow incoming connections, or ping in either direction, and are slower than a tap-device based network connection. With this enhancement, **`libvirt`** has been updated to support QEMU's new SUID “network helper”, so that non-privileged **`libvirt`** users are able to create guest network connections using tap devices and host bridges. Users who require this behavior need to set the interface type to **`bridge`** in the virtual machine's configuration, **`libvirtd`** then automatically notices that it is running as a non-privileged user, and notifies QEMU to set up the network connection using its “network helper”.

NOTE

This feature is only supported when the interface type is **`bridge`**, and does not work with the **`network`** interface type even if the specified network uses a bridge device.

BZ#822641

Previously, core dumps for domains with a large amount of memory were unnecessarily huge. With this update, a new **`dumpCore`** option has been added to control whether guest's memory should be included in a core dump. When this option is set to **`off`**, core dumps are reduced by the size of the guest's memory.

BZ#831099

This enhancement allows the **`libvirt`** library to set the *World Wide Name* (WWN), which provides stable device paths, for IDE and SCSI disks.

BZ#836462

This enhancement adds the possibility to control the advertising of S3 (Suspend-to-RAM) and S4 (Suspend-to-Disk) domain states to a guest. As a result, supported versions of QEMU can be configured to not advertise its S3 or S4 capability to a guest.

BZ#838127

With this update, support for the AMD Opteron G5 processor model has been added to the **`libvirt`** library. This change allows the user to utilize the full potential of new features, such as **`16c`**, **`fma`**, and **`tbm`**.

BZ#843087

This enhancement adds support for the next generation Intel Core and Intel Xeon processors to the **`libvirt`** library. The next generation supports the following features: **`fma`**, **`pcid`**, **`movbe`**, **`fsgsbase`**, **`bmi1`**, **`hle`**, **`avx2`**, **`smep`**, **`bmi2`**, **`erms`**, **`invpcid`**, and **`rtm`**, compared to the previous Intel Xeon Processor E5-XXXX and Intel Xeon Processor E5-XXXX V2 family of processors.

BZ#844404

When changing the configuration of a **`libvirt`** virtual network, it was necessary to restart the network for these changes to take effect. This enhancement adds a new **`virsh net-update`** command that allows certain parts of a network configuration to be modified, and the changes to be applied immediately without requiring a restart of the network and disconnecting of guests. As a result, it is now possible to add static host entries to and remove them from a network's dhcp section; change the range of IP addresses dynamically assigned by the DHCP server; modify, add, and remove portgroup elements; and add and remove interfaces from a forward element's pool of interfaces, all without restarting the network. Refer to the **`virsh(1)`** man page for more details about the **`virsh net-update`** command.

BZ#860570

With this enhancement, the **virsh** program supports the **`--help`** option for all its commands and displays appropriate documentation.

BZ#864606

With this enhancement, the **`libvirt`** library can now control the **`hv_relaxed`** feature. This feature makes a Windows guest more tolerant to long periods of inactivity.

BZ#874171

Current release of the **`libvirt`** library added several capabilities related to snapshots. Among these was the ability to create an external snapshot, whether the domain was running or was offline. Consequently, it was also necessary to improve the user interface to support those features in the **virsh** program. With this update, these snapshot-related improvements were added to **virsh** to provide full support of these features.

BZ#878578

For security reasons, certain SCSI commands were blocked in a virtual machine. This behavior was related to applications where *logical unit numbers* (LUNs) of SCSI disks were passed to trusted guests. This enhancement improves **`libvirt`** to support a new **`sgio`** attribute. Setting this attribute to **`unfiltered`** allows trusted guests to invoke all supported SCSI commands.

All users of libvirt are advised to upgrade to these updated packages, which fix these issues and add these enhancements. After installing the updated packages, the **`libvirtd`** daemon must be restarted using the **`service libvirtd restart`** command for this update to take effect.

7.128.3. RHSA-2013:1272 — Important: libvirt security and bug fix update

Updated libvirt packages that fix two security issues and several bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remote management of virtualized systems.

Security Fixes

CVE-2013-4311

libvirt invokes the PolicyKit pkcheck utility to handle authorization. A race condition was found in the way libvirt used this utility, allowing a local user to bypass intended PolicyKit authorizations or execute arbitrary commands with root privileges.

CVE-2013-4296

Note: With this update, libvirt has been rebuilt to communicate with PolicyKit via a different API that is not vulnerable to the race condition. The polkit RHSA-2013:1270 advisory must also be installed to fix the CVE-2013-4311 issue.

An invalid free flaw was found in libvirtd's remoteDispatchDomainMemoryStats function. An attacker able to establish a read-only connection to libvirtd could use this flaw to crash libvirtd.

The CVE-2013-4296 issue was discovered by Daniel P. Berrange of Red Hat.

Bug Fixes

BZ#984556

Prior to this update, the libvirtd daemon leaked memory in the virCgroupMoveTask() function. A fix has been provided which prevents libvirtd from incorrect management of memory allocations.

BZ#984561

Previously, the libvirtd daemon was accessing one byte before the array in the virCgroupGetValueStr() function. This bug has been fixed and libvirtd now stays within the array bounds.

BZ#984578

When migrating, libvirtd leaked the migration URI (Uniform Resource Identifier) on destination. A patch has been provided to fix this bug and the migration URI is now freed correctly.

BZ#1003934

Updating a network interface using virDomainUpdateDeviceFlags API failed when a boot order was set for that interface. The update failed even if the boot order was set in the provided device XML. The virDomainUpdateDeviceFlags API has been fixed to correctly parse the boot order specification from the provided device XML and updating network interfaces with boot orders now works as expected.

Users of libvirt are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, libvirtd will be restarted automatically.

7.129. LIBWACOM

7.129.1. RHEA-2013:0333 — libwacom enhancement update

Updated libwacom packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The libwacom packages contain a library that provides access to a tablet model database. The libwacom packages expose the contents of this database to applications, allowing for tablet-specific user interfaces. The libwacom packages allow the GNOME tools to automatically configure screen mappings and calibrations, and provide device-specific configurations.

Enhancement

BZ#857073

Previously, the Wacom Cintiq 22HD graphics tablet was not supported by the libwacom library. Consequently, this specific type of graphics tablet was not recognized by the system. This update adds the support for Wacom Cintiq 22HD, which can be now used without complications.

All users of libwacom are advised to upgrade to these updated packages, which add this enhancement.

7.130. LLDPAD

7.130.1. RHBA-2013:0414 — lldpad bug fix and enhancement update

Updated lldpad packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The lldpad packages provide the Linux user space daemon and configuration tool for Intel's Link Layer Discovery Protocol (LLDP) agent with Enhanced Ethernet support.

NOTE

The lldpad packages have been upgraded to upstream version 0.9.45, which provides a number of bug fixes and enhancements over the previous version. In particular, a new subpackage, lldpad-libs, has been introduced. It contains the liblldp_clif shared library which provides an easy way for applications to talk to the LLDPAD daemon (lldpad). (BZ#819938)

Bug Fixes

BZ#818598

Previously, LLDPAD did not listen to multicast MAC addresses. Consequently, it could not gather information from locally connected bridges and lldptool displayed the wrong information. A patch has been applied to enable monitoring of broadcast MAC addresses and users can now display the correct information about locally connected bridges.

BZ#824188

Previously, dcbtool commands could, under certain circumstances, fail to enable the Fibre Channel over Ethernet (FCoE) application type-length-values (TLV) for a selected interface during the installation process. Consequently, various important features might have not been enabled (for example priority flow control, or PFC) by the Data Center Bridging Exchange (DCBX) peer. To prevent such problems, application-specific parameters (such as the FCoE application TLV) in DCBX are now enabled by default.

BZ#829857

Previously, an error in the DCBX (Data Center Bridging Exchange) version selection logic could cause LLDPDUs (Link Layer Discovery Protocol Data Units) to be not encoded in the TLV (Type-Length Value) format during the transition from IEEE DCBX to the legacy DCBX mode. Consequently, link flaps, a delay, or a failure in synchronizing up DCBX between the host and a peer device could occur. In the case of booting from a remote FCoE (Fibre-Channel Over Ethernet) LUN (Logical Unit Number), this bug could result in a failure to boot. This update fixes the bug and TLV is now always used in the described scenario.

BZ#870576

When none of the user priority attributes were PFC (Priority-based Flow Control) enabled, attempting to query the currently configured LocalAdminParam values for the "enabled" parameter produced the message "End of LLDPDU TLV". An upstream patch has been applied and now the lldptool utility returns "none" as expected in the scenario described.

BZ#870578

Previously, when a peer removed a TLV (ETS, PFC, or APP) the 802.1Qaz module did not update the local MIB. Consequently, this resulted in the old peer data persisting even though it was no longer in the received PDU. This update resolves the problem by clearing the local MIB even in the case of a NULL PTR indicating that no MIB was received. As a result, the operational status for PFC reverts to the localAdminParams settings as expected in the scenario described.

Enhancement

BZ#738897

This update adds support for the IEEE 802.1Qbg standard over bonded interfaces. Users can now take full advantage of 802.1Qbg capabilities.

All users of lldpad are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.131. LM_SENSORS

7.131.1. RHBA-2012:1309 — lm_sensors bug fixes

Updated lm_sensors packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The lm_sensors packages provide a set of modules for general SMBus access and hardware monitoring.

Bug Fixes

BZ#610000, BZ#623587

Prior to this update, the sensors-detect script did not detect all GenuineIntel CPUs. As a consequence, lm_sensors did not load coretemp module automatically. This update uses a more generic detection for Intel CPUs. Now, the coretemp module is loaded as expected.

BZ#768365

Prior to this update, the sensors-detect script reported an error when running without user-defined input. This behavior had no impact on the function but could confuse users. This update modifies the underlying code to allow for the sensors-detect script to run without user.

All users of lm_sensors are advised to upgrade to these updated packages, which fix these bugs.

7.132. LOGROTATE

7.132.1. RHBA-2012:1172 — logrotate bug fix update

Updated logrotate packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The logrotate utility simplifies the administration of multiple log files, allowing the automatic rotation, compression, removal, and mailing of log files.

Bug Fix

BZ#827570

Attempting to send a file to a specific e-mail address failed if the "mailfirst" and "delaycompress" options were used at the same time. This was because logrotate searched for a file with the "gz" suffix, however the file had not yet been compressed. The underlying source code has been modified, and logrotate correctly finds and sends the file under these circumstances.

All users of logrotate are advised to upgrade to these updated packages, which fix this bug.

7.133. LOHIT-TELUGU-FONTS

7.133.1. RHBA-2012:1212 — lohit-telugu-fonts bug fix update

An updated lohit-telugu-fonts package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The lohit-telugu-fonts package provides a free Telugu TrueType/OpenType font.

Bug Fix

BZ#640610

Due to a bug in the lohit-telugu-fonts package, four certain syllables were rendering incorrectly. This bug has been fixed and these syllables now render correctly.

All users of lohit-telugu-fonts are advised to upgrade to this updated package, which fixes this bug.

7.134. LUCI

7.134.1. RHBA-2013:0309 — luci bug fix and enhancement update

Updated luci packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The luci packages contain a web-based high-availability cluster configuration application.

Bug Fixes

BZ#807344

Previously, the resource and service names in the **/etc/cluster/cluster.conf** configuration file that contained non-standard characters, like hash (#), question mark (**?**), or slash (**/**), were not properly handled by the **luci** application. Consequently, when processing such configuration file, **luci** failed with the following message:

```
Error 500
We're sorry but we weren't able to process this request.
```

This bug has been fixed, and **luci** now handles resources and services whose names contain the aforementioned characters without complications.

BZ#815666

When the **fence** instance was configured with the ***delay*** attribute in the **/etc/cluster/cluster.conf** file, the **luci** application ignored the subsequently enabled **unfence** instance that was configured without the ***delay*** attribute. The unfence status was incorrectly displayed as disabled in the **luci** interface, but unfencing was performed without complications. With this update, the underlying source code has been modified to address this issue. As a result, unfence is now properly reported in **luci**.

BZ#826951

Previously, it was possible to create a fencing device with an invalid name (starting with a number) using the **luci** application. The device was successfully created, but the **/etc/cluster/cluster.conf** file did not pass the schema validation check. The bug has been fixed, and a warning message is now displayed to prevent users from setting invalid device names in the **/etc/cluster/cluster.conf** file.

BZ#853151

Previously, certain errors related to the communication between the **luci** and **ricci** applications could have been dropped without notification to the user. Also, the following message could occur in the **/var/log/luci/luci.log** file:

```
No object (name: translator) has been registered for this thread
```

With this update, this behavior has been modified and the described errors are now properly written to the log file.

BZ#856253

Prior to this update, a double click on the **Connect** button in the **Add Existing Cluster** dialog window led to listing the cluster twice. With this update, the underlying source code has been modified to address this issue, and the cluster is now listed only once regardless of how many times the **Connect** button was pressed.

BZ#860042

Previously, when attempting to create a service that referenced the same global resource twice, the **luci** application terminated unexpectedly with the following message:

```
A resource named "<name>" already exists
```

This bug has been fixed, and **luci** now accepts multiple references inside a service group.

BZ#877188

Previously, the **luci** application allowed the **`max_restarts`**, **`__max_restarts`**, and **`__max_failures`** variables to be set without setting their corresponding timeout variables (**`restart_expire_time`**, **`__restart_expire_time`**, **`__failure_expire_time`**), and in the opposite way. This behavior has been changed, and an error is now issued in case the corresponding variables are not set.

BZ#877392

When the self_fence property was enabled using the **`luci`** interface, the corresponding entry in the **`/etc/cluster/cluster.conf`** file was written incorrectly. A value was assigned in the form of **`self_fence="on"`** instead of **`self_fence="1"`** or **`self_fence="yes"`**. Consequently, fencing actions failed. The bug has been fixed, and self_fence is now assigned with the correct value. As a result, fencing now works properly when enabled with **luci**.

BZ#881796

Certain previous versions of Microsoft Internet Explorer incorrectly processed JavaScript files containing trailing commas. Consequently, several dialog windows of the **luci** interface were affected. With this update, the trailing commas have been removed from luci JavaScript files to assure proper **luci** functionality in older versions of Microsoft Internet Explorer.

BZ#881955

Prior to this update, resource and service attributes that accept boolean input did not use consistent values to denote enabled or disabled status. The accepted values were: **`1`** or **`0`**, **`on`** or **`off`**, **`yes`** or **`no`**, **`true`** or **`false`**. With this update, only the values **`1`** or **`0`** are accepted in attributes that use boolean input.

BZ#882995

Previously, after renaming a fencing device with an enabled **`unfence`** option, this **`unfence`** instance was not updated with the new name and referred to a non-existent device. This bug has been fixed, and an **`unfence`** reference is now correctly updated when a fencing device was renamed.

BZ#886678

Prior to this update, the **luci** resource template searched for the ***`oracletype`*** attribute instead of ***`type`*** when processing the **`/etc/cluster/cluster.conf`** file. Consequently, the oracledb attribute was always displayed as **`Default`** in the **luci** interface, regardless of its actual assigned value. This bug has been fixed, and ***`oracletype`*** type is now correctly displayed by **luci**.

Enhancements

BZ#740867

With this update, support for the IBM iPDU fence device has been added to the **luci** application.

BZ#809892

With this update, a new user table has been added to the **Admin**/**User** and **Permissions** pages of the **luci** interface. It is now possible to remove users from **luci**.

BZ#821928

With this update, support for configuring the ***`privlvl`*** (privilege level) attribute used by the **fence_ipmilan** fencing agent has been added to the **luci** application. As a result, ***`privlvl`*** can now be successfully configured by **luci**.

BZ#822502

With this update, support for the **`nfsrestart`** option for the file system and cluster file system resource agents has been added to the **luci** application. This option provides a way to forcefully restart NFS servers and allow a clean unmount of an exported file system.

BZ#865300

This update adds the **fence_eaton** agent to support Eaton ePDU (Enclosure Power Distribution Unit) devices in Red Hat Enterprise Linux 6, into the luci package.

BZ#865533

With this update, an interface for configuring and displaying the **fence_hpblade** fence devices has been added to the **luci** application.

Users of luci are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.134.2. RHBA-2013:1445 — luci bug fix update

Updated luci packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The luci package provides a web-based high-availability cluster configuration application.

Bug Fixes

BZ#969328

Previously, luci did not include concurrent additions to parameters for some fence devices (including "cmd_prompt", "login_timeout", "power_timeout", "retry_on", "shell_timeout") or respective instances ("delay") as happened in the fence-agents package. Consequently, the valid parameters could be dropped from the respective part of the configuration upon submitting the dedicated forms in luci. This update restores the capability of luci to work with a full intended set of fence agents parameters and, in turn, prevents luci from unexpectedly discarding the already configured ones.

BZ#996423

Previously, luci did not include concurrent additions to fence devices coverage as happened in the fence-agents package. Consequently, Dell iDRAC (idrac), HP iLO2 (ilo2), HP iLO3 (ilo3), and IBM Integrated Management Module (imm) devices or agents were not honored in luci, leading to an inability to properly work with or to setup a cluster comprising them. This update restores the capability of luci to work with a full intended set of fence devices.

Users of luci are advised to upgrade to these updated packages, which fix these bugs.

7.135. LVM2

7.135.1. RHBA-2013:0501 — lvm2 bug fix and enhancement update

Updated lvm2 packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The lvm2 packages provide support for Logical Volume Management (LVM).

Bug fixes

BZ#837927

When creating a RAID Logical Volume, if the **`--regionsize(-R)`** option (used with the **`lvcreate`** command) was not specified, LVs larger than 2 TB could not be created or extended. Consequently, creating or extending such volumes caused errors. With this update, the region size is automatically adjusted upon creation or extension and large LVs can now be created.

BZ#834703

Extending a RAID 4/5/6 Logical Volume failed to work properly because the parity devices were not properly accounted for. This has been corrected by covering the "simple" case where the LV is extended with the same number of stripes as the original (reducing or extending a RAID 4/5/6 LV with different number of stripes is not implemented yet). As a result, it is now possible to extend a RAID 4/5/6 Logical Volume.

BZ#832392

When the **`issue_discards=1`** configuration option was used or configured in the **`/etc/lvm/lvm.conf`** file, moving Physical Volumes via the **`pvmove`** command resulted in data loss. The problem has been fixed with this update.

BZ#713599, BZ#800801

Device-mapper devices (including LVM devices) were not deactivated at system shutdown or reboot. Consequently, when device-mapper devices were layered on the top of other block devices and these were detached during the shutdown or reboot procedure, any further access to the device-mapper devices ended up with either I/O errors or an unresponsive system as the underlying devices were unreachable (for example iSCSI or FCoE devices). With this update, a new **`blkdeactivate`** script along with **`blk-availability`** shutdown script have been provided. These scripts unmount and deactivate any existing device-mapper devices before deactivating and detaching the underlying devices on shutdown or reboot. As a result, there are no I/O errors or hangs if using attached storage that detaches itself during the shutdown or reboot procedure.

BZ#619574

An LVM mirror can be created with three different types of log devices: core (in-memory), disk, and mirrored. The *mirrored* log is itself redundant and resides on two different Physical Volumes. Previously, if both devices composing the mirror log were lost, they were not always properly replaced during repair, even if spare devices existed. With this update, a *mirrored* log is properly replaced with a *mirrored* log if there are sufficient replacement PVs.

BZ#832120, BZ#743505

A mirror Logical Volume can itself have a mirrored log device. When a device in an image of the mirror and its log failed at the same time, it was possible for unexpected I/O errors to appear on the mirror LV. The kernel did not absorb the I/O errors from the failed device by relying on the remaining device. This bug then caused file systems built on the device to respond to the I/O errors (turn read-only in the case of the ext3/4 file systems). The cause was found to be that the mirror was not suspended for repair using the **noflush** flag. This flag allows the kernel to re-queue I/O requests that need to be retried. Because the kernel was not allowed to re-queue the requests, it had no choice but to return the I/O as errored. This bug has been corrected by allowing the log to be repaired first, thus, the top-level mirror's log can be completed successfully. As a result, the mirror is now properly suspended with the **noflush** flag.

BZ#803271

When using the **lvmetad** daemon (**global/use_lvmetad=1** LVM2 configuration option) while processing LVM2 commands in a cluster environment (**global/locking_type=3**), the LVM2 commands did not work correctly and issued various error messages. With this update, if clustered locking is set, the **lvmetad** daemon is disabled automatically as this configuration is not yet supported with LVM2. As a result, there is now a fallback to non-lvmetad operation in LVM2, if clustered locking is used and a warning message is issued:

```
WARNING: configuration setting the use_lvmetad parameter overriden to 0
due to the locking_type 3 parameter. Clustered environment is not
supported by the lvmetad daemon yet.
```

BZ#855180

When the user tried to convert a thin snapshot volume into a read-only volume, internal error messages were displayed and the operation failed. With this update, thin snapshot volumes can be converted to read-only mode. Also for the conversion of the thin pool to read-only mode, en explicit error message about an unsupported feature is added.

BZ#801571

Previously, if a device failed while a RAID Logical Volume was not in-sync, any attempts to fix it failed. This case is now handled, however the following limitations are to be noted:

1. The user cannot repair or replace devices in a RAID Logical Volume that is not active. The tool (the **lvconvert -repair** command) must know the sync status of the array and can only get that when the array is active.

2. The user cannot replace a device in a RAID Logical Volume that has not completed its initial synchronization. Doing so would produce unpredictable results and is therefore disallowed.

3. The user can repair a RAID Logical Volume that has not completed its initial synchronization, but some data may not be recoverable because it had not had time to make that data fully redundant. In this case, a warning is printed and the user is queried if they would like to proceed.

BZ#871058

A race condition in the **lvmetad** daemon occasionally caused LVM commands to fail intermittently, failing to find a VG that was being updated at the same time by another command. With this update, the race condition does no longer occur.

BZ#857554

If the **issue_discards** option was enabled in the configuration file and the **lvremove** command ran against a partial Logical Volume where Physical Volumes were missing, the **lvremove** command terminated unexpectedly. This bug has been fixed. Also, the new **p** attribute in the LVS command output is set when the Logical Volume is partial.

BZ#820116

Previously, when there was a Physical Volume in the Volume Group with zero Physical Extents (PEs), so the Physical Volume was used to store metadata only, the **`vgcfgrestore`** command failed with a *"Floating point exception"* error, because the command attempted to divide by zero. A proper check for this condition has been added to prevent the error and now, after using the **`vgcfgrestore`** command, VG metadata is successfully written.

BZ#820229

Previously, when attempting to rename thin Logical Volumes, the procedure failed with the following error message:

```
"lvrename Cannot rename <volume_name>: name format not recognized for
internal LV <pool_name>"
```

This bug is now fixed and the user can successfully rename thin Logical Volumes.

BZ#843546

Previously, it was not possible to add a Physical Volume to a Volume Group if a device failure occurred in a RAID Logical Volume and there were no spare devices in the VG. Therefore users could not replace the failed devices in a RAID LV and the VG could not be made consistent without physically editing LVM metadata. It is now possible to add a PV to a VG with missing or failed devices and to replace failed devices in a RAID LV with the **`lvconvert --repair <vg>/<LV>`** command.

BZ#855398

An improper restriction placed on mirror Logical Volumes caused them to be ignored during activation. Users were unable to create Volume Groups on top of clustered mirror LV and could not recursively stack cluster VG. The restriction has been refined to pass over mirrors that cause LVM commands to block indefinitely and it is now possible to layer clustered VG on clustered mirror LV.

BZ#865035

When a device was missing from a Volume Group or Logical Volume, tags could not be added or removed from the LV. If the activation of an LV was based on tagging using the ***`volume_list`*** parameter in the configuration file (**`lvm.conf`**), the LV could not be activated. This affected High Availability LVM (HA-LVM) and without the ability to add or remove tags while a device was missing, RAID LVs in **HA-LVM** configuration could not be used. This update allows **`vgchange`** and **`lvchange`** to alter the LVM metadata for a limited set of options while PVs are missing. The "- --[add|del]" tag is included and the set of allowable options do not cause changes to the device-mapper kernel target and do not alter the structure of the LV.

BZ#845269

When an LVM command encountered a response problem with the **`lvmetad`** daemon, the command could cause the system to terminate unexpectedly with a segmentation fault. Currently, LVM commands work properly with **`lvmetad`** and crashes no longer occur even if there is a malformed response from **`lvmetad`**.

BZ#823918

A running LVM process could not switch between the **`lvmetad`** daemon and non-lvmetad modes of operation and this caused the LVM process to terminate unexpectedly with a segmentation fault when polling for the result of running **`lvconvert`** operation. With this update, the segmentation fault no longer occurs.

BZ#730289

The **clvmd** daemon consumed a lot of memory resource to process every request. Each request invoked a thread, and by default each thread allocated approximately 9 MB of RAM for stack. To fix this bug, the default thread's stack size has been reduced to 128 KB which is enough for the current version of LVM to handle all tasks. This leads to massive reduction of memory used during runtime by the **clvmd** daemon.

BZ#869254

Previously, disabling the **udev** synchronisation caused **udev** verification to be constantly enabled, ignoring the actual user-defined setting. Consequently, **libdevmapper**/LVM2 incorrectly bypassed **udev** when processing relevant nodes. The **libdevmapper** library has been fixed to honor the actual user's settings for **udev** verification. As a result, **udev** works correctly even in case the **udev** verification and **udev** synchronization are disabled at the same time.

BZ#832033

Previously, when using the **lvmetad** daemon, passing the **--test** argument to commands occasionally caused inconsistencies in the **lvmetad** cache that **lvmetad** maintains. Consequently, disk corruption occurred when shared disks were involved. An upstream patch has been applied to fix this bug.

BZ#870248

Due to a missing dependency on the device-mapper-persistent-data thin pool devices were not monitored on activation. Consequently, unmonitored pools could overfill the configured threshold. To fix this bug, the code path for enabling monitoring of thin pool has been fixed and the missing package dependency added. As a result, when monitoring for thin pool is configured, the **dmeventd** daemon is enabled to watch for pool overfill.

BZ#836653

A failed attempt to reduce the size of a Logical Volume was sometimes not detected and the **lvremove** command exited successfully even though it had failed to operate the LV. With this update, **lvremove** returns the right exit code in the described scenario.

BZ#836663

When using a Physical Volume (PV) that contained ignored metadata areas, an LVM command, such as **pvs**, could incorrectly display the PV as being an orphan due to the order of processing individual PV in the VG. With this update, the processing of PVs in a VG has been fixed to properly account for PVs with ignored metadata areas so that the order of processing is no longer important, and LVM commands now always give the same correct result, regardless of PVs with ignored metadata areas.

BZ#837599

Issuing the **vgscan --cache** command (to refresh the **lvmetad** daemon) did not remove data about Physical Volumes or Volume Groups that no longer existed — it only updated metadata of existing entities. With this update, the **vgscan --cache** command removes all metadata that are no longer relevant.

BZ#862253

When there were numerous parallel LVM commands running, the **lvmetad** daemon could deadlock and cause other LVM commands to stop responding. This behavior was caused by a race condition in **lvmetad's** multi-threaded code. The code has been improved and now the parallel commands succeed and no deadlocks occur.

BZ#839811

Previously, the first attribute flag was incorrectly set to **S** when an invalid snapshot occurred, whereas this value in the first position is supposed to indicate a merging snapshot. Invalid snapshot is normally indicated by capitalizing the fifth Logical Volume attribute character. This bug has been fixed and the **lvs** utility no longer capitalizes the first LV attribute character for invalid snapshots but the fifth, as required.

BZ#842019

Previously, it was possible to specify incorrect arguments when creating a RAID Logical Volume, which could harmfully affect the created device. These inappropriate arguments are no longer allowed.

BZ#839796

Due to incorrect handling of sub-Logical-Volumes (LVs), the **pvmove** utility was inconsistent and returned a misleading message for RAID. To fix this bug, **pvmove** has been disallowed from operating on RAID LVs. Now, if it is necessary to move a RAID LV's components from one device to another, the **lvconvert --replace <old_pv> <vg>/<lv> <new_pv>** command is used.

BZ#836381

The kernel does not allow adding images to a RAID Logical Volume while the array is not synchronized. Previously, the LVM RAID code did not check whether the LV was synchronized. As a consequence, an invalid request could be issued, which caused errors. With this update, the aforementioned condition is checked and the user is now informed that the operation cannot take place until the array is synchronized. The kernel does not allow to add additional images to a RAID Logical Volume when the array is not synchronized. Previously, the LVM RAID code did not check whether the LV was in synchronized condition, which could have caused invalid requests. With this update, LVM RAID has been modified to check for the aforementioned condition and the user is now informed in case the operation is stopped due to unsynchronized array.

BZ#855171, BZ#855179

Prior to this update, the conversion of a thin pool into a mirror resulted in an aborting error message. As this conversion is not supported, an explicit check which prohibits this conversion before the **lvm** utility attempts to perform it has been added. Now, the error message returns an explicit error message stating that the feature is not supported.

BZ#822248

Prior to this update, RAID Logical Volumes could become corrupted if they were activated in a clustered Volume Group. To fix this bug, a VG is no longer allowed to be changed to a clustered VG if there are RAID LVs in a VG.

BZ#822243

Previously, it was possible to create RAID Logical Volumes in a clustered Volume Group. As RAID LVs are not cluster capable and activating them in a cluster could cause data damage, the ability to create RAID LVs in a cluster has been disabled.

BZ#821007

Previously, if no last segment on an pre-existing Logical Volume was defined, the normal **cling** allocation policy was applied and an LV could be successfully created or extended even though there was not enough space on a single Physical Volume and no additional PV was defined in the **lvm.conf** file. This update corrects the behavior of the **cling** allocation policy and any attempts to create or extend an LV under these circumstances now fail as expected.

BZ#814782

The interaction of LVM filters and **`lvmetad`** could have lead to unexpected and undesirable results. Also, updates to the "filter" settings while the **`lvmetad`** daemon was running did not force **`lvmetad`** to forget the devices forbidden by the filter. Since the normal "filter" setting in the **`lvm.conf`** file is often used on the command line, a new option has been added to **`lvm.conf`** (global_filter) which also applies to **`lvmetad`**. The traditional "filter" settings only applies at the command level and does not affect device visibility to **`lvmetad`**. The options are documented in more detail in the example configuration file.

BZ#814777

Prior to this update, the **`lvrename`** utility did not work with thin provisioning (pool, metadata, or snapshots) correctly. This bug has been fixed by implementing full support for stacked devices. Now, **`lvrename`** handles all types of thin Logical Volumes as expected.

BZ#861456

When creating a Logical Volume using the **`lvcreate`** command with the **`--thinpool`** and **`--mirror`** options, the **`thinpool`** flag was ignored and a regular Logical Volume was created. With this update, use of the **`--thinpool`** option with the **`--mirror`** option is no longer allowed and the **`lvcreate`** command fails with a proper error message under these circumstances.

BZ#861841

Previously, the **`lvm_percent_to_float()`** function declared in the **`lvm2app.h`** header file did not have an implementation in the **`lvm2app`** library. Any program, which tried to use this function, failed at linking time. A patch for **`lvm2app.h`** has been applied to fix this bug and **`lvm_percent_to_float()`** now works as expected.

BZ#813766

Prior to this update, the LVM utilities returned spurious warning messages during the boot process, if the **`use_lvmetad = 1`** option was set in the **`lvm.conf`** file. This has been fixed and warning messages are no longer issued during boot.

BZ#862095

Due to the unimplemented **`<data_percent>`** property for the **`lvm2app`** library, incorrect value **`-1`** was returned for thin volumes. This bug has been fixed by adding proper support for the **`lvm_lv_get_property(lv, <data_percent>)`** function. Now, **`lvm2app`** returns correct values.

BZ#870534

Due to a wrong initialization sequence, running an (LVM) command caused the LVM utility to abort instead of proceeding with scanning-based metadata discovery (requested by using the **`--config "global{use_lvmetad=0"}`** option). This bug occurred only when an LVM command was run with **`lvmetad`** cache daemon running. The bug has been fixed and LVM no longer aborts.

BZ#863401

Previously, the **`pvscan --cache`** command failed to read part of LVM1 metadata. As a consequence, when using LVM1 (legacy) metadata and the **`lvmetad`** daemon together, LVM commands could run into infinite loops when invoked. This bug has been fixed and LVM1 and **`lvmetad`** now work together as expected.

BZ#863881

Due to the missing **`lvm2app`** library support, incorrect values for thin snapshots **`origin`** field were reported. A patch has been updated to return the correct response to the **`lvm_lv_get_property(lv, "origin")`** function.

BZ#865850

Previously, the degree to which RAID 4/5/6 Logical Volumes had completed their initial array synchronization (i.e. initial parity calculations) was not printed in the **`lvs`** command output. This information is now included under the heading that has been changed from **`Copy%`** to **`Cpy%Sync`**. Users can now request the **`Cpy%Sync`** information directly via **`lvs`** with either the **`lvs -o copy_percent`** or the **`lvs -o sync_percent`** option.

BZ#644752

Previously, when using Physical Volumes, the exclusive lock was held to prevent other PVs commands to run concurrently in case any Volume Group metadata needed to be read in addition. This is not necessary anymore when using **`lvmetad`** as **`lvmetad`** caches VG metadata and thus avoids taking the exclusive lock. As a consequence, numerous PVs commands reading VG metadata can be run in parallel without the need for the exclusive lock.

BZ#833180

Attempting to convert a linear Logical Volume to a RAID 4/5/6 Logical Volume is not allowed. When the user tried to execute this operation, a message indicating that the original LV had been **`striped`** instead of **`linear`**, was returned. The messages have been updated to provide correct information and only messages with correct and relevant content are now returned under these circumstances.

BZ#837114

Previously, an attempt to test the **`create`** command of a RAID Logical Volume resulted in failure even though the process itself succeeded without the **`--test`** argument of the command. With this update, a test run of the **`create`** command now properly indicates success if the command is successful.

BZ#837098

Previously, a user-instantiated resynchronization of a RAID Logical Volume failed to cause the RAID LV to perform the actual resynchronization. This bug has been fixed and the LV now performs the resynchronization as expected.

BZ#837093

When a RAID or mirror Logical Volume is created with the **`--nosync`** option, an attribute with this information is attached to the LV. Previously, a RAID1 LV did not clear this attribute when the LV was converted to a linear LV and back, even though it underwent a complete resynchronization in the process. With this update, **`--nosync`** has been fixed and the attribute is now properly cleared after the LV conversion.

BZ#836391

Due to an error in the code, user-initiated resynchronization of a RAID Logical Volume was ineffective. With this update, the **`lvchange --resync`** command has been added on a RAID LV, which makes the LV undergo complete resynchronization.

BZ#885811

Previously, an error in the Volume Group (VG) auto-activation code could cause LVM commands to terminate unexpectedly with the following message:

```
Internal error: Handler needs existing VG
```

With this update, cached VG metadata are used instead of relying on an absent MDA content of the last discovered PV. As a result, the aforementioned error no longer occurs.

BZ#885993

Prior to this update, testing the health status of the **`mirror`** utility caused a minor memory leak. To fix this bug, all resources taken in the function have been released, and memory leaks for longterm living processes (such as the **`dmeventd`** daemon) no longer occur.

BZ#887228

Previously, a nested mutex lock could result in a deadlock in the **`lvmetad`** daemon. As a consequence, Logical Volume Manager (LVM) commands trying to talk to **`lvmetad`** became unrepsonsive. The nested lock has been removed, and the deadlock no longer occurs.

BZ#877811

Previously, the **`lvconvert`** utility handled the **`-y`** and **`-f`** command line options inconsistently when repairing mirror or RAID volumes. Whereas the **`-f`** option alone worked correctly, when used along with the **`-y`** option, the **`-f`** option was ignored. With this update, **`lvconvert`** handles the **`-f`** option correctly as described in the manual page.

BZ#860338

When Physical Volumes were stored on read-only disks, the **`vgchange -ay`** command failed to activate any Logical Volumes and the following error message was returned:

```
/dev/dasdf1: open failed: Read-only file system
device-mapper: reload ioctl failed: Invalid argument
1 logical volume(s) in volume group "v-9c0ed7a0-1271-452a-9342-
60dacafe5d17" now active
```

However, this error message did not reflect the nature of the bug. With this update, the command has been fixed and Volume Group can now be activated on a read-only disk.

BZ#832596

An error in the space allocation logic caused Logical Volume creation with the **`--alloc anywhere`** option to occasionally fail. RAID 4/5/6 systems were particularly affected. The bug was fixed to avoid picking already-full areas for RAID devices.

Enhancements

BZ#783097

Previously, the **`device-mapper`** driver UUIDs could have been used to create the **`/dev`** content with the **`udev`** utility. If mangling was not enabled, **`udev`** created incorrect entries for UUIDs containing unsupported characters. With this update, character-mangling support in the **`libdevmapper`** library and the **`dmsetup`** utility for characters not on the udev-supported whitelist has been enhanced to process **`device-mapper`** UUIDs the same way as **`device-mapper`** names are. The UUIDs and names are now always controlled by the same mangling mode, thus the existing **`--manglename dmsetup`** option affects UUIDs as well. Furthermore, the **`dmsetup info -c -o`** command has new fields to display: ***`mangled_uuid`*** and ***`unmangled_uuid`***.

BZ#817866, BZ#621375

Previously, users had to activate Volume Groups and Logical Volumes manually by calling **vgchange/lvchange -ay** on the command line. This update adds the autoactivation feature, LVM2 now lets the user specify precisely which Logical Volumes should be activated at boot time and which ones should remain inactive. Currently, the feature is supported only on non-clustered and complete VGs. Note that to activate the feature, **lvmetad** must be enabled (**global/use_lvmetad=1** LVM2 configuration option).

BZ#869402

The manual page for the **lvconvert** utility has been updated with new supported options for conversion of existing volumes into a thin pool.

BZ#814732

Previously, the user could not specify conversion of an Logical Volume already containing pool information ("pre-formatted LV") into a legitimate thin pool LV. Furthermore, it was rather complex to guide the allocation mechanism to use proper Physical Volumes (PVs) for data and metadata LV. As the **lvconvert** utility is easier to use in these cases, **lvconvert** has been enhanced to support conversion of pre-formatted LVs into a thin pool volume. With the **--thinpool data_lv_name** and **--poolmetadata metadata_lv_name** options, the user may use a pre-formatted LV to construct a thin pool as with the **lvcreate** utility.

BZ#636001

A new optional metadata caching daemon (**lvmetad**) is available as part of this LVM2 update, along with **udev** integration for device scanning. Repeated scans of all block devices in the system with each LVM command are avoided if the daemon is enabled. The original behavior can be restored at any time by disabling **lvmetad** in the **lvm.conf** file.

BZ#814766

Previously, no default behavior could be used to fine-tune performance of some workloads. Now, the thin pool support has been enhanced with configurable discards support. The user may now select from three types of behavior: **passdown** is default and allows to pass-through discard requests to the thin pool backing device; **nopassdown** processes allows discards only on the thin pool level and requests are not passed to the backing device; **ignore** allows ignoring of discard request.

BZ#844492

LVM support for 2-way mirror RAID10 has been added. LVM is now able to create, remove, and resize RAID10 Logical Volumes. To create a RAID10 Logical Volume, specify individual RAID parameters similarly as for other RAID types, like in the following example:

```
~]# lvcreate --type raid10 -m 1 -i 2 -L 1G -n lv vg
```

Note that the **-m** and **-i** arguments behave in the same way they would for other segment types. That is, **-i** is the total number of stripes while **-m** is the number of (additional) copies (that is, **-m 1 -i 2** gives 2 stripes on the top of 2-way mirrors).

BZ#861843

The **lvm2app** library now reports the data_percent field which indicates how full snapshots, thin pools and volumes are. The Logical Volume needs to be active to obtain this information.

BZ#814824

The thin pool now supports non-power-of-2 chunk size. However, the size must be a multiple of 64KiB.

BZ#823660

The **-l** option has been added to the **lvmetad** daemon to allow logging of wire traffic and more detailed information on internal operation to the **standard error** stream. This new feature is mainly useful for troubleshooting and debugging.

BZ#834031

Previously, it was possible to pass an incorrect argument on the command line when creating a RAID Logical Volume, for example the **--mirrors** command for RAID5. Consequently, erroneous and unexpected results were produced. With this update, invalid arguments are caught and reported.

BZ#823667

The **lvmdump** utility has been extended to include a dump of the internal **lvmetad** daemon state, helping with troubleshooting and analysis of **lvmetad**-related problems.

BZ#830250

In Red Hat Enterprise Linux 6.4, LVM adds support for Micron PCIe Solid State Drives (SSDs) as devices that may form a part of a Volume Group.

BZ#883416

The **DM_DISABLE_UDEV** environment variable is now recognized and takes precedence over other existing setting when using LVM2 tools, dmsetup and libdevmapper to fallback to non-udev operation. Setting the **DM_DISABLE_UDEV** environment variable provides a more convenient way of disabling udev support in libdevmapper, dmsetup and LVM2 tools globally without a need to modify any existing configuration settings. This is mostly useful if the system environment does not use **udev**.

BZ#829221

Physical Volumes (PV) are now automatically restored from the *missing* state after they become reachable again and even if they had no active metadata areas. In cases of transient inaccessibility of a PV, for example with Internet Small Computer System Interface (iSCSI) or other unreliable transport, LVM required manual action to restore a PV for use even if there was no room for conflict, because there was no active metadata area (MDA) on the PV. With this update, the manual action is no longer required if the transiently inaccessible PV has no active metadata areas.

Users of lvm2 should upgrade to these updated packages, which fix these bugs and add these enhancements.

7.135.2. RHBA-2013:1504 — lvm2 bug fix update

Updated lvm2 packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The lvm2 packages include all of the support for handling read and write operations on physical volumes, creating volume groups from one or more physical volumes and creating one or more logical volumes in volume groups.

Bug Fix

BZ#1024911

> When there were visible clustered Volume Groups in the system, it was not possible to silently skip them with proper return error code while non-clustered locking type was used (the global/locking_type lvm.conf setting). To fix this bug, "--ignoreskippedcluster" option has been added for several LVM commands (pvs, vgs, lvs, pvdisplay, vgdisplay, lvdisplay, vgchange, and lvchange). With this option, the clustered Volume Groups are skipped correctly while the return error code does not depend on these clustered Volume Groups.

Users of lvm2 are advised to upgrade to these updated packages, which fix this bug.

7.135.3. RHBA-2013:1471 — lvm2 bug fix update

Updated lvm2 packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The lvm2 packages include all of the support for handling read and write operations on physical volumes, creating volume groups from one or more physical volumes and creating one or more logical volumes in volume groups.

Bug Fixes

BZ#965810

> Previously, on certain HP servers using Red Hat Enterprise Linux 6 with the xfs file system, a regression in the code caused the lvm2 utility to ignore the "optimal_io_size" parameter and use a 1MB offset start. Consequently, there was an increase in the disk write operations which caused data misalignment and considerably lowered the performance of the servers. With this update, lvm2 no longer ignores "optimal_io_size" and data misalignment no longer occurs in this scenario.

BZ#965968

> The lvm2 tools determine the PowerPath major number by searching for an "emcpower" line in the /proc/devices file. Previously, some versions of PowerPath used the ID string "power2". As a consequence, on systems with such an identifier, PowerPath devices were not given the expected precedence over PowerPath components which exhibit the same physical volume UUID. With this update, detection of EMC power devices works as expected, and the priority of devices is now set properly.

BZ#1016083

> Due to an error in the LVM allocation code, lvm2 attempted free space allocation contiguous to an existing striped space. When trying to extend a 3-way striped logical volume using the lvextend command, the lvm2 utility terminated unexpectedly with a segmentation fault. With this update, the behavior of LVM has been modified, and lvextend now completes the extension without a segmentation fault.

Users of lvm2 are advised to upgrade to these updated packages, which fix these bugs.

7.136. MAILMAN

7.136.1. RHBA-2012:1474 — mailman bug fix update

Updated mailman packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

Mailman is a program used to help manage e-mail discussion lists.

Bug Fixes

BZ#772998

The reset_pw.py script contained a typo, which could cause the mailman utility to fail with a traceback. The typo has been corrected, and mailman now works as expected.

BZ#799323

The "urlhost" argument was not handled in the newlist script. When running the "newlist" command with the "--urlhost" argument specified, the contents of the index archive page was not created using proper URLs; the hostname was used instead. With this update, "urlhost" is now handled in the newlist script. If the "--urlhost" argument is specified on the command line, the host URL is used when creating the index archive page instead of the hostname.

BZ#832920

Previously, long lines in e-mails were not wrapped in the web archive, sometimes requiring excessive horizontal scrolling. The "white-space: pre-wrap;" CSS style has been added to all templates, so that long lines are now wrapped in browsers that support that style.

BZ#834023

The "From" string in the e-mail body was not escaped properly. A message containing the "From" string at the beginning of a line was split and displayed in the web archive as two or more messages. The "From" string is now correctly escaped, and messages are no longer split in the described scenario.

All users of mailman are advised to upgrade to these updated packages, which fix these bugs.

7.137. MAN-PAGES-OVERRIDES

7.137.1. RHBA-2013:0464 — man-pages-overrides bug fix update

Updated man-pages-overrides package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The man-pages-overrides package provides a collection of manual (man) pages to complement other packages or update those contained therein.

Bug Fixes

BZ#806845

Prior to this update, documentation about SMBIOS on the dmidecode(8) manual page was unclear. This update fixes the information about SMBIOS on the dmidecode(8) manual page.

BZ#814417

Prior to this update, description of the "-SecurityTypes" option in the TigerVNC utility was missing in the vncviewer(1) and Xvnc(1) manual pages. This update adds a description to the vncviewer(1) and Xvnc(1) manual pages.

BZ#845657

Prior to this update, the localalloc option on the numactl(8) manual page was not clearly described. This update adds a clear description of the localalloc option to the numactl(8) utility.

BZ#846591

Prior to this update, some options were missing from the ipmitool(1) manual page. With this update, all options are described on the ipmitool(1) manual page.

BZ#849201

Previously, the alsaunmute(1) manual page was missing. This update adds the alsaunmute(1) manual page.

BZ#853959

Prior to this update, the "--no-tpm" option was not described in the rngd(8) manual page. This update adds a description of the "--no-tpm" option.

BZ#867332

Prior to this update, the groupmems(8) manual page was missing information about the setuid permission of the groupmems binary. This update clarifies the setuid permission in the groupmems(8) manual page.

BZ#872526

Prior to this update, the dump(8) manual page was missing information about the ext4 file system support. This update adds this information to the dump(8) manual page.

Users of man-pages-overrides are advised to upgrade to this updated package, which fixes these bugs.

7.138. MAN-PAGES

7.138.1. RHBA-2013:0447 — man-pages bug fix and enhancement update

An updated man-pages package that fixes numerous bugs and add two enhancements is now available for Red Hat Enterprise Linux 6.

The man-pages package provides man (manual) pages from the Linux Documentation Project (LDP).

Bug Fixes

BZ#714073

Prior to this update, a manual page for the `fattach()` function was missing. This update adds the `fattach(2)` manual page.

BZ#714074

Prior to this update, a manual page for the `recvmmsg()` call was missing. This update adds the `recvmmsg(2)` manual page.

BZ#714075

Prior to this update, manual pages for the `cciss` and `hpsa` utilities were missing. This update adds the `cciss(4)` and `hpsa(4)` manual pages.

BZ#714078

The **host.conf(5)** manual page contained a description for the unsupported **order** keyword. This update removes the incorrect description.

BZ#735789

Prior to this update, the **clock_gettime(2)**, **clock_getres(2)**, and **clock_nanosleep(2)** manual pages did not mention the **-lrt** option. With this update, the description of the **-lrt** option has been added to the aforementioned manual pages.

BZ#745152

This update adds the description of the **single-request-reopen** to the **resolv.conf(5)** manual page.

BZ#745501

With this update, usage of **SSSD** in the **nsswitch.conf** file is now described in the **nsswitch.conf(5)** manual page.

BZ#745521

With this update, the new **UMOUNT_NOFOLLOW** flag is described in the **umount(2)** manual page.

BZ#745733

Previously, a manual page for the **sendmmsg()** function was missing. This update adds the **sendmmsg(2)** manual page.

BZ#752778

Previously, the **db(3)** manual page was pointing to the non-existent **dbopen(3)** manual page. When the **man db** command was issued, the following error message was returned:

```
fopen: No such file or directory.
```

With this update, the **db(3)** manual page is removed.

BZ#771540

This update adds the missing description of the **TCP_CONGESTION** socket option to the **tcp(7)** manual page.

BZ#804003

Descriptions of some socket options were missing in the **ip(7)** manual page. This update adds these descriptions to the **ip(7)** manual page.

BZ#809564

Prior to this update, the **shmat(2)** manual page was missing the description for the **EIDRM** error code. With this update, this description has been added to the **shmat(2)** manual page.

BZ#822317

The **bdflush(2)** system call manual page was missing information that this system call is obsolete. This update adds this information to the **bdflush(2)** manual page.

BZ#835679

The **nscd.conf(5)** manual page was not listing “services” among valid services. With this update, “services” are listed in the **nscd.conf(5)** manual page as expected.

BZ#840791

Previously, the **nsswitch.conf(5)** manual page lacked information on the search mechanism, particularly about the **notfound** status. This update provides an improved manual page with added description of **notfound**.

BZ#840796

Prior to this update, the behavior of the **connect()** call with the local address set to the **INADDR_ANY** wildcard address was insufficiently described in the **ip(7)** manual page. Possible duplication of the local port after the call was not acknowledged. With this update, the documentation has been reworked in order to reflect the behavior of the **connect()** call correctly.

BZ#840798

Due to the vague description of the **getdents()** function in the **getdents(2)** manual page, the risk of using this function directly was not clear enough. The description has been extended with a warning to prevent incorrect usage of the **getdents()** function.

BZ#840805

The **nscd.conf(5)** manual page was missing descriptions and contained several duplicate entries. With this update, the text has been clarified and redundant entries have been removed.

BZ#857163

Previously, the **tzset(3)** manual page contained an incorrect interval in the description of the start and end format for Daylight Saving Time. Consequently, users thought the number was 1-based rather than 0-based when not using the **J** option. With this update, the manual page has been corrected. The Julian day can be specified with an interval of 0 to 365 and February 29 is counted in leap years when the **J** option is not used.

BZ#857962

The description of the **/proc/sys/fs/file-nr** file in the **proc(5)** manual page was outdated. This update adds the current information to this manual page.

BZ#858278

The **connect(2)** manual page in the Error section listed **EAGAIN** error code instead of **EADDRNOTAVAIL** error code. This update amends the manual page with correct information.

Enhancements

BZ#857162

An update in the **close(2)** man page explains the interaction between system calls **close()** and **recv()** in different threads.

BZ#858240

This update adds the description of the **--version** switch to the **zdump(8)** manual page.

All users of man-pages are advised to upgrade to this updated package, which fixes these bugs and add these enhancements.

7.139. MAN

7.139.1. RHBA-2013:0392 — man bug fix update

Updated man packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The man packages provide the man, apropos, and whatis tools to find information and documentation about the Linux system.

Bug Fix

BZ#815209

Previously, the patch for the man-pages-overrides package ignored localized man pages. Consequently, installing this package also overrode man pages localized in different languages. With this update, this bug has been fixed and man pages from the man-pages-overrides package now override only man pages in the same language.

All users of man are advised to upgrade to these updated packages, which fix this bug.

7.140. MATAHARI

7.140.1. RHBA-2013:0404 — removed packages: matahari

The matahari packages have been removed from Red Hat Enterprise Linux 6.

The matahari packages provide a set of APIs for operating system management that are exposed to remote access over the Qpid Management Framework (QMF).

With this update, an empty package has been provided to ensure that the matahari packages are removed from Red Hat Enterprise Linux 6. (BZ#833109)

All users of matahari are advised to remove these packages.

7.141. MCELOG

7.141.1. RHBA-2013:0285 — mcelog bug fix and enhancement update

Updated mcelog packages that fix numerous bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The mcelog package contains a daemon that collects and decodes Machine Check Exception (MCE) data on AMD64 and Intel 64 machines.

NOTE

The mcelog packages have been upgraded to upstream version 0.6, which provides a number of bug fixes and enhancements over the previous version. (BZ#795931)

Bug Fixes

BZ#851406

The mcelog(8) man page contained incorrect information about usage of the "--supported" flag. This man page has been updated and the information is correct now.

BZ#871249

Previously, the mcelog daemon ignored the 15h microarchitecture family of AMD processors and did not report the Machine Check Exception (MCE) errors. Consequently, reported errors were unavailable to system administrators. The 15h microarchitecture family of AMD processors has been included to the list of supported processors and mcelog reports MCE errors correctly in this case.

Enhancement

BZ#740915

This enhancement adds support for the Intel Core i5 and i7 processors to the mcelog packages.

All users of mcelog are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.142. MDADM

7.142.1. RHBA-2013:0440 — mdadm bug fix update

Updated mdadm packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The mdadm packages contain a utility for creating, managing, and monitoring Linux MD (multiple disk) devices.

NOTE

The mdadm packages have been upgraded to upstream version 3.2.5, which provides a number of bug fixes and enhancements over the previous version. (BZ#812358)

Bug Fixes

BZ#824815

While an Intel Matrix Storage Manager (IMSM) RAID volume was in the process of a reshape, an attempt to stop all arrays could cause an IMSM RAID array to be broken or corrupted. The underlying source code has been modified and mdadm works as expected in the described scenario.

BZ#862565

This update clarifies a number of mdadm license ambiguities.

BZ#878810

The IMSM optional ROM (OpROM) does not support RAID volumes across more than one controller. Previously, creating an IMSM RAID volume across more than one controller caused data loss. With this update, creating an IMSM RAID volume on multiple controllers is forbidden to prevent the data loss.

BZ#880208

Previously, it was possible to create a second RAID1 volume with the size equal to 0. As a consequence, when resyncing the first RAID1 volume was finished, the system became unresponsive. This update applies a patch to correct this error and it is no longer possible to create a second RAID1 volume with the size equal to 0.

BZ#880225

After turning off two disk drives of a RAID1 volume, using the "mdadm --detail" command caused mdadm to terminate unexpectedly with a segmentation fault. This update applies a patch that fixes this bug. Using the "mdadm --detail" command now returns valid information and mdadm no longer crashes in the described scenario.

BZ#820643

This update fixes the map file location in mdadm(8) man page.

Users of mdadm are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.143. MESA

7.143.1. RHBA-2013:0344 — mesa bug fix and enhancement update

Updated mesa packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Mesa provides a 3D graphics API that is compatible with Open Graphics Library (OpenGL). It also provides hardware-accelerated drivers for many popular graphics chips.

NOTE

The mesa packages have been upgraded to upstream version 9.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#835200)

Bug Fixes

BZ#786508, BZ#820746

If the user logged in from Red Hat Enterprise Linux 5 to a Red Hat Enterprise Linux 6 machine by using the "ssh" command with the "-Y" option, an attempt to run an application that uses GLX failed with the "Error: couldn't find RGB GLX visual or fbconfig" error message. This bug has been fixed and the remote login now works as expected.

BZ#885882

Due to an error in the mesa packages, using the multisample anti-aliasing (MSAA) technique with the KWin window manager caused errors in the desktop compositing. This update provides a patch that fixes this bug and MSAA now works correctly with the KWin window manager.

BZ#901627

Previously, when connecting to a remote machine using SSH with the X11 forwarding enabled caused a "failed to load driver: i965" error in the libGL library. With this update, a patch has been provided to fix this bug and drivers are now loaded as expected.

Enhancements

BZ#816661

An accelerated driver for Intel Core i5 and i7 processors has been added to the mesa packages.

BZ#835201

This update adds the new mesa-dril-drivers package to mesa. This package implements support for the DRI1 drivers.

All users of mesa are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.143.2. RHSA-2013:0897 — Important: mesa security update

Updated mesa packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mesa provides a 3D graphics API that is compatible with Open Graphics Library (OpenGL). It also provides hardware-accelerated drivers for many popular graphics chips.

Security Fixes

CVE-2013-1872

An out-of-bounds access flaw was found in Mesa. If an application using Mesa exposed the Mesa API to untrusted inputs (Mozilla Firefox does this), an attacker could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2013-1993

It was found that Mesa did not correctly validate messages from the X server. A malicious X server could cause an application using Mesa to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

All users of Mesa are advised to upgrade to these updated packages, which contain backported patches to correct these issues. All running applications linked against Mesa must be restarted for this update to take effect.

7.144. MICROCODE_CTL

7.144.1. RHBA-2013:0348 — microcode_ctl bug fix and enhancement update

Updated microcode_ctl packages that fix a bug and add various enhancements are now available for Red Hat Enterprise Linux 6.

The microcode_ctl packages provide utility code and microcode data to assist the kernel in updating the CPU microcode at system boot time. This microcode supports all current x86-based, Intel 64-based, and AMD64-based CPU models. It takes advantage of the mechanism built-in to Linux that allows microcode to be updated after system boot. When loaded, the updated microcode corrects the behavior of various processors, as described in processor specification updates issued by Intel and AMD for those processors.

Bug Fix

BZ#740932

Previously, a udev rule in /lib/udev/rules.d/89-microcode.rules allowed the module to load more than once. On very large systems (for example, systems with 2048 or more CPUs), this could result in the system becoming unresponsive on boot. With this update, the udev rule has been changed to ensure the module loads only once. Very large systems now boot as expected.

Enhancements

BZ#818096

The Intel CPU microcode file has been updated to version 20120606.

BZ#867078

The AMD CPU microcode file has been updated to version 20120910.

All users of microcode_ctl are advised to upgrade to these updated packages, which fix this bug and add these enhancements. Note: a system reboot is necessary for this update to take effect.

7.145. MLOCATE

7.145.1. RHBA-2012:1355 — mlocate bug fix update

Updated mlocate packages that fix two bugs are now available for Red Hat Enterprise 6.

The mlocate packages provide a locate/updatedb implementation. Mlocate keeps a database of all existing files and allows you to look up files by name.

Bug Fixes

BZ#690800

Prior to this update, the locate(1) manual page contained a misprint. This update corrects the misprint.

BZ#699363

Prior to this update, the mlocate tool aborted the "updatedb" command if an incorrect filesystem implementation returned a zero-length file name. As a consequence, the locate database was not be updated. This update detects invalid zero-length file names, warns about them, and continues to the locate database.

All users of mlocate are advised to upgrade to these updated packages, which fix these bugs.

7.146. MOD_AUTHZ_LDAP

7.146.1. RHBA-2012:1389 — mod_authz_ldap bug fix update

Updated mod_authz_ldap packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The mod_authz_ldap packages provide a module for the Apache HTTP Server to authenticate users against an LDAP database.

Bug Fixes

BZ#607797

Prior to this update, the License field of the mod_authz_ldap packages contained an incorrect tag. This update modifies the license text. Now, the license tag correctly reads "ASL1.0".

BZ#643691

Prior to this update, the mod_authz_ldap module could leak memory. As a consequence, the memory consumption of the httpd process could increase as more requests were processed. This update modifies the underlying code to handle LDAP correctly. Now, the memory consumption as at expected levels.

BZ#782442

Prior to this update, passwords were logged in plain text to the error log when an LDAP bind password was configured if a connection error occurred. This update modifies the underlying code to prevent passwords from being logged in error conditions.

All users of mod_authz_ldap are advised to upgrade to this updated package, which fixes these bugs.

7.147. MOD_NSS

7.147.1. RHBA-2013:0513 — mod_nss bug fix and enhancement update

Updated mod_nss packages that fix one bug and add two enhancements are now available for Red Hat Enterprise Linux 6.

The mod_nss module provides strong cryptography for the Apache HTTP Server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, using the Network Security Services (NSS) security library.

Bug Fix

BZ#769906

The mod_nss module reported 'Required value NSSCipherSuite not set.' even though a value for NSSCipherSuite was present in the virtual host. This bug was a configuration issue which was exacerbated by a couple of confusing log messages. As a result, several log messages were changed to help clarify what values were actually missing.

Enhancements

BZ#816394

Added support for TLSv1.1 to mod_nss module.

BZ#835071

Added the ability to share mod_proxy with other SSL providers.

Users of mod_nss are advised to upgrade to these updated packages, which fix this bug and add these enhancements.

7.148. MOD_REVOCATOR

7.148.1. RHBA-2013:0411 — mod_revocator bug fix update

Updated mod_revocator packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The mod_revocator module retrieves and installs remote Certificate Revocation Lists (CRLs) into an Apache web server.

Bug Fix

BZ#861999

When "exec" URIs were used to configure Certificate Revocate Lists (CRLs), the mod_revocator module failed to load these URIs with the following error message:

Unable to load Revocation module, NSS error -8187. CRL retrieval will be disabled.

A patch has been provided to fix this problem, and CRL URIs are now loaded as expected in this scenario.

Users of mod_revocator are advised to upgrade to these updated packages, which fix this bug.

7.149. MODULE-INIT-TOOLS

7.149.1. RHBA-2013:0442 — module-init-tools bug fix update

Updated module-init-tools packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The module-init-tools packages include various programs needed for automatic loading and unloading of modules under kernels version 2.6 and later, as well as other module management programs. Device drivers and file systems are two examples of loaded and unloaded modules.

Bug Fix

BZ#670653

Previously, the rpmbuild utility received warnings about specific tags being deprecated for module-init-tools. This update fixes the module-init-tools spec file and rpmbuild no longer receives warnings.

Users of module-init-tools are advised to upgrade to these updated packages, which fix this bug.

7.150. MOD_WSGI

7.150.1. RHBA-2012:1358 — mod_wsgi bug fix and enhancement update

Updated mod_wsgi packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The mod_wsgi packages provide a Apache httpd module, which implements a WSGI compliant interface for hosting Python based web applications.

Bug Fix

BZ#670577

Prior to this update, a misleading warning message from the mod_wsgi utilities was logged during startup of the Apache httpd daemon. This update removes this message from the mod_wsgi module.

Enhancement

BZ#719409

With this update, access to the SSL connection state is now available in WSGI scripts using the methods "mod_ssl.is_https" and "mod_ssl.var_lookup".

All users of mod_wsgi are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

7.151. MRTG

7.151.1. RHBA-2012:1449 — mrtg bug fix update

Updated mrtg packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The mrtg packages provide the Multi Router Traffic Grapher (MRTG) to monitor the traffic load on network-links. MRTG generates HTML pages containing Portable Network Graphics (PNG) images, which provide a live, visual representation of this traffic.

Bug Fix

BZ#706519

Prior to this update, the MRTG tool did not handle the socket6 correctly. As a consequence, MRTG reported errors when run on a system with an IPv6 network interface due to a socket conflict. This update modifies the underlying code to socket6 as expected. (#706519)

BZ#707188

Prior to this update, changing the "kMG" keyword in the MRTG configuration could cause the labels on the y-axis to overlap the main area of the generated chart. With this update, an upstream patch has been applied to address this issue, and changing the "kMG" keyword in the configuration no longer leads to the incorrect rendering of the resulting charts.

BZ#836197

Prior to this update, the wrong value was returned from the IBM Fibrechannel switch when using the ifSpeed interface. As a consequence, mrtg cfgmaker failed to use ifHighSpeed on IBM FibreChannel switches. This update modifies the underlying code to return the correct value.

All users of mrtg are advised to upgrade to these updated packages, which fix these bugs.

7.152. MT-ST

7.152.1. RHBA-2012:1409 — mt-st bug fix update

Updated mt-st packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The mt-st package contains the mt and st tape drive management programs. Mt (for magnetic tape drives) and st (for SCSI tape devices) can control rewinding, ejecting, skipping files and blocks and more.

Bug Fix

BZ#820245

Prior this update, the stinit init script did not support standard actions like "status" or "restart". As a consequence, an error code was returned. This update modifies the underlying code to use all use all standard actions.

All users of mt-st are advised to upgrade to these updated packages, which fix this bug.

7.153. NETCF

7.153.1. RHBA-2013:0494 — netcf bug fix update

Updated netcf packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The netcf packages contain a library for modifying the network configuration of a system. Network configuration is expressed in a platform-independent XML format, which netcf translates into changes to the system's "native" network configuration files.

Bug Fix

BZ#886862

Previously, the netcf utility had been calling the nl_cache_mngt_provide() function in the libnl library, which was not thread-safe. Consequently, the libvirtd daemon could terminate unexpectedly. As nl_cache_mngt_provide() was not necessary for proper operation, it is no longer called by netcf, thus preventing this bug.

Users of netcf are advised to upgrade to these updated packages, which fix this bug.

7.154. NET-SNMP

7.154.1. RHBA-2013:0421 — net-snmp bug fix update

Updated net-snmp packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The net-snmp packages provide various libraries and tools for the Simple Network Management Protocol (SNMP), including an SNMP library, an extensible agent, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the `netstat` utility which uses SNMP, and a Tk/Perl Management Information Base (MIB) browser.

Bug Fixes

BZ#829271

Previously, there was a limit of 50 **exec** entries in the **/etc/snmp/snmpd.conf** congiguration file. With more than 50 such entries in the file, the **snmpd** daemon reported the following error message:

```
Error: No further UCD-compatible entries
```

With this update, the fixed limit has been removed, and there can now be any number of **exec** entries in **/etc/snmp/snmpd.conf**.

BZ#848319

Prior to this update, the **libnetsnmpmibs.so.20** and **libnetsnmphelpers.so.20** libraries did not contain an RPATH entry to the libperl.so package for embedding Perl. This could cause problems when linking custom SNMP applications or modules. An upstream patch, which adds RPATH for the Perl libraries, has been provided, and all libperl.so references are now resolved.

BZ#800671

Previously, the **snmpd** daemon ignored the **trapsess -e <engineID>** configuration option in the **/etc/snmp/snmpd.conf** file and sent a default engineID string even if **trapsess** was configured with an explicit engineID value. An upstream patch has been provided to fix this bug and **snmpd** now sends outgoing traps with an engineID string as specified in **/etc/snmp/snmpd.conf**.

BZ#846436

Due to a possible race condition, the **snmpd** daemon could fail to count some processes when filling in the **UCD-SNMP-MIB::prTable** table. With this update, the underlying source code has been adapted to prevent such a race condition, so that all processes are now counted as expected.

BZ#833013

Prior to this update, the **snmpd** daemon ignored the port number of the **clientaddr** option when specifying the source address of outgoing SNMP requests. As a consequence, the system assigned a random port number to the **udp** socket. This update introduces a new configuration option **clientaddrUsesPort**, which, if set to **yes**, allows to specify both the port number and the source IP address in the **clientaddr** option. Now, administrators can increase security with firewall rules and SELinux policies by configuring a specific source port of outgoing traps and other requests.

BZ#851637

When the **snmpd** daemon was shutting down during processing of internal queries, a request was neither marked as failed nor finished, and **snmpd** waited indefinitely for the request to be processed. With this update, **snmpd** marks all internal queries as failed during shutdown.

BZ#842279

Previously, implementation of the **UCD-SNMP-MIB::extCommand** variable in the **snmpd** daemon reported only names of the executable parameters, missing all other command line parameters. With this update, **UCD-SNMP-MIB::extCommand** has been fixed and **snmpd** returns the full command line output.

BZ#784502

Previously, **snmptrapd(8)** manual page did not properly describe how to load multiple configuration files using the **-c** option. With this update, the manual page has been fixed and describes that multiple configuration files must be separated by the comma character.

BZ#846532, BZ#861152

In the previous net-snmp update, implementation of the **HOST-RESOURCES-MIB::hrStorageTable** table was rewritten and devices with CentraVision File System (CVFS) and OpenVZ container file systems (**simfs**) were not reported. With this update, the **snmpd** daemon properly recognizes **CVFS** and **simfs** devices and reports them in **HOST-RESOURCES-MIB::hrStorageTable**.

BZ#846906

When the **snmpd** daemon was not able to expand 32-bit counter provided by the operating system to 64-bits, as required by SNMP standards, the **snmpd** daemon occasionally reported the following error messages:

```
c64 32 bit check failed
```

```
Error expanding XXX to 64bits
```

```
looks like a 64bit wrap, but prev!=new
```

These messages were in fact harmless but confusing. This update suppresses them and they are no longer returned in the described scenario.

BZ#845157

The **snmpd** daemon reported an error message to system log files when it could not open the following files: **/proc/net/if_inet6**, **/proc/net/snmp6**, **/proc/net/ipv6_route**, **/proc/net/tcp6**, and **/proc/net/udp6**. These files are typically missing on machines with disabled IPv6 networking, and thus reporting such error messages for them is meaningless. With this update, the error messages are suppressed, and the system log files are not filled with redundant messages.

BZ#848155

Prior to this update, the **net-snmp** utility failed to read the **diskIOLA1**, **diskIOLA5**, and **diskIOLA15** object variables of the UCD-DISKIO-MIB object, as these variables were not implemented on the Linux operating system. Consequently, the **snmptable** utility failed to return values of the three variables correctly. With this update, these objects are implemented and their values are now displayed in the **UCD-DISKIO-MIB::diskIOTable** table as expected.

BZ#825889

Previously, the **snmpd** daemon was updated to send an SNMP response to broadcast requests from the same interface, on which a SNMP response had been received. However, this update also introduced a bug which prevented **snmpd** from sending responses to unicast request on multihomed machines. This update fixes this bug, so the **snmpd** daemon is now able to both answer unicast requests on multihomed machines and send responses to broadcast requests from the same interface, on which the request has been received.

BZ#824402

Previously, the **snmptrapd** daemon terminated the embedded Perl interpreter immediately after the **TERM** signal was received, regardless of whether embedded Perl code was still being used. Consequently, **snmptrapd** could rarely terminate unexpectedly during shutdown. With this update, the embedded Perl interpreter is destroyed later during the **snmptrapd** shutdown, when all Perl processing is finished.

Users of net-snmp are advised to upgrade to these updated packages, which fix these bugs.

7.155. NETWORKMANAGER

7.155.1. RHBA-2013:0429 — NetworkManager bug fix and enhancement update

Updated NetworkManager packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

NetworkManager is a system network service that manages network devices and connections, attempting to keep active network connectivity when available. It manages Ethernet, wireless, mobile broadband (WWAN), and PPPoE (Point-to-Point Protocol over Ethernet) devices, and provides VPN integration with a variety of different VPN services.

Bug Fixes

BZ#813573

Previously, NetworkManager did not allow selecting the WPA protocol version for a connection. Certain enterprise WLAN networks using Cisco equipment do not allow roaming between WPA and WPA2 Virtual Access Points (VAP) provided by the same physical access point, requiring the use of a specific WPA protocol version to prevent disconnections. This update adds a WPA protocol combo box to the NetworkManager user interface allowing a specific WPA protocol version to be used when necessary, thus preventing this problem.

BZ#829499

Previously, NetworkManager tried to enable an interface only once. Consequently, after a network failure, if a link was restored before the connection to a DHCP server was functioning, NetworkManager sometimes timed out and failed to bring up the interface. A patch has been applied so that NetworkManager now tries three times to connect after a failure and then again in five minute intervals. As a result, NetworkManager can now more reliably restore connections after a network failure.

BZ#833199

Due to a bug in reading and writing network configuration files, network connections using the LEAP authentication method could not be made available to all users. A patch has been applied to address this issue and the network configuration files now allow LEAP as expected.

BZ#834349

When a connection was locked to a specific WPA protocol version (either v1 or v2/RSN) via either the GConf system or settings in the "/etc/sysconfig/network-scripts/" configuration files, NetworkManager overwrote that preference when the connection was edited and saved. This bug has been fixed and such WPA preferences are now preserved in the described scenario.

BZ#837056

When attempting to configure a wireless LEAP authenticated connection, the credentials were asked for twice by the authentication dialog. A patch has been applied and the problem no longer occurs.

BZ#840580

The NetworkManager service logged a warning when the Bluetooth service was not running or not installed. A patch has been applied to prevent this and the problem no longer occurs.

Enhancements

BZ#558983

This update adds bridging support for NetworkManager. Note that this is dependent on the NM_BOND_VLAN_ENABLED directive in /etc/sysconfig/network. If and only if that directive is present and is one of yes, y, or true, will NetworkManager detect and manage bridging, bonding and VLAN interfaces.

BZ#465345

The NetworkManager service now provides support for bonding network connections as well as creating VLAN and IPoIB network connections.

BZ#817660

NetworkManager now copies the DHCP lease files created by init scripts if they are newer then those NetworkManager currently has. This results in a more seamless takeover of DHCP assigned connections.

BZ#834444

This update enables Proactive Key Caching (PKC), also known as Opportunistic Key Caching (OKC), for all WPA-Enterprise configurations.

BZ#901662

A number of improvements have been made to NetworkManager to allow more bonding options and to handle incompatibilities between options. As a result, more complex bonding configurations can now be controlled by NetworkManager.

All users of NetworkManager are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.156. NFS-UTILS-LIB

7.156.1. RHBA-2013:0467 — nfs-utils-lib bug fix update

Updated nfs-utils-lib packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The nfs-utils-lib packages provide support libraries that programs in the nfs-utils package require.

Bug Fix

BZ#804812

When building the list of local realms, idmapd overwrote the string buffer, which is used to keep that list, every time a new realm was added to the list. As a consequence, the idmapd daemon logged only the last local realm added to the list. This update modifies the source code so the realms are correctly appended to the string buffer and idmapd now logs the complete list of the local realms as expected. Also, buffer size calculation has been corrected.

Users of nfs-utils-lib are advised to upgrade to these updated packages, which fix this bug.

7.157. NFS-UTILS

7.157.1. RHBA-2013:0468 — nfs-utils bug fix update

Updated nfs-utils packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The nfs-utils packages provide a daemon for the kernel Network File System (NFS) server, and related tools such as the mount.nfs, umount.nfs, and showmount.

Bug Fixes

BZ#797209

Prior to this update, the rpc.mound daemon could cause NFS clients with already mounted NFSv3 shares to become suspended. This update modifies the underlying code to parse the IP address earlier.

BZ#802469

Prior to this update, nfs-utils allowed stronger encryption types than Single DES. As a consequence, mounts to legacy servers that used the "-o sec=krb5" option failed. This update adds the -l flag to allow only Single DES. Now, secure mounts work with legacy servers as expected.

BZ#815673

Prior to this update, NFS clients could fail to mount a share with the NFSv4 server if the server had a large amount of exports to netgroups. As a consequence, NFSv4 mounts could become suspended. This update modifies the use_ipaddr case so that NFSv4 now mounts as expected.

BZ#849945

Prior to this update, the NFS idmapper failed to initialize as expected. As a consequence, file permissions were incorrect. This update modifies the underlying code so that the idmapper initializes correctly.

Users of nfs-utils are advised to upgrade to these updated packages, which fix these bugs.

7.158. NSS-PAM-LDAPD

7.158.1. RHBA-2013:0413 — nss-pam-ldapd bug fix update

Updated nss-pam-ldapd packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The nss-pam-ldapd packages provides the nss-pam-ldapd daemon (nslcd), which uses a directory server to look up name service information on behalf of a lightweight nsswitch module.

Bug Fixes

BZ#747281

Prior to this update, the disconnect logic contained a misprint and a failure return value was missing. This update corrects the misprint and adds the missing return value.

BZ#769289

Prior to this update, the nslcd daemon performed the idle time expiration check for the LDAP connection before starting an LDAP search operation. On a lossy network or if the LDAP server was under a heavy load, the connection could time out after the successful check and the search operation then failed. With this update, the idle time expiration test is now performed during the LDAP search operation so that the connection now no longer expires under these circumstances.

BZ#791042

Prior to this update, when the nslcd daemon requested access to a large group, a buffer provided by the glibc library could not contain such a group and retried again with a larger buffer to process the operation successfully. As a consequence, redundant error messages were logged in the /var/log/message file. This update makes sure that even when glibc provides a buffer that is too small on first attempt in the described scenario, no redundant error messages are returned.

All users of nss-pam-ldapd are advised to upgrade to these updated packages, which fix these bugs.

7.158.2. RHSA-2013:0590 — Important: nss-pam-ldapd security update

Updated nss-pam-ldapd packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The nss-pam-ldapd packages provide the nss-pam-ldapd daemon (nslcd), which uses a directory server to lookup name service information on behalf of a lightweight nsswitch module.

Security Fix

CVE-2013-0288

An array index error, leading to a stack-based buffer overflow flaw, was found in the way nss-pam-ldapd managed open file descriptors. An attacker able to make a process have a large number of open file descriptors and perform name lookups could use this flaw to cause the process to crash or, potentially, execute arbitrary code with the privileges of the user running the process.

Red Hat would like to thank Garth Mollett for reporting this issue.

All users of nss-pam-ldapd are advised to upgrade to these updated packages, which contain a backported patch to fix this issue.

7.159. NSS, NSS-UTIL, NSPR

7.159.1. RHBA-2013:0445 — nss, nss-util, nspr bug fix and enhancement update

Updated nss, nss-util, and nspr packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. Netscape Portable Runtime (NSPR) provides platform independence for non-GUI operating system facilities.

NOTE

The nss and nss-util packages have been upgraded to upstream version 3.14 which provides a number of bug fixes and enhancements over the previous version. In particular, support for TLS version 1.1 in NSS (RFC 4346). In addition, the nspr packages have been upgraded to upstream version 4.9.2. Note that support for certificate signatures using the MD5 hash algorithm is now disabled by default. For more information, refer to the Mozilla NSS 3.14 Release Notes. (BZ#837089, BZ#863285, BZ#863286)

Bug Fixes

BZ#555019

The Privacy Enhanced Mail (PEM) module initialization function did not return an error informing the caller that it is not thread-safe. Consequently, invalid writes were made resulting in unexpected terminations in multi-threaded libcurl-based applications. The PEM module initialization function now returns the PKCS #11 prescribed KR_CANT_LOCK constant when the type of locking requested by the caller for thread safety is not available. As a result, clients are informed of the lack of thread safety and can provide their own locking to prevent crashes.

BZ#827351

Due to a missing out-of-memory (OOM) check and improper freeing of allocated memory, the Privacy Enhanced Mail (PEM) module did not fully validate the encoding of certificates stored in a PEM-formatted file. As a consequence, error handling tests failed. With this update, the PEM module correctly validates the encoding, handles memory deallocation consistently, and error handling tests pass as expected.

Users of nss, nspr, and nss-util are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. After installing this update, applications using NSS, NSPR, or nss-util must be restarted for this update to take effect.

7.160. NTP

7.160.1. RHBA-2013:0495 — ntp bug fix update

Updated ntp packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The Network Time Protocol (NTP) is used to synchronize a computer's time with a referenced time source.

Bug Fix

BZ#875798

When at least one system network interface had an IPv6 address and the network service was stopped or started, the ntpd daemon could terminate unexpectedly. This happened if the ntpd service attempted to read the device addresses at the moment when the network service had managed to configure only the IPv6 address of the first device. With this update, the underlying library function has been fixed and the daemon no longer crashes in the scenario described.

All users of ntp are advised to upgrade to these updated packages, which fix this bug.

7.161. NUMACTL

7.161.1. RHBA-2013:0401 — numactl bug fix and enhancement update

Updated numactl packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The numactl packages provide a simple Non-Uniform Memory Access (NUMA) policy support and consist of the numactl program to run other programs with a specific NUMA policy and the libnuma library to do allocations in applications using the NUMA policy.

Bug Fixes

BZ#804480

Previously, the number of CPUs were miscalculated in the "/sys/devices/system/cpu" directory, because the "cpufreq" and "cpuidle" files were counted, so, the additional two CPUs were added erroneously. With this update, the number of CPUs is now counted correctly.

BZ#814294

The global pointer "numa_all_cpus_ptr" was supposed to be set to a bitmask allocated by the library with bits that represent all CPUs on which the calling thread can execute. Consequently, it did not function as documented when the bitmask was only set to CPU0. With this update, the underlying source code is now fixed and the "numa_all_cpus_ptr" contains only specified CPUs, when the taskset option contains CPU0.

Enhancement

BZ#829896

The existing tool numastat, which was a Perl script, was rewritten to a C program to provide much more NUMA information. The default operation of numastat will remain the same for compatibility with current users' end scripts.

Users of numactl are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.162. NUMAD

7.162.1. RHBA-2013:0358 — numad bug fix and enhancement update

Updated numad packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The numad packages provide a daemon for NUMA (Non-Uniform Memory Architecture) systems. Numad monitors NUMA characteristics and manages placement of processes and memory to minimize memory latency.

Bug Fix

BZ#825153

Prior to this update, the "-lpthread" linker flag was supplied from both the Makefile and from the spec file. As a consequence, the numad packages encountered linkage problems and failed to build when trying to rebuild these packages from the source rpm. With this update, the flag is supplied only from the specfile and rebuilding the packages no longer fails.

Enhancement

BZ#830919

This update upgrades the numad source code to version 20121015 to be fully supported by Red Hat Enterprise Linux 6.

All users of numad are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

7.163. OPENCHANGE

7.163.1. RHSA-2013:0515 — Moderate: openchange security, bug fix and enhancement update

Updated openchange packages that fix one security issue, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The openchange packages provide libraries to access Microsoft Exchange servers using native protocols. Evolution-MAPI uses these libraries to integrate the Evolution PIM application with Microsoft Exchange servers.

> **NOTE**
>
> The openchange packages have been upgraded to upstream version 1.0, which provides a number of bug fixes and enhancements over the previous version, including support for the rebased samba4 packages and several API changes. (BZ#767672, BZ#767678)

Security Fix

CVE-2012-1182

A flaw was found in the Samba suite's Perl-based DCE/RPC IDL (PIDL) compiler. As OpenChange uses code generated by PIDL, this could have resulted in buffer overflows in the way OpenChange handles RPC calls. With this update, the code has been generated with an updated version of PIDL to correct this issue.

Bug Fixes

BZ#680061

When the user tried to modify a meeting with one required attendee and himself as the organizer, a segmentation fault occurred in the memcpy() function. Consequently, the evolution-data-server application terminated unexpectedly with a segmentation fault. This bug has been fixed and evolution-data-server no longer crashes in the described scenario.

BZ#870405

Prior to this update, OpenChange 1.0 was unable to send messages with a large message body or with extensive attachment. This was caused by minor issues in OpenChange's exchange.idl definitions. This bug has been fixed and OpenChange now sends extensive messages without complications.

All users of openchange are advised to upgrade to these updated packages, which fix these issues and add these enhancements.

7.164. OPENIPMI

7.164.1. RHBA-2013:0492 — OpenIPMI bug fix update

Updated OpenIPMI packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The OpenIPMI packages provide command-line tools and utilities to access platform information using Intelligent Platform Management Interface (IPMI). System administrators can use OpenIPMI to manage systems and to perform system health monitoring.

Bug Fix

BZ#881450

The kernel ipmi_msghandler and ipmi_si modules are no longer delivered as standalone modules. As a consequence, an error occurred if these modules were used independently. With this update, the OpenIPMI init script has been modified to enable IPMI service operations on a kernel with ipmi_si and ipmi_msghandler statically compiled in the kernel. Also, the service status message now includes a new "in kernel" module state.

Users of OpenIPMI are advised to upgrade to these updated packages, which fix this bug.

7.165. OPENLDAP

7.165.1. RHBA-2013:0364 — openldap bug fix and enhancement update

Updated openldap packages that fix multiple bugs and add an enhancement are now available for Red Hat Enterprise Linux 6.

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. LDAP is a set of protocols for accessing directory services (usually phone book style information, but other information is possible) over the Internet, similar to the way DNS (Domain Name System) information is propagated over the Internet. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.

Bug Fixes

BZ#820278

When the **`smbk5pwd`** overlay was enabled in an OpenLDAP server and a user changed their password, the Microsoft NT LAN Manager (NTLM) and Microsoft LAN Manager (LM) hashes were not computed correctly. Consequently, the **`sambaLMPassword`** and **`sambaNTPassword`** attributes were updated with incorrect values, preventing the user from logging in using a Windows-based client or a Samba client. With this update, the **`smbk5pwd`** overlay is linked against OpenSSL. As such, the NTLM and LM hashes are computed correctly and password changes work as expected when using **`smbk5pwd`**.

BZ#857390

If the **TLS_CACERTDIR** configuration option used a prefix, which specified a Mozilla NSS database type, such as **sql:**, and when a TLS operation was requested, the certificate database failed to open. This update provides a patch, which removes the database type prefix when checking the existence of a directory with certificate database, and the certificate database is now successfully opened even if the database type prefix is used.

BZ#829319

When a file containing a password was provided to open a database without user interaction, a piece of unallocated memory could be read and be mistaken to contain a password, leading to the connection to become unresponsive. A patch has been applied to correctly allocate the memory for the password file and the connection no longer hangs in the described scenario.

BZ#818572

When a TLS connection to an LDAP server was established, used, and then correctly terminated, the order of the internal TLS shutdown operations was incorrect. Consequently, unexpected terminations and other issues could occur in the underlying cryptographic library (Mozilla NSS). A patch has been provided to reorder the operations performed when closing the connection. Now, the order of TLS shutdown operations matches the Mozilla NSS documentation, thus fixing this bug.

BZ#859858

When TLS was configured to use a certificate from a PEM file while **TLS_CACERTDIR** was set to use a Mozilla NSS certificate database, the PEM certificate failed to load. With this update, the certificate is first looked up in the Mozilla NSS certificate database and if not found, the PEM file is used as a fallback. As a result, PEM certificates are now properly loaded in the described scenario.

BZ#707599

The OpenLDAP server could be configured for replication with TLS enabled for both accepting connections from remote peers and for TLS client authentication to the other replicas. When different TLS configuration was used for server and for connecting to replicas, a connection to a replica could fail due to TLS certificate lookup errors or due to unknown PKCS#11 TLS errors. This update provides a set of patches, which makes multiple TLS LDAP contexts within one process possible without affecting the others. As a result, OpenLDAP replication works properly in the described scenario.

BZ#811468

When the CA (Certificate Authority) certificate directory hashed via OpenSSL was configured to be used as a source of trusted CA certificates, the **libldap** library incorrectly expected that filenames of all hashed certificates end with the **.0** suffix. Consequently, even though any numeric suffix is allowed, only certificates with **.0** suffix were loaded. This update provides a patch that properly checks filenames in OpenSSL CA certificate directory and now all certificates that are allowed to be in that directory are loaded with **libldap** as expected.

BZ#843056

When multiple LDAP servers were specified with TLS enabled and a connection to a server failed because the host name did not match the name in the certificate, fallback to another server was performed. However, the fallback connection became unresponsive during the TLS handshake. This update provides a patch that re-creates internal structures, which handle the connection state, and the fallback connection no longer hangs in the described scenario.

BZ#864913

When the OpenLDAP server was configured to use the **rwm** overlay and a client sent the **modrdn** operation, which included the **newsuperior** attribute matching the current **superior** attribute of the entry being modified, the **slapd** server terminated unexpectedly with a segmentation fault. With this update, **slapd** is prevented from accessing uninitialized memory in the described scenario, the crashes no longer occur, and the client operation now finishes successfully.

BZ#828787

When a self-signed certificate without Basic Constraint Extension (BCE) was used as a server TLS certificate and the TLS client was configured to ignore any TLS certificate validation errors, the client could not connect to the server and an incorrect message about missing BCE was returned. This update provides a patch to preserve the original TLS certificate validation error if BCE is not found in the certificate. As a result, clients can connect to the server, proper error messages about untrusted certification authority which signed the server certificate are returned, and the connection continues as expected.

BZ#821848

When the **slapd** server configuration database (**cn=config**) was configured with replication in mirror mode and the replication configuration (**olcSyncrepl**) was changed, the **cn=config** database was silently removed from mirror mode and could not be futher modified without restarting the **slapd** daemon. With this update, changes in replication configuration are properly handled so that the state of mirror mode is now properly preserved and the **cn=config** database can be modified in the described scenario.

BZ#835012

Previously, the OpenLDAP library looked up for an **AAAA** (IPv6) DNS record while resolving the server IP address even if IPv6 was disabled on the host, which could cause extra delays when connecting. With this update, the **AI_ADDRCONFIG** flag is set when resolving the remote host address. As a result, the OpenLDAP library no longer looks up for the **AAAA** DNS record when resolving the server IP address and IPv6 is disabled on the local system.

Enhancements

BZ#852339

When **libldap** was configured to use TLS, not all TLS ciphers supported by the Mozilla NSS library could be used. This update provides all missing ciphers supported by Mozilla NSS to the internal list of ciphers in **libldap**, thus improving **libldap** security capabilities.

Users of openldap are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.166. OPENSCAP

7.166.1. RHBA-2013:0362 — openscap bug fix and enhancement update

Updated openscap packages that fix various bugs and add several enhancements are now available for Red Hat Enterprise Linux 6.

The openscap packages provide OpenSCAP, which is a set of open source libraries for the integration of the Security Content Automation Protocol (SCAP). SCAP is a line of standards that provide a standard language for the expression of Computer Network Defense (CND) related information.

NOTE

The openscap packages have been upgraded to upstream version 0.9.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#829349)

All users of openscap are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.167. OPENSSH

7.167.1. RHSA-2013:0519 — Moderate: openssh security, bug fix and enhancement update

Updated openssh packages that fix one security issue, multiple bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

OpenSSH is OpenBSD's Secure Shell (SSH) protocol implementation. These packages include the core files necessary for the OpenSSH client and server.

Security Fix

CVE-2012-5536

Due to the way the pam_ssh_agent_auth PAM module was built in Red Hat Enterprise Linux 6, the glibc's error() function was called rather than the intended error() function in pam_ssh_agent_auth to report errors. As these two functions expect different arguments, it was possible for an attacker to cause an application using pam_ssh_agent_auth to crash, disclose portions of its memory or, potentially, execute arbitrary code.

NOTE

Note that the pam_ssh_agent_auth module is not used in Red Hat Enterprise Linux 6 by default.

Bug Fixes

BZ#821641

All possible options for the new RequiredAuthentications directive were not documented in the sshd_config man page. This update improves the man page to document all the possible options.

BZ#826720

When stopping one instance of the SSH daemon (sshd), the sshd init script (/etc/rc.d/init.d/sshd) stopped all sshd processes regardless of the PID of the processes. This update improves the init script so that it only kills processes with the relevant PID. As a result, the init script now works more reliably in a multi-instance environment.

BZ#836650

Due to a regression, the ssh-copy-id command returned an exit status code of zero even if there was an error in copying the key to a remote host. With this update, a patch has been applied and ssh-copy-id now returns a non-zero exit code if there is an error in copying the SSH certificate to a remote host.

BZ#836655

When SELinux was disabled on the system, no on-disk policy was installed, a user account was used for a connection, and no "~/.ssh" configuration was present in that user's home directory, the SSH client terminated unexpectedly with a segmentation fault when attempting to connect to another system. A patch has been provided to address this issue and the crashes no longer occur in the described scenario.

BZ#857760

The "HOWTO" document /usr/share/doc/openssh-ldap-5.3p1/HOWTO.ldap-keys incorrectly documented the use of the AuthorizedKeysCommand directive. This update corrects the document.

Enhancements

BZ#782912

When attempting to enable SSH for use with a Common Access Card (CAC), the ssh-agent utility read all the certificates in the card even though only the ID certificate was needed. Consequently, if a user entered their PIN incorrectly, then the CAC was locked, as a match for the PIN was attempted against all three certificates. With this update, ssh-add does not try the same PIN for every certificate if the PIN fails for the first one. As a result, the CAC will not be disabled if a user enters their PIN incorrectly.

BZ#860809

This update adds a "netcat mode" to SSH. The "ssh -W host:port ..." command connects standard input and output (stdio) on a client to a single port on a server. As a result, SSH can be used to route connections via intermediate servers.

BZ#869903

Due to a bug, arguments for the RequiredAuthentications2 directive were not stored in a Match block. Consequently, parsing of the config file was not in accordance with the man sshd_config documentation. This update fixes the bug and users can now use the required authentication feature to specify a list of authentication methods as expected according to the man page.

All users of openssh are advised to upgrade to these updated packages, which fix these issues and add these enhancements. After installing this update, the OpenSSH server daemon (sshd) will be restarted automatically.

7.168. OPENSSL

7.168.1. RHBA-2013:0443 — openssl bug fix update

Updated openssl packages that fix four bugs are now available for Red Hat Enterprise Linux 6.

The openssl packages provide a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, as well as a full-strength general-purpose cryptography library.

Bug Fixes

BZ#770872

Prior to this update, the pkgconfig configuration files of OpenSSL libraries contained an invalid libdir value. This update modifies the underlying code to use the correct libdir value.

BZ#800088

Prior to this update, the openssl function "BIO_new_accept()" failed to listen on IPv4 addresses when this function was invoked with the "*:port" parameter. As a consequence, users failed to connect via IPv4 to a server that used this function call with the "*:port" parameter. This update modifies this function to listen on IPv4 address with this parameter as expected.

BZ#841645

Prior to this update, encrypted private key files that were saved in FIPS mode were corrupted because the PEM encryption uses hash algorithms that are not available in FIPS mode. This update uses the PKCS#8 encrypted format to write private keys to files in FIPS mode. This file format uses only algorithms that are available in FIPS mode.

BZ#841645

The manual page for "rand", the pseudo-random number generator, is named "sslrand" to avoid conflict with the manual page for the C library "rand()" function. This update provides the "openssl" manual page update to reflect this.

All users of openssl are advised to upgrade to these updated packages, which fix these bugs.

7.169. PACEMAKER

7.169.1. RHBA-2013:0375 — pacemaker bug fix and enhancement update

Updated pacemaker packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Pacemaker is a high-availability cluster resource manager with a powerful policy engine.

NOTE

The pacemaker packages have been upgraded to upstream version 1.1.8, which provides a number of bug fixes and enhancements over the previous version. (BZ#768522)

To minimize the difference between the supported cluster stack, Pacemaker should be used in combination with the CMAN manager. Previous versions of Pacemaker allowed to use the Pacemaker plug-in for the Corosync engine. The plug-in is not supported in this environment and will be removed very soon. Please see http://clusterlabs.org/quickstart-redhat.html and Chapter 8 of "Clusters from Scratch" (http://clusterlabs.org/doc/en-US/Pacemaker/1.1-plugin/html/Clusters_from_Scratch) for details on using Pacemaker with CMAN.

Bug Fixes

BZ#801355

Multiple parts of the system could notice a node failure at different times. Consequently, if more than one component requested a node to be fenced, the fencing components did so multiple times. This bug has been fixed by merging identical requests from different clients if the first one is still in progress, so the node is fenced only once.

BZ#846983

Canceled operations were incorrectly stored in the cluster status. As a consequence, the cluster detected those operations and tried to clarify the status that led to additional logging and other confusing behavior. The underlying code has been modified so that the canceled operations are no longer stored in the cluster status, and Pacemaker now works as expected.

BZ#860684

An improper definition in the spec file caused unexpected implicit dependencies between Pacemaker subpackages; a certain library was in the incorrect location. The libstonithd.so.2 library has been relocated and the dependencies between Pacemaker subpackages are now defined correctly.

BZ#877364

On the systems running on AMD64 or Intel 64 architectures, the pacemaker-cts subpackage depends on some libraries from the pacemaker.libs subpackage. However, pacemaker-cts did not specify explicit package version requirement, which could cause dependency problems between new and old subpackages. The version specification of pacemaker-libs has been added to pacemaker-cts to prevent these dependency problems.

BZ#880249

Previously, deleting a master or slave resource led to one of the nodes being fenced. This update applies a patch to fix this bug and nodes are no longer fenced in such a case.

BZ#886151

Previously, the crm_report package did not install the perl-TimeData package as a dependency. Consequently, an attempt to run the crm_report utility on a system without this package failed with an error. This update adds this missing dependency and the crm_report utility can now be run as expected.

BZ#886989

Previously, it was possible to introduce non-significant whitespace characters into the Pacemaker configuration file. Consequently, Pacemaker returned confusing error messages when reading the configuration file. With this update, a patch has been applied to filter the undesired characters from the configuration file and Pacemaker no longer returns such error messages.

Enhancements

BZ#816875

With this update, Pacemaker provides a simpler XML output, which allows the users easier parsing and querying of the status of cluster resources.

BZ#816881

With this update, Pacemaker indicates when a cluster resource is reported as running based on cached information about a node that is no longer connected.

All users of Pacemaker are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.169.2. RHEA-2013:1493 — pacemaker bug fix and enhancement update

Updated pacemaker packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Pacemaker Resource Manager is a collection of technologies working together to provide data integrity and the ability to maintain application availability in the event of a failure.

NOTE

The pacemaker packages have been upgraded to upstream version 1.1.10, which provides a number of bug fixes and enhancements over the previous version. This update is required to enable Pacemaker full support exclusively in combination with Red Hat Open Stack deployments. General Pacemaker support for the Red Hat High Availability add-on will be included in future Red Hat Enterprise Linux 6 releases. (BZ#1016617)

Users of Pacemaker are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.170. PACKAGEKIT

7.170.1. RHBA-2013:0394 — PackageKit bug fix update

Updated PackageKit packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The PackageKit packages provide a D-Bus abstraction layer that allows the session user to manage packages in a secure way using a cross-distribution, cross-architecture API.

Bug Fix

BZ#735597

Prior to this update, the PackageKit daemon could abort with a segmentation fault when the user tried to authenticate with PolicyKit if the "/usr/sbin/consolekit" process failed or was manually stopped. This update modifies the underlying code so that PackageKit no longer fails when unable to access ConsoleKit. Now, a console warning message is displayed for PackageKit instead.

All users of PackageKit are advised to upgrade to these updated packages, which fix this bug.

7.171. PAM

7.171.1. RHSA-2013:0521 — Moderate: pam security, bug fix and enhancement update

Updated pam packages that fix two security issues and several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Pluggable Authentication Modules (PAM) provide a system whereby administrators can set up authentication policies without having to recompile programs to handle authentication.

Security Fixes

CVE-2011-3148

A stack-based buffer overflow flaw was found in the way the **pam_env** module parsed users' **~/.pam_environment** files. If an application's PAM configuration contained "user_readenv=1" (this is not the default), a local attacker could use this flaw to crash the application or, possibly, escalate their privileges.

CVE-2011-3149

A denial of service flaw was found in the way the **pam_env** module expanded certain environment variables. If an application's PAM configuration contained **user_readenv=1** (this is not the default), a local attacker could use this flaw to cause the application to enter an infinite loop.

Red Hat would like to thank Kees Cook of the Google ChromeOS Team for reporting the CVE-2011-3148 and CVE-2011-3149 issues.

Bug Fixes

BZ#680204

The limit on number of processes was set in the **/etc/limits.d/90-nproc.conf** file to 1024 processes even for the root account. Consequently, root processes confined with **SELinux**, such as the prelink utility started from the **crond** daemon, failed to start if there were more than 1024 processes running with UID 0 on the system. The limit for root processes has been set to unlimited and the confined processes are no longer blocked in the described scenario.

BZ#750601

The **require_selinux** option handling in the **pam_namespace** module was broken. As a consequence, when **SELinux** was disabled, it was not possible to prevent users from logging in with the **pam_namespace** module. This option has been fixed and **PAM** works as expected now.

BZ#811168

The **pam_get_authtok_verify()** function did not save the **PAM_AUTHTOK_TYPE PAM** item properly. Consequently, the authentication token type, as specified with the **authtok_type** option of the **pam_cracklib** module, was not respected in the “Retype new password” message. The **pam_get_authtok_verify()** function has been fixed to properly save the **PAM_AUTHTOK_TYPE** item and **PAM** now works correctly in this case.

BZ#815516

When the **remember** option was used, the **pam_unix** module was matching usernames incorrectly while searching for the old password entries in the **/etc/security/opasswd** file. Due to this bug, the old password entries could be mixed; the users whose usernames were a substring of another username could have the old passwords entries of another user. With this update, the algorithm that is used to match usernames has been fixed. Now only the exact same usernames are matched and the old password entries are no longer mixed in the described scenario.

BZ#825270

Prior to this update, using the **pam_pwhistory** module caused an error to occur when the root user was changing user's password. It was not possible to choose any password that was in user's password history as the new password. With this update, the root user can change the password regardless of whether it is in the user's history or not.

Enhancements

BZ#588893

Certain authentication policies require enforcement of password complexity restrictions even for root accounts. Thus, the **`pam_cracklib`** module now supports the **`enforce_for_root`** option, which enforces the complexity restrictions on new passwords even for the root account.

BZ#673398

The GECOS field is used to store additional information about the user, such as the user's full name or a phone number, which could be used by an attacker for an attempt to crack the password. The **`pam_cracklib`** module now also allows to specify the maximum allowed number of consecutive characters of the same class (lowercase, uppercase, number, and special characters) in a password.

BZ#681694

Certain authentication policies do not allow passwords which contain long continuous sequences such as “abcd” or “98765”. This update introduces the possibility to limit the maximum length of these sequences by using the new **`maxsequence`** option.

BZ#732050

Certain authentication policies require support for locking of an account that is not used for a certain period of time. This enhancement introduces an additional function to the **`pam_lastlog`** module, which allows users to lock accounts after a configurable number of days.

BZ#769694

On a system with multiple tmpfs mounts, it is necessary to limit their size to prevent them from occupying all of the system memory. This update allows to specify the maximum size and some other options of the tmpfs file system mount when using the tmpfs polyinstantiation method.

All pam users are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements.

7.172. PARTED

7.172.1. RHBA-2013:0407 — parted bug fix and enhancement update

Updated parted packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The parted packages provide a disk partitioning and partition resizing program to create, destroy, resize, move and copy ext2, linux-swap, FAT, FAT32, and reiserfs partitions.

Bug Fixes

BZ#797979

Prior to this update, the parted program did not handle unexpected values in the HFS+ filesystem correctly. As a consequence, parted aborted with a segmentation fault. This update adds additional checks for unexpected values to the HFS+ code. Now, parted no longer aborts when handling unexpected values.

BZ#803108

Prior to this update, the parted program re-synchronized only the first 16 partitions on dm devices. As a consequence, all partitions after the 16th only appeared after reboot. This update modifies the underlying code to resynchronize all of the partitions. Now, new partitions also appear without a reboot.

All parted users are advised to upgrade to these updated packages, which fix these bugs.

7.173. PCIUTILS

7.173.1. RHBA-2013:0380 — pciutils bug fix and enhancement update

Updated pciutils packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The pciutils packages provide various utilities for inspecting and manipulating devices connected to the Peripheral Component Interconnect (PCI) bus.

NOTE

The pciutils packages have been upgraded to upstream version 3.1.10, which provides several minor bug fixes and enhances support of PCI Express devices over the previous version. (BZ#826112)

Users of pciutils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.174. PCRE

7.174.1. RHBA-2012:1240 — pcre bug fix release

Updated pcre packages that fix four bugs are now available for Red Hat Enterprise Linux 6.

The pcre packages provide the Perl-compatible regular expression (PCRE) library.

Bug Fixes

BZ#756105

Prior to this update, matching patterns with repeated forward reference failed to match if the first character was not repeated at the start of the matching text. This update modifies the matching algorithm not to expect the first character again. Now, patterns with repeated forward references match as expected.

BZ#759475

Prior to this update, case-less patterns in UTF-8 mode did not match characters at the end of input text with encoding length that was shorter than the encoding length of character in the pattern, for example "/ⱥ/8i".This update modifies the pcre library to count the length of matched characters correctly. Now, case-less patterns match characters with different encoding length correctly even at the end of an input string.

BZ#799003

Prior to this update, manual pages for the pcre library contained misprints. This update modifies the manual pages.

BZ#842000

Prior to this update, applications that were compiled with the libpcrecpp library from the pcre version 6 could not been executed against libpcrecpp library from the pcre version 7 because the application binary interface (ABI) was mismatched. This update adds the compat RE::Init() function for the pcre version 6 to the pcre version 7 libpcrecpp library. Applications that were compiled on Red Hat Enterprise Linux 5 and use the RE::Init function can now be executed on Red Hat Enterprise Linux 6.

All users of pcre are advised to upgrade to these updated packages, which fix these bugs.

7.175. PCSC-LITE

7.175.1. RHSA-2013:0525 — Moderate: pcsc-lite security and bug fix update

Updated pcsc-lite packages that fix one security issue and three bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

PC/SC Lite provides a Windows SCard compatible interface for communicating with smart cards, smart card readers, and other security tokens.

Security Fix

CVE-2010-4531

A stack-based buffer overflow flaw was found in the way pcsc-lite decoded certain attribute values of Answer-to-Reset (ATR) messages. A local attacker could use this flaw to execute arbitrary code with the privileges of the user running the pcscd daemon (root, by default), by inserting a specially-crafted smart card.

Bug Fixes

BZ#788474, BZ#814549

Due to an error in the init script, the chkconfig utility did not automatically place the pcscd init script after the start of the HAL daemon. Consequently, the pcscd service did not start automatically at boot time. With this update, the pcscd init script has been changed to explicitly start only after HAL is up, thus fixing this bug.

BZ#834803

Because the chkconfig settings and the startup files in the /etc/rc.d/ directory were not changed during the update described in the RHBA-2012:0990 advisory, the user had to update the chkconfig settings manually to fix the problem. Now, the chkconfig settings and the startup files in the /etc/rc.d/ directory are automatically updated as expected.

BZ#891852

Previously, the SCardGetAttrib() function did not work properly and always returned the "SCARD_E_INSUFFICIENT_BUFFER" error regardless of the actual buffer size. This update applies a patch to fix this bug and the SCardGetAttrib() function now works as expected.

All users of pcsc-lite are advised to upgrade to these updated packages, which fix these issues. After installing this update, the pcscd daemon will be restarted automatically.

7.176. PERL-GSSAPI

7.176.1. RHBA-2012:1340 — perl-GSSAPI bug fix update

Updated perl-GSSAPI packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The perl-GSSAPI packages provide Perl extension for GSSAPIv2 access.

Bug Fix

BZ#657274

Prior to this update, the perl-GSSAPI specification file used a krb5-devel file which was removed. As a consequence, the perl-GSSAPI package could not be rebuilt. This update modifies the specification file to use the current krb5-devel files.

All users of perl-GSSAPI are advised to upgrade to these updated packages, which fix this bug.

7.177. PERL-IPC-RUN3

7.177.1. RHBA-2012:1440 — perl-IPC-Run3 bug fix update

Updated perl-IPC-Run3 packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The perl-IPC-Run3 packages provide a module to run subprocesses and redirect the stdin, stdout, and stderr functionalities to files and perl data structures. The perl-IPC-Run3 package allows to use system, qx, and open3 modules with a simple API.

Bug Fix

BZ#657487

Prior to this update, binary perl-IPC-Run3 packages failed to build if the perl-Time-HiRes module was not installed. This update adds the perl-Time-HiRes package to the build-time dependencies for perl-IPC-Run3.

BZ#870089

Prior to this update, tests that called the IP-Run3 profiler failed when the internal perl-IPC-Run3 test suite was used. This update, adds run-time dependencies on perl(Getopt::Long) and perl(Time::HiRes) to the perl-IPC-Run3 package because certain IP-Run3 functions require the perl modules. Now, the IPC-Run3 profiler runs as expected.

All users of perl-IPC-Run3 are advised to upgrade to these updated packages, which fix these bugs.

7.178. PERL-IPC-RUN

7.178.1. RHBA-2012:1336 — perl-IPC-Run bug fix update

Updated perl-IPC-Run packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The perl-IPC-Run packages provide a mechanism for Perl scripts to interact with child processes.

Bug Fix

BZ#856840

Prior to this update, the IO::Pty Perl module was not loaded when using the command "IPC::Run::harness" with the ">pty>" argument if the perl-IO-Tty package was not installed. As a consequence, the Perl code failed. This update adds a perl-IO-Tty dependency to the perl-IPC-Run packages.

All users of perl-IPC-Run are advised to upgrade to these updated packages, which fix this bug.

7.179. PERL-SOAP-LITE

7.179.1. RHBA-2012:1388 — perl-SOAP-Lite bug fix update

An updated perl-SOAP-Lite package that fixes one bug is now available for Red Hat Enterprise Linux 6.

SOAP::Lite is a collection of Perl modules, which provides a simple and lightweight interface to the Simple Object Access Protocol (SOAP) both on client and server side.

Bug Fix

BZ#748376

XMLRPC requests could fail if the MOD_PERL environment value was defined. The standard read() function is now used instead of the sysread() function when MOD_PERL is defined. As a result, XMLRPC no longer fails in this scenario.

All users of perl-SOAP-Lite are advised to upgrade to this updated package, which fixes this bug.

7.180. PERL-SYS-VIRT

7.180.1. RHBA-2013:0377 — perl-Sys-Virt bug fix and enhancement update

Updated perl-Sys-Virt packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The perl-Sys-Virt packages provide application programming interfaces (APIs) to manage virtual machines from Perl with the libvirt library.

NOTE

The perl-Sys-Virt package has been upgraded to upstream version 0.10.2, which provides a number of enhancements over the previous version. (BZ#836955)

Bug Fixes

BZ#848309

Previously, the Perl binding was setting an incompatible flag for the set_blkio_parameters() function. Consequently, it was impossible to use this function to apply block tuning. The incorrect flag has been removed and set_blkio_parameters() can now be used as expected.

BZ#861581

Prior to this update, an incorrect string length was used when setting hash keys, and thus names of certain hash keys were truncated. The correct string lengths were provided for hash keys and the hash keys for the get_node_memory_stats() function now match their documentation.

BZ#865310

When setting memory parameters, the set_node_memory_parameters() function was trying to also update some read-only values. Consequently, set_node_memory_parameters() always returned an error message. To fix this bug, the method has been changed to only set parameters, and set_node_memory_parameters() now works as expected.

BZ#869130

Previously, the API documentation contained formatting errors. This update provides correction of the API documentation, which formats the documentation correctly.

BZ#873203

Due to missing default values for parameters in the pm_suspend_for_duration() and pm_wakeup() functions, callers of the API had to supply the parameters even though they were supposed to be optional. With this update, the default values have been added to these functions, which now succeed when called.

BZ#882829

Prior to this update, mistakes were present in the Plain Old Documentation (POD) for the list_all_volumes() parameters, which could mislead users. The documentation has been updated and, for list_all_volumes() now describes the API usage correctly.

BZ#883775

Previously, an incorrect class name was used with the list_all_nwfilters() function. Consequently, the objects returned from list_all_nwfilters() could not be used. Now, the object name has been fixed and the list_all_nwfilters() function works as expected.

BZ#886028

When checking return value of the screenshot() and current_snapshot() functions, a wrong data type was assumed. Consequently, certain errors were not handled properly and applications could eventually terminate unexpectedly. With this update, API errors are correctly handled in screenshot() and current_snapshot(), and the applications no longer crash.

Users of perl-Sys-Virt are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.181. PERL

7.181.1. RHBA-2013:0444 — perl bug fix update

Updated perl packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The perl packages provide the high-level programming language Perl, which is commonly used for system administration utilities and web programming.

Bug Fix

BZ#720644

Prior to this update, computed Perl strings became corrupted or the interpreter could abort when a string with the "x" operator was repeated more than 2^31 times, for example, "my $s = "a' x (2**31+1);". This limits the right side of the "x" operator to 2^31 to prevent it from wrapping the internal representation of the count.

All users of perl are advised to upgrade to these updated packages, which fix this bug.

7.182. PHP

7.182.1. RHSA-2013:0514 — php bug fix and enhancement update

Updated php packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE link(s) associated with each description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fixes

CVE-2011-1398

It was found that PHP did not check for carriage returns in HTTP headers, allowing intended HTTP response splitting protections to be bypassed. Depending on the web browser the victim is using, a remote attacker could use this flaw to perform a HTTP response splitting attacks.

CVE-2012-2688

An integer signedness issue, leading to a heap-based buffer underflow, was found in the PHP scandir() function. If a remote attacker could upload an excessively large number of files to a directory the scandir() function runs on, it could cause the PHP interpreter to crash or, possibly, execute arbitrary code.

CVE-2012-0831

It was found that PHP did not correctly handle the magic_quotes_gpc configuration directive. A remote attacker could use this flaw to disable the option, which may make it easier to perform SQL injection attacks.

Bug Fixes

BZ#771738

Prior to this update, if a negative array index value was sent to the **`var_export()`** function, the function returned an unsigned index ID. With this update, the function has been modified to process negative array index values correctly.

BZ#812819

Previously, the **`setDate()`**, **`setISODate()`** and **`setTime()`** functions did not work correctly when the corresponding **`DateTime`** object was created from the timestamp. This bug has been fixed and the aforementioned functions now work properly.

BZ#824199

Previously, a segmentation fault occurred when PDOStatement was reused after failing due to the NOT NULL integrity constraint. This occurred when the **pdo_mysql** driver was in use. With this update, a patch has been introduced to fix this issue.

BZ#833545

Prior to this update, the dependency of the php-mbstring package on php-common packages was missing an architecture-specific requirement. Consequently, attempts to install or patch php-common failed on machines with php-mbstring installed. With this update, the architecture-specific requirement has been added and php-common can now be installed without complications.

BZ#836264

Previously, the **`strcpy()`** function, called by the **`extract_sql_error_rec()`** function in the **unixODBC** API, overwrote a guard variable in the **`pdo_odbc_error()`** function. Consequently, a buffer overflow occurred. This bug has been fixed and the buffer overflow no longer occurs.

BZ#848186, BZ#868375

Under certain circumstances, the **`$this`** object became corrupted, and behaved as a non-object. A test with the **`is_object()`** function remained positive, but any attempt to access a member variable of **`$this`** resulted in the following warning:

```
Notice: Trying to get property of non-object
```

This behavior was caused by a bug in the **Zend garbage collector**. With this update, a patch has been introduced to fix garbage collection. As a result, **`$this`** no longer becomes corrupted.

BZ#858653

Previously, the Fileinfo extension did not use the **`stat`** interface from the stream wrapper. Consequently, when used with a stream object, the Fileinfo extension failed with the following message:

```
file not found
```

With this update, the Fileinfo extension has been fixed to use the stream wrapper's stat interface. Note that only the **`file`** and **`phar`** stream wrappers support the stat interface in PHP 5.3.3.

BZ#859371

When the ***`DISABLE_AUTHENTICATOR`*** parameter of the **`imap_open()`** function was specified as an array, it ignored the array input. Consequently, a GSSAPI warning was shown. This bug has been fixed and ***`DISABLE_AUTHENTICATOR`*** now processes the array input correctly.

BZ#864951

Previously, a PHP script using the **ODBC** interfaces could enter a deadlock when the maximum execution time period expired while it was executing an SQL statement. This occurred because the execution timer used a signal and the invoked **ODBC** functions were not re-entered. With this update, the underlying code has been modified and the deadlock is now less likely to occur.

Enhancements

BZ#806132, BZ#824293

This update adds the php-fpm package, which provides the FastCGI Process Manager.

BZ#837042

With this update, a php(language) virtual provide for specifying the PHP language version has been added to the php package.

BZ#874987

Previously, the **php-xmlreader** and **php-xmlwriter** modules were missing virtual provides. With this update, these virtual provides have been added.

All users of php are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.182.2. RHSA-2013:1049 — Critical: php security update

Updated php packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fix

CVE-2013-4113

A buffer overflow flaw was found in the way PHP parsed deeply nested XML documents. If a PHP application used the xml_parse_into_struct() function to parse untrusted XML content, an attacker able to supply specially-crafted XML could use this flaw to crash the application or, possibly, execute arbitrary code with the privileges of the user running the PHP interpreter.

All php users should upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

7.183. PIRANHA

7.183.1. RHBA-2013:0351 — piranha bug fix and enhancement update

Updated piranha packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

Piranha provides high-availability and load-balancing services for Red Hat Enterprise Linux. The piranha packages contain various tools to administer and configure the Linux Virtual Server (LVS), as well as the heartbeat and failover components. LVS is a dynamically-adjusted kernel routing mechanism that provides load balancing, primarily for Web and FTP servers.

Bug Fixes

BZ#857917

The IPVS timeout values in the Piranha web interface could be reset whenever the Global Settings page was visited. As a consequence, if the Transmission Control Protocol (TCP) timeout, TCP FIN timeout, or User Datagram Protocol (UDP) timeout values had been set, these values could be erased from the configuration file. This bug has been fixed and all IPVS timeout values are preserved as expected.

BZ#860924

Previously, the Piranha web interface incorrectly displayed the value "5" for a virtual server interface. With this update, the Piranha web interface properly displays the interface associated with a virtual server.

All users of piranha are advised to upgrade to these updated packages, which fix these bugs.

7.183.2. RHBA-2013:0576 — piranha bug fix update

Updated piranha packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Piranha provides high-availability and load-balancing services for Red Hat Enterprise Linux. The piranha packages contain various tools to administer and configure the Linux Virtual Server (LVS), as well as the heartbeat and failover components. LVS is a dynamically-adjusted kernel routing mechanism that provides load balancing, primarily for Web and FTP servers.

Bug Fix

BZ#915584

Previously, the lvsd daemon did not properly activate the sorry server fallback service when all real servers were determined to be unavailable. As a result, incoming traffic for a virtual service with no available real servers were not directed to the sorry server. With this update, the lvsd daemon properly activates the sorry server when no real servers are available.

Users of piranha are advised to upgrade to these updated packages, which fix this bug.

7.184. PKI-CORE

7.184.1. RHSA-2013:0511 — Moderate: pki-core security, bug fix and enhancement update

Updated pki-core packages that fix multiple security issues, two bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Red Hat Certificate System is an enterprise software system designed to manage enterprise public key infrastructure (PKI) deployments. PKI Core contains fundamental packages required by Red Hat Certificate System, which comprise the Certificate Authority (CA) subsystem.

Security Fix

CVE-2012-4543

Note: The Certificate Authority component provided by this advisory cannot be used as a standalone server. It is installed and operates as a part of Identity Management (the IPA component) in Red Hat Enterprise Linux.

Multiple cross-site scripting flaws were discovered in Certificate System. An attacker could use these flaws to perform a cross-site scripting (XSS) attack against victims using Certificate System's web interface.

Bug Fixes

BZ#841663

Previously, due to incorrect conversion of large integers while generating a new serial number, some of the most significant bits in the serial number were truncated. Consequently, the serial number generated for certificates was sometimes smaller than expected and this incorrect conversion in turn led to a collision if a certificate with the smaller number already existed in the database. This update removes the incorrect integer conversion so that no serial numbers are truncated. As a result, the installation wizard proceeds as expected.

BZ#844459

The certificate authority used a different profile for issuing the audit certificate than it used for renewing it. The issuing profile was for two years, and the renewal was for six months. They should both be for two years. This update sets the default and constraint parameters in the caSignedLogCert.cfg audit certificate renewal profile to two years.

Enhancements

BZ#858864

IPA (Identity, Policy and Audit) now provides an improved way to determine that PKI is up and ready to service requests. Checking the service status was not sufficient. This update creates a mechanism for clients to determine that the PKI subsystem is up using the getStatus() function to query the cs.startup_state in CS.cfg.

BZ#891985

This update increases the default root CA validity period from eight years to twenty years.

All users of pki-core are advised to upgrade to these updated packages, which fix these issues and add these enhancements.

7.185. PLYMOUTH

7.185.1. RHBA-2013:0321 — plymouth bug fix and enhancement update

Updated plymouth packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The plymouth packages provide a graphical boot animation in place of the text messages that are normally displayed. Text messages are instead redirected to a log file for viewing after boot.

NOTE

The plymouth packages have been upgraded to upstream version 0.8.3, which provides a number of bug fixes and enhancements over the previous version. (BZ#853207)

All users of plymouth are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.186. PM-UTILS

7.186.1. RHBA-2012:1094 — pm-utils bug fix update

Updated pm-utils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The pm-utils packages contain a set of utilities and scripts for tasks related to power management.

Bug Fix

BZ#800630

Prior to this update, the RPM description contained wrong product names. This update removes all wrong information.

All users of pm-utils are advised to upgrade to these updated packages, which fix this bug.

7.187. POLICYCOREUTILS

7.187.1. RHBA-2013:0396 — policycoreutils bug fix and enhancement update

Updated policycoreutils packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The policycoreutils packages contain the policy core utilities that are required for basic operation of SELinux. These utilities include load_policy to load policies, setfiles to label file systems, newrole to switch roles, and run_init to run /etc/init.d scripts in the proper context.

Bug Fixes

BZ#816460, BZ#885527

Previously, when the policycoreutils-gui utility was used to add an SELinux policy for a socket file, policycoreutils-gui failed with a traceback. This bug has been fixed, policycoreutils-gui now succeeds, and the SELinux policy is now added in this scenario.

BZ#824779

Due to a bug in the code, when the restorecon utility failed, it returned the success exit code. This bug has been fixed and restorecon now returns appropriate exit codes.

BZ#843727

When multiple type accesses from the same role occurred, the audit2allow utility produced policy files that could not be parsed by the checkmodule compiler. With this update, audit2allow produces correct policy files which can be compiled by checkmodule.

BZ#876971

The restorecond init script allows to use the "reload" operation. Previously, the usage message produced by restorecond did not mention the operation. The operation has been added to the usage message, which is now complete.

BZ#882862

Prior to this update, the audit2allow utility produced a confusing output when one of the several processed AVCs could be allowed by a boolean, as it was not clear which AVC the message was related to. The layout of the output has been corrected and the audit2allow output no longer causes confusion.

BZ#893065

Due to a regression, the vdsm package failed to be installed on Red Hat Enterprise Linux 6.4 if SELinux was disabled. A patch which enables the vdsm installation has been provided.

Enhancements

BZ#834160

A new function to the semanage utility has been implemented. Now, the user is able to notice that a specified file context semanage command is wrong and an appropriate error message is returned.

BZ#851479

With this update, the restorecon utility now returns a warning message for paths for which a default SELinux security context is not defined in the policy.

Users of policycoreutils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.188. POWERPC-UTILS

7.188.1. RHBA-2013:0384 — powerpc-utils bug fix and enhancement update

Updated powerpc-utils packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The powerpc-utils packages provide various utilities for the PowerPC platform.

NOTE

The powerpc-utils packages have been upgraded to upstream version 1.2.13, which provides a number of bug fixes and enhancements over the previous version, including support for physical Ethernet devices. The snap and hvcsadmin scripts now use the "use strict" construct to prevent a Perl interpreter from allowing usage of unsafe constructs, such as symbolic references, undeclared variables and using strings without quotation marks. The snap script now also enables to add a hostname and timestamp to its output file name by specifying the "-t" option. (BZ#822656)

Bug Fixes

BZ#739699

The bootlist command is used to read and modify the bootlist in NVRAM so that a system can boot from the correct device. Previously, when using a multipath device as a boot device, the bootlist command used its Linux logical name. However, Open Firmware, which is used on IBM POWER systems, is unable to parse Linux logical names. Therefore booting from a multipath device on IBM POWER systems failed. This update modifies the bootlist script so that bootlist now supports multipath devices as a parameter. The script converts Linux logical names of multipath devices to the path names that are parsable by Open Firmware. Booting from a multipath device on IBM POWER systems now succeeds as expected.

BZ#857841

Previously, the "hvcsadmin -status" command did not provide any output if no IBM hypervisor virtual console server (hvcs) adapters were found on the system. This update corrects the hvcsadmin script so that when executing the "hvcsadmin -status" command, the user can now see a message indicating that no hvcs adapters were found.

BZ#870212

The lsdevinfo script did not previously take into consideration the "status" attribute for Ethernet devices. This attribute is essential for the End-to-End Virtual Device View feature so the feature did not work without it. This update modifies lsdevinfo so the script now also checks the status of Ethernet devices and sets the status attribute to 1. The End-to-End Virtual Device View feature now works as expected.

All users of powerpc-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.189. PPC64-DIAG

7.189.1. RHBA-2013:0382 — ppc64-diag bug fix and enhancement update

Updated ppc64-diag packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The ppc64-diag packages provide diagnostic tools for Linux on the 64-bit PowerPC platforms. The platform diagnostics write events reported by the firmware to the service log, provide automated responses to urgent events, and notify system administrators or connected service frameworks about the reported events.

NOTE

The ppc64-diag packages have been upgraded to upstream version 2.5.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#822653)

Bug Fixes

BZ#833619

Previously, the GARD functionality could fail to "gard out" a CPU that was being deconfigured on a logical partition (LPAR) if a predictive CPU failure was received. Consequently, the CPU could not be deconfigured. This was caused by incorrect behavior of the SIGCHLD signal handler, which under certain circumstances performed cleanup on a pipe child process that had already exited. This update modifies the underlying source code so that the SIGCHLD signal handler is reset to the default action before a pipe is open and set up again after the pipe is closed. The CPU is now correctly "garded out" and deconfigured as expected in this scenario. Also, vital product data (VPD) extraction from the lsvpd command did not work correctly. This has been fixed by correcting the lsvpd_init() function, and VPD is now obtained as expected.

BZ#878314

The diag_encl command was previously enhanced with a comparison feature. The feature requires the /etc/ppc64-diag/ses_pages directory to be created on ppc64-diag installation. However, the ppc64-diag spec file was not modified accordingly so that the required directory was not created when installing the ppc64-diag packages. Consequently, the comparison feature of the diag_encl command did not work. This update corrects the ppc64-diag spec file so that the /etc/ppc64-diag/ses_pages directory is now created as expected, and the comparison feature works properly.

All users of ppc64-diag are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.190. PROCPS

7.190.1. RHBA-2012:1463 — procps bug fix update

Updated procps packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The procps packages provide a set of system utilities to provide system information using the /proc file system. The procps package includes the free, pgrep, pkill, pmap, ps, pwdx, skill, slabtop, snice, sysctl, tload, top, uptime, vmstat, w, and watch utilities.

Bug Fixes

BZ#851664

Prior to this update, the 'si' and 'so' values were always zero for "m" or "M" units. This was caused by an arithmetic precision loss in the expressions used for the calculations. This update modifies the expressions to avoid precision losses.

BZ#875077

Prior to this update, the vmstat tool could be terminated unexpectedly raising the SIGFPE exception when the total sum of 'us', 'sy', 'id', 'wa' and 'st' values returned by the kernel was zero. This situation could only appear on certain specific platforms. this update modifies the internal evaluation so that the vmstat tool is more robust and does no longer terminate.

All users of procps are advised to upgrade to these updated packages, which fix these bugs.

7.191. PYKICKSTART

7.191.1. RHBA-2013:0507 — pykickstart bug fix and enhancement update

Updated pykickstart packages that fix four bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The pykickstart packages contain a python library for manipulating kickstart files.

Bug Fixes

BZ#823856, BZ#832688, BZ#837440

Previously, when using the volgroup command with the --useexisting option without specifying the physical volume (PV), the system installation failed with the following message:

volgroup must be given a list of partitions

With this update, the library scripts have been set to check if the PVs are defined prior to the installation. In case of undefined PVs, the scripts raise a warning message to notify the user.

BZ#815573

Previously, the kickstart command options marked as deprecated were not allowed to carry a value. Consequently, a kickstart file containing a deprecated command option with an assigned value, such as --videoram="value", could not be validated. The ksvalidator tool terminated with the following message:

--videoram option does not take a value

With this update, the deprecated options have been allowed to take values and the error no longer occurs in the aforementioned scenario.

Enhancement

BZ#843174

The "autopart", "logvol", "part", and "raid" commands can now take the --cipher option to specify the encryption algorithm to be used for encrypting devices. If this option is not provided, the installer will use the default algorithm.

All users of pykickstart are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.192. PYQT4

7.192.1. RHBA-2012:1241 — PyQt4 bug fix update

Updated PyQt4 packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The PyQt4 packages contain python bindings for Qt4.

Bug Fixes

BZ#757411

Prior to this update, the PyQt4 utility did not contain the deleteResource method of PyQt4.QtNetwork.QNetworkAccessManager. This update modifies the underlying code to include the missing qnetwork-deleteResource method.

BZ#821061

Prior to this update, the PyQt4 utility did not contain the QMenuBar.setCornerWidget method. This update modifies the underlying code to include the missing qmenubar-cornerWidget method.

All users of PyQt4 are advised to upgrade to these updated packages, which fix these bugs.

7.193. PYTHON-ETHTOOL

7.193.1. RHBA-2013:0454 — python-ethtool bug fix and enhancement update

Updated python-ethtool packages that fix four bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The python-ethtool package makes the ethtool kernel interface available within the Python programming environment to allow querying and changing of Ethernet card settings, such as speed, port, auto-negotiation, and PCI locations.

Bug Fixes

BZ#692028

With this update, a typographical error has been corrected in the output of the "pethtool --help" command.

BZ#698125

Prior to this update, a memory leak occurred when the get_active_devices() and get_interfaces_info() functions were called repeatedly. This bug has been fixed and the memory leak no longer occurs in the described scenario.

BZ#714753

Due to a bug in the command-line parser, the pifconfig utility did not accept an interface as an argument if specified on the command line. Consequently, the utility displayed all interfaces rather than just information about the specified interface as was expected. The bug in the parser has been fixed and pifconfig now correctly parses passed arguments.

BZ#759150

Previously, if one network interface controller (NIC) had more IP addresses, only the first address was reported multiple times. With this update, the get_ipv4_addresses() method has been implemented to report all IP addresses on the NIC.

Enhancement

BZ#698192

With this update, support for devices configured with IPv6 has been added to the pifconfig utility.

All users of python-ethtool are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.194. PYTHON-NSS

7.194.1. RHBA-2013:0405 — python-nss bug fix and enhancement update

Updated python-nss packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The python-nss packages provide bindings for Network Security Services (NSS) that allow Python programs to use the NSS cryptographic libraries for SSL/TLS and PKI certificate management.

NOTE

The python-nss packages have been upgraded to upstream version 0.13, which provides a number of bug fixes and enhancements over the previous version. (BZ#827616)

Bug Fixes

BZ#698663

On the 64-bit architecture, the setup_certs.py script contained an incorrect path to the libnssckbi.so library. As a consequence, the script attempted to run the "modutil -dbdir pki -add ca_certs -libfile /usr/lib/libnssckbi.so" command and failed with an error, because on this architecture, the libnssckbi.so library is located in the /usr/lib64/ directory. This update allows the modutil command-line utility to find the libnssckbi.so module based on its knowledge of the system.

BZ#796295

When setting Basic Constraints for a CA certificate, the python-nss package failed with the following message:

```
cannot decode Basic Constraints
```

This was because of an incorrect format specifier, which is now fixed and python-nss no longer fails in this scenario.

Enhancement

BZ#642795

The python-nss package has been updated to add support for PKCS#12 files.

Users of python-nss are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.195. PYTHON-PASTE

7.195.1. RHBA-2013:0472 — python-paste bug fix update

An updated python-paste package that fixes one bug is now available for Red Hat Enterprise Linux 6.

Python Paste provides middleware for building and running Python web applications.

Bug Fix

BZ#783158

Previously, the auth_tkt plugin used MD5 checksums, which are not FIPS (Federal Information Processing Standard) compliant. Consequently, when FIPS compliance mode was active on the system, auth_tkt failed. The auth_tkt plugin has been set to use Secure Hash Algorithm (SHA) 256, which is FIPS-compliant, instead of MD5 checksums. As a result, auth-tkt no longer fails in this situation.

All users of python-paste are advised to upgrade to this updated package, which fixes this bug.

7.196. PYTHON-PSYCOPG2

7.196.1. RHBA-2013:0327 — python-psycopg2 bug fix and enhancement update

Updated python-psycopg2 packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The python-psycopg2 packages provide a PostgreSQL database adapter for the Python programming language (like pygresql and popy). The main advantages of psycopg2 are that it supports the full Python DBAPI-2.0 and that it is thread safe at level 2.

NOTE

The python-psycopg2 packages have been upgraded to upstream version 2.0.14, which provides a number of bug fixes and enhancements over the previous version, including the fix for a memory leak in cursor handling. This update also ensures better compatibility with the PostgreSQL object-relational database management system version 8.4. (BZ#765998)

Bug Fixes

BZ#711095

Prior to this update, a copy operation terminated unexpectedly if a second thread in a single application triggered the Python garbage collection while the copy operation was in progress. This update adds the appropriate object reference count adjustments to the code.

BZ#843723

Prior to this update, object reference counting could, under certain circumstances, cause assertion failures in Python. This update modifies the underlying code to avoid these failures.

All users of psycopg2 are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.197. PYTHON-RHSM

7.197.1. RHBA-2013:0371 — python-rhsm bug fix and enhancement update

Updated python-rhsm packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The python-rhsm packages contain a library for communicating with the representational state transfer (REST) interface of Red Hat's subscription and content service. This interface is used by the Subscription Management tools for management of system entitlements, certificates, and access to content.

NOTE

The python-rhsm packages have been upgraded to upstream version 1.1.7, which provides a number of bug fixes and enhancements over the previous version. (BZ#860306)

Enhancement

BZ#790481

> This enhancement allows the opportunity to add the value of the subscription-manager version to the X-HTTP header field.

All users of python-rhsm are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.198. PYTHON-RTSLIB

7.198.1. RHBA-2013:0466 — python-rtslib bug fix update

An updated python-rtslib package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The python-rtslib package provides a Python library to configure the kernel target subsystem, using the configfs file system.

Bug Fix

BZ#838759

> Previously, it was possible to create more than one "fileio" backstore with the same backing file. This behavior could lead to data loss. This update prevents "fileio" backstores from using the same backing store.

All users of python-rtslib are advised to upgrade to this updated package, which fixes this bug.

7.199. PYTHON

7.199.1. RHBA-2013:0437 — python bug fix update

Updated python packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme, or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC).

Bug Fixes

BZ#707944

> Previously, applying the python-2.6.5-ctypes-noexecmem patch caused the ctypes.CFUNCTYPE() function to allocate memory in order to avoid running the process in a SELinux domain with the execmem permission. When this allocation process forked without using the exec() function (for example in a multi-processing module), the state of the allocator was shared between parent and child processes. This shared state caused unpredictable interactions between the processes, potentially leading to segmentation faults or lack of termination of a multiprocessing workload. With this update, python-2.6.5-ctypes-noexecmem has been reverted, and the unpredictable behavior no longer occurs. In addition, Python programs are now required to run within a SELinux domain with execmem permissions.

BZ#814391

Prior to this update, any usage of the ctypes module (such as via the "uuid" module used by the Django application framework) triggered the ctypes.CFUNCTYPE() function on module import. Consequently, if the process was missing SELinux permissions, AVC denial messages were returned. This bug has been fixed, and SELinux permissions are now required only in relevant cases of ctypes usage, such as passing a Python callable to a C callback.

BZ#810847, BZ#841748

In certain cases, enabled C-level assertions caused the python library to fail when building valid Python code. Consequently, code containing four or more nested "IF" statements within a list comprehension or generator expression failed to compile. Moreover, an error occurred when formatting certain numpy objects. With this update, the C-level assertions have been deactivated and the aforementioned problems no longer occur.

BZ#833271

As part of the fix for CVE-2012-0876, a new symbol ("XML_SetHashSalt") was added to the system libexpat library, which Python standard library uses in the pyexpat module. If an unpatched libexpat.so.1 was present in a directory listed in LD_LIBRARY_PATH, then attempts to use the pyexpat module (for example from yum) would fail with an ImportError exception. This update adds an RPATH directive to pyexpat to ensure that libexpat is used by pyexpat, regardless of whether there is an unpatched libexpat within the LD_LIBRARY_PATH, thus preventing the ImportError exception.

BZ#835460

Due to a bug in the Python logging module, the SysLogHandler class continued to send log message against a closed connection. Consequently, an infinite loop occurred when SysLogHandler was used together with the Eventlet library. The bug has been fixed, and the described issue no longer occurs.

All users of python are advised to upgrade to these updated packages, which fix these bugs.

7.200. PYTHON-VIRTINST

7.200.1. RHBA-2013:0463 — python-virtinst bug fix and enhancement update

Updated python-virtinst package that fixes one bug and adds two enhancements is now available for Red Hat Enterprise Linux 6.

The python-virtinst package contains several command-line utilities, including virt-install for building and installing new virtual machines, and virt-clone for cloning existing virtual machines.

Bug Fix

BZ#834495

Prior to this update, executing the "virt-install --cpuset=auto" command led to a backtrace, and the optimal configuration of the "cpuset" string was not formed. With this update, a patch has been backported from upstream and the described error no longer occurs.

Enhancements

BZ#803631

With this update, Red Hat Enterprise Linux 7 has been added to the list of known Linux distributions in both the virt-manager and virt-install utilities.

BZ#832339

Previously, the virt-install utility supported only the first security label listed in the libvirt capabilities. With this update, support for more labels has been added.

All users of python-virtinst are advised to upgrade to this updated package, which fixes this bug and adds these enhancements.

7.201. QEMU-KVM

7.201.1. RHBA-2013:0539 — qemu-kvm bug fix update

Updated qemu-kvm packages that fix one bug are now available for Red Hat Enterprise Linux 6.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems that is built into the standard Red Hat Enterprise Linux kernel. The qemu-kvm packages form the user-space component for running virtual machines using KVM.

Bug Fix

BZ#908396

Previously, a guest using the e1000 network adapter could do auto-negotiation during a system reset when the link_down flag was set. Consequently, after the reset, the guest network was unavailable. A patch has been provided to address this bug and the guest can now connect to the network after a system reset in the described scenario.

All users of qemu-kvm are advised to upgrade to these updated packages, which fix this bug.

7.201.2. RHBA-2013:0527 — qemu-kvm bug fix and enhancement update

Updated qemu-kvm packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems that is built into the standard Red Hat Enterprise Linux kernel. The qemu-kvm packages form the user-space component for running virtual machines using KVM.

NOTE

The QEMU guest agent (qemu-ga) provided by the qemu-guest-agent package has been updated to upstream version 1.1, which provides a number of bug fixes and enhancements over the previous version including the following notable changes:

- This update provides persist tracking of the state of the fsfreeze command using the file system so that the qemu-ga daemon is aware of the fsfreeze state even if the daemon dies or is restarted.
- The guest-fsfreeze-thaw command has been allowed to run unconditionally so that the qemu-ga daemon is still able to thaw the file system even if the daemon dies or is restarted.
- The qemu-qa daemon has been modified to read the /proc/self/mounts file instead of re-reading the /etc/mtab file when the guest-fsfreeze-thaw command is performed on the frozen file system. With this change, the daemon avoids an attempt to change the atime timestamp of the /etc/mtab file, which would be blocked.
- The guest-suspend-disk and guest-suspend-ram commands can now be used to suspend to RAM or to disk on a Windows system.
- This update fixes a memory leak in the Windows communication code.
- The guest-network-get-interfaces command can now be used to acquire network interface information in Linux.
- This update provides file system freeze support improvements and fixes.

Besides the above-mentioned important changes, this update also includes various documentation fixes and small improvements. (BZ#827612)

Bug Fixes

BZ#866736

In the SVVP (Server Virtualization Validation Program) environment, when the e1000 network driver was used, the PCI Hardware Compliance Test For Systems job failed. Consequently, the HCK (Hardware Certification Kit) SVVP certification could not be passed on the system. A patch has been provided to address this issue and the test now passes as expected in the described scenario.

BZ#887897

The dynamic hard disk uses the Virtual Hard Disk (VHD) format, and the size of the data offset in its header is 64 bits. Although Microsoft's VHD specification allows initialization of only the first 32 bits, Microsoft Windows VHD images initialize all 64 bits. QEMU previously initialized only the first 32 bits in the VPC code. Consequently, the VHD images generated by the qemu-img utility may not have been recognized in some environments (for example Microsoft Hyper-v virtualization) and by some tools (for example vhd-util). This update modifies QEMU to initialize all 64 bits of the data offset field in the header of the dynamic disks. Images in VHD format generated by qemu-img are now accepted by Microsoft Hyper-V virtualization and can be mounted successfully using the Mount-VHD command.

BZ#851143

With some initial guest OS installations using the QXL driver and VNC as the display protocol, virtual machines were terminating unexpectedly with a segmentation fault during setup and returned the "lost connection with kvm process" error message. A patch has been provided to address this issue and virtual machines now run properly in the described scenario.

BZ#821692

When migrating a guest with the HDA audio device from the host using a newer version of QEMU than the version used by the target host, the migration failed. This was caused by a recent change of the live migration format for the HDA audio device which was not recognized by the older version of QEMU. This update addresses this issue and modifies QEMU to allow sending the data in the old migration format by using the "-M $oldversion" option. The live migration now succeeds in this scenario.

BZ#733720

The initial APIC ID was not set with the correct topology bits when the number of CPU cores or threads was not a power of 2. As a consequence, CPU topology (assignment of CPU cores and threads to CPU sockets) visible to the guest was incorrect. With this update, the underlying code has been modified so that the initial APIC ID is set as expected in this scenario and the guest is now able to obtain the correct CPU topology.

BZ#689665

Previously, qemu-kvm defined an incorrect CPU level for certain CPU models, such as Intel Core 2 Duo P9xxx (Penryn Class Core 2), Intel Celeron_4x0 (Conroe/Merom Class Core 2), and Intel Core i7 9xx (Nehalem Class Core i7). Consequently, the guest system was unable to obtain any additional information about the CPU topology and was able to provide only the CPU level two topology information (package and thread information). This update corrects the underlying code to define the CPU level to be the level four for the aforementioned CPU models so that the guest now can obtain expected CPU topology information.

BZ#831708

When creating a virtual machine (VM) using the "-spice" command line option with the "streaming-video=" sub-option which was assigned an invalid value, the incorrect value was ignored and the VM was successfully created with the default value. This update corrects this behavior, and if the "streaming-video" sub-option is given an invalid value, an attempt to create a VM fails and qemu-kvm exits gracefully.

BZ#852083

Previously, virtual Performance Monitoring Unit (vPMU) pass-through mode was enabled by default on the Intel Xeon Processor E5-XXXX model in qemu-kvm. This could pose a problem when performing a live migration of virtual machines to a new host with less PMU counters than the original host had. The guest expected the same set of PMU counters and could terminate unexpectedly due to an attempt to use the non-existing PMU counters. With this update, vPMU pass-through mode has been disabled for the Intel Xeon Processor E5-XXXX model in QEMU on Red Hat Enterprise Linux 6.4 and can only be enabled when using the "-cpu host" option. The guest can no longer crash during live migration in this scenario on Red Hat Enterprise Linux 6.4, however, to keep backward compatibility of live migration, QEMU keeps the old behavior on Red Hat Enterprise Linux 6.3.

BZ#819915

When sending multi-descriptor packets, QEMU emulation of the e1000 NIC previously loaded the packet options field (POPTS) for every data descriptor. This was in conflict with the e1000 specification that requires the POPTS field to be ignored with exception of the first data descriptor of the packet. As a consequence, performance of the emulated e1000 NIC was very poor when working with multi-descriptor packets. With this update, QEMU emulation of e1000 has been corrected so it now behaves in accordance with the specification and POPTS is loaded only for the first data descriptor of the packet. Performance of the emulated e1000 NIC fulfills the user's expectations when processing multi-descriptor packets.

BZ#854528

In VGA mode, SPICE previously used dirty page tracking mechanism to determine which screen areas needed to be updated. Screen areas that had to be updated were tracked with scanline granularity so that even small updates resulted in huge loads of data to be sent. This had a significant impact on SPICE performance in VGA mode. This update modifies SPICE to keep the most recent copy of the screen content that was sent to the SPICE client. The copy is used to determine the exact areas of the screen that need to be updated, and only those pieces are now updated instead of whole scanlines. SPICE performance in VGA mode has increased as expected.

Enhancements

BZ#843084

Red Hat Enterprise Linux 6.4 adds support for Intel's next-generation Core processor to qemu-kvm so that KVM guests can utilize the new features this processor provides, the most important of which are: Advanced Vector Extensions 2 (AVX2), Bit-Manipulation Instructions 1 (BMI1), Bit-Manipulation Instructions 2 (BMI2), Hardware Lock Elision (HLE), Restricted Transactional Memory (RTM), Process-Context Identifier (PCID), Invalidate Process-Context Identifier (INVPCID), Fused Multiply-Add (FMA), Big-Endian Move instruction (MOVBE), F Segment and G Segment BASE instruction (FSGSBASE), Supervisor Mode Execution Prevention (SMEP), Enhanced REP MOVSB/STOSB (ERMS).

BZ#767233

Red Hat Enterprise Linux 6.4 supports merging of external snapshots into a backing file chain while the guest is live. Merging snapshots into the backing file chains is often faster, and fits certain workflows better than forward streaming. Snapshot data resides in the backing file specified for the merge, and merged snapshots can then be removed.

BZ#805172

KVM now supports live migration of guests with USB devices. The following devices are supported: Enhanced Host Controller Interface (EHCI) and Universal Host Controller Interface (UHCI) local passthrough and emulated devices such as storage devices, mice, keyboards, hubs, and others.

BZ#838126

The AMD Opteron 4xxx series processor is now supported by qemu-kvm. This allows the new features of this processor series to be exposed to KVM guests, such as: the F16C instruction set, Trailing Bit Manipulation, BMI1 decimate functions, and the Fused Multiply-Add (FMA) instruction set.

BZ#852665

With this update, the e1000 driver has been modified to flush the receive queue whenever it is replenished. Also, whenever the receive queue is emptied, the drivers now notify the I/O thread to repoll the file descriptor. This improvement significantly decreases the guest's latency.

BZ#861331

KVM now supports live migration of guests using USB forwarding via SPICE, while maintaining existing USB device redirection for all configured devices.

BZ#835101

When both host and guest systems are updated to Red Hat Enterprise Linux 6.4 or newer, interrupt-intensive workloads, such as incoming network traffic with a virtio network device, have the number of context switches between the VM and the hypervisor optimized. This significantly reduces CPU utilization of the host.

BZ#801063

This update allows a sound device to be detected as a microphone or a speaker in the guest system (in addition to being detected as line-in and line-out). Sound devices can now function properly in guest applications that accept only certain types of input for voice recording and audio.

BZ#854191

The QEMU user was previously unable to control the time delay before SeaBIOS rebooted a guest if no bootable device was found. This update enables the QEMU user to control the boot process of the guest by adding a new boot option, "-boot reboot-timeout=T", where T is the delay time in milliseconds. The option allows QEMU to transfer the /etc/boot-fail-wait configuration file to SeaBIOS and set the reboot timeout. The user can even prevent SeaBIOS from rebooting the guest by setting the reboot-timeout option to "-1", which is the default value.

Users of qemu-kvm are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.201.3. RHSA-2013:0609 — Important: qemu-kvm security update

Updated qemu-kvm packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. qemu-kvm is the user-space component for running virtual machines using KVM.

Security Fix

CVE-2012-6075

A flaw was found in the way QEMU-KVM emulated the e1000 network interface card when the host was configured to accept jumbo network frames, and a guest using the e1000 emulated driver was not. A remote attacker could use this flaw to crash the guest or, potentially, execute arbitrary code with root privileges in the guest.

All users of qemu-kvm should upgrade to these updated packages, which contain backported patches to correct this issue. After installing this update, shut down all running virtual machines. Once all virtual machines have shut down, start them again for this update to take effect.

7.201.4. RHSA-2013:1100 — Important: qemu-kvm security update

Updated qemu-kvm packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with each description below.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. qemu-kvm is the user-space component for running virtual machines using KVM.

Security Fix

CVE-2013-2231

> An unquoted search path flaw was found in the way the QEMU Guest Agent service installation was performed on Windows. Depending on the permissions of the directories in the unquoted search path, a local, unprivileged user could use this flaw to have a binary of their choosing executed with SYSTEM privileges.

This issue was discovered by Lev Veyde of Red Hat.

All users of qemu-kvm should upgrade to these updated packages, which contain backported patches to correct this issue. After installing this update, shut down all running virtual machines. Once all virtual machines have shut down, start them again for this update to take effect.

7.202. QL2400-FIRMWARE

7.202.1. RHBA-2013:0402 — ql2400-firmware bug fix and enhancement update

An updated ql2400-firmware package that fixes multiple bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The ql2400-firmware package provides the firmware required to run the QLogic 2400 Series of mass storage adapters.

> **NOTE**
>
> This update upgrades the ql2400 firmware to upstream version 5.08.00, which provides a number of bug fixes and enhancements over the previous version. (BZ#826665)

All users of QLogic 2400 Series Fibre Channel adapters are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

7.203. QL2500-FIRMWARE

7.203.1. RHBA-2013:0403 — ql2500-firmware bug fix and enhancement update

An updated ql2500-firmware package that fixes multiple bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The ql2500-firmware package provides the firmware required to run the QLogic 2500 Series of mass storage adapters.

NOTE

This update upgrades the ql2500 firmware to upstream version 5.08.00., which provides a number of bug fixes and enhancements over the previous version. (BZ#826667)

All users of QLogic 2500 Series Fibre Channel adapters are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

7.204. QT

7.204.1. RHBA-2012:1246 — qt bug fix update

Updated qt packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The qt packages contain a software toolkit that simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System.

Bug Fixes

BZ#678604

Prior to this update, the mouse pointer could, under certain circumstances, disappear when using the IRC client Konversation. This update modifies the underlying codes to reset the cursor on the parent and set the cursor on the new window handle. Now, the mouse pointer no longer disappears.

BZ#847866

Prior to this update, the high precision coordinates of the QTabletEvent class failed to handle multiple Wacom devices. As a consequence, only the device that was loaded first worked correctly. This update modifies the underlying code so that multiple Wacom devices are handled as expected.

All users of qt are advised to upgrade to these updated packages, which fix this bugs.

7.205. QUOTA

7.205.1. RHBA-2012:1472 — quota bug fix update

Updated quota packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

The quota packages contain a suite of system administration tools for monitoring and limiting user and group disk usage on file systems.

Bug Fixes

BZ#680919

Prior to this update, warnquota sent emails from <root@myhost.com> if the quota limit was exceeded and the warnquota tool was enabled to send warning emails and the default warnquota configuration was not changed. As a consequence, users could wrongly reply to this address and email bounces were delivered to the mailbox of <root@myhost.com>. This update modifies the default warnquota configuration to use the reserved domain "example.com".

BZ#683554

Prior to this update, the option "-r" for setquota and edquota failed to set the grace times for NFS-mounted file systems without reporting errors because the underlying remote procedure call protocol does not support this option. This update disables the option "-r". With this update, the option to set grace times over the network is disabled and error messages are sent when using the "-r" option.

BZ#692390

Prior to this update, the quotacheck tool could mishandle UIDs in processed fsv1 quota files if a user's block limit was reached. This update zeroes uninitialized padding in the "v2r1 ddquot" structure before running subsequent checks.

BZ#704216

Prior to this update, the edquota tool could abort with a segmentation fault if the name server switch was configured to use the libdb back end. This update modifies the underlying code to make the "dirname" symbol in edquota sources static to avoid pollution of the symbol name space confusing the dynamic linker. Now, edquota runs on systems which use the Berkeley DB (BDB) database for storing user names, group names, or passwords.

BZ#730057

Prior to this update, the quota_nld service logged the error message "Failed to find tty of [UID] to report warning to" when users without an interactive session exceeded the disk quota limit while running quota_nld service. This update applies these warnings to non-daemon debugging mode of quota_nld only.

BZ#770307

Prior to this update, the warnquota tool sent a badly worded email message. This update changes the wording and the text is now worded more representative.(

All users of quota are advised to upgrade to these updated packages, which fix these bugs.

7.206. RDESKTOP

7.206.1. RHBA-2012:1276 — rdesktop bug fix update

Updated rdesktop packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

The rdesktop packages provide a client for the Remote Desktop Server in Microsoft Windows. The rdesktop client uses the Remote Desktop Protocol (RDP) to remotely present a user's desktop.

Bug Fixes

BZ#680917, BZ#772020

Prior to this update, redundant conversions functions did not handle the PC/SC (Personal Computer/Smart Card) integration correctly. As a consequence, the rdesktop on AMD64 and Intel 64 platforms failed to connect and incorrectly. This update removes these redundant functions. This update also adds smart card reader support for AMD64 and Intel 64 platforms. Now, the rdesktop connects as expected.

BZ#680926

Prior to this update, the rdesktop code for smart card integration with PC/SC caused a buffer overflow on AMD64 and Intel 64 platforms. As a consequence, the glibc function "free()" was aborted with a segmentation fault. This update uses the correct structure and the glibc function "free()" works now as expected.

BZ#782494

Prior to this update, the server generated a cursor-related command that the rdesktop client did not support when using rdesktop to connect to Windows Server 2008 R2 platforms. As a consequence, the mouse pointer was all black. With this update, the mouse pointer is drawn correctly when connecting to Windows Server 2008 R2.

BZ#820008

Prior to this update, the specification file incorrectly listed the libao-devel package as an install dependency for rdesktop. This update removes the libao-devel dependency from the specification file.

BZ#831095

Prior to this update, the rdesktop client did not handle the licenses correctly, As a consequence, certain Terminal Services failed to connect after the first connection with the error message "disconnect: Internal licensing error". This update modifies the underlying code to handle licenses as expected. Now, Terminal Services connect as expected.

All users of rdesktop are advised to upgrade to these updated packages, which fix these bugs.

7.207. RDMA

7.207.1. RHSA-2013:0509 — Low: rdma security, bug fix and enhancement update

Updated RDMA packages that fix multiple security issues, various bugs, and add an enhancement are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Red Hat Enterprise Linux includes a collection of InfiniBand and iWARP utilities, libraries and development packages for writing applications that use Remote Direct Memory Access (RDMA) technology.

Security Fixes

CVE-2012-4517

A denial of service flaw was found in the way ibacm managed reference counts for multicast connections. An attacker could send specially-crafted multicast packets that would cause the ibacm daemon to crash.

CVE-2012-4518

It was found that the ibacm daemon created some files with world-writable permissions. A local attacker could use this flaw to overwrite the contents of the ibacm.log or ibacm.port file, allowing them to mask certain actions from the log or cause ibacm to run on a non-default port.

CVE-2012-4518 was discovered by Florian Weimer of the Red Hat Product Security Team and Kurt Seifried of the Red Hat Security Response Team.

The InfiniBand/iWARP/RDMA stack components have been upgraded to more recent upstream versions.

Bug Fixes

BZ#818606

Previously, the "ibnodes -h" command did not show a proper usage message. With this update the problem is fixed and "ibnodes -h" now shows the correct usage message.

BZ#822781

Previously, the ibv_devinfo utility erroneously showed iWARP cxgb3 hardware's physical state as invalid even when the device was working. For iWARP hardware, the phys_state field has no meaning. This update patches the utility to not print out anything for this field when the hardware is iWARP hardware.

BZ#834428

Prior to the release of Red Hat Enterprise Linux 6.3, the kernel created the InfiniBand device files in the wrong place and a udev rules file was used to force the devices to be created in the proper place. With the update to 6.3, the kernel was fixed to create the InfiniBand device files in the proper place, and so the udev rules file was removed as no longer being necessary. However, a bug in the kernel device creation meant that, although the devices were now being created in the right place, they had incorrect permissions. Consequently, when users attempted to run an RDMA application as a non-root user, the application failed to get the necessary permissions to use the RDMA device and the application terminated. This update puts a new udev rules file in place. It no longer attempts to create the InfiniBand devices since they already exist, but it does correct the device permissions on the files.

BZ#847129

Previously, using the "perfquery -C" command with a host name caused the perfquery utility to become unresponsive. The list of controllers to process was never cleared and the process looped infinitely on a single controller. A patch has been applied to make sure that in the case where the user passes in the -C option, the controller list is cleared out once that controller has been processed. As a result, perfquery now works as expected in the scenario described.

BZ#862857

The OpenSM init script did not handle the case where there were no configuration files under "/etc/rdma/opensm.conf.*". With this update, the script as been patched and the InfiniBand Subnet Manager, OpenSM, now starts as expected in the scenario described.

Enhancement

BZ#869737

This update provides an updated mlx4_ib Mellanox driver which includes Single Root I/O Virtualization (SR-IOV) support.

All users of RDMA are advised to upgrade to these updated packages, which fix these issues and add this enhancement.

7.208. REDHAT-LSB

7.208.1. RHBA-2013:0448 — redhat-lsb bug fix and enhancement update

Updated redhat-lsb packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 6.

Linux Standards Base (LSB) provides a set of standards that increases compatibility among Linux distributions. The redhat-lsb packages provide utilities needed for LSB compliant applications. It also contains requirements that ensure that all components required by LSB are installed on the system.

Bug Fixes

BZ#709016

Previously, the redhat-lsb-core subpackage was missing from the redhat-lsb packages. Consequently, a large number of unnecessary dependencies was pulled in when redhat-lsb was required. This update provides redhat-lsb-core, which has minimal requirements, thus preventing this bug.

BZ#844602

An inaccurate brand name was used in the redhat-lsb package description. This update fixes the description.

BZ#833058

Previously, the /etc/lsb-release file specified in the lsb_release man page was missing from the redhat-lsb packages. This update adds this file, which provides information about LSB modules installed on the system.

Enhancement

BZ#801158

It is now possible to install LBS subpackages, such as redhat-lsb-core, redhat-lsb-c++, redhat-lsb-graphics, or redhat-lsb-printing, separately without having to install the redhat-lsb package with all dependencies that might be unnecessary on a system.

Users of redhat-lsb are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.209. REDHAT-RELEASE

7.209.1. RHEA-2013:0379 — redhat-release enhancement update for Red Hat Enterprise Linux 6.4

Enhanced redhat-release packages are now available for Red Hat Enterprise Linux 6.4.

The redhat-release package contains licensing information regarding, and identifies the installed version of, Red Hat Enterprise Linux.

These updated redhat-release packages reflect changes made for the release of Red Hat Enterprise Linux 6.4.

Users of Red Hat Enterprise Linux 6 are advised to upgrade to these updated redhat-release packages, which add this enhancement.

7.210. REDHAT-RPM-CONFIG

7.210.1. RHBA-2013:0460 — redhat-rpm-config bug fix and enhancement update

Updated redhat-rpm-config packages that fix two bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The redhat-rpm-config packages are used during the build of RPM packages to apply various default distribution options determined by Red Hat. It also provides a few Red Hat RPM macro customizations, such as those used during the building of Driver Update packages.

Bug Fixes

BZ#795577

The kmodtool script is a helper script for building kernel module RPMs. Previously, the "verrel" parameter in the kmodtool script returned the kernel version and variant string with a dangling sign ("."). With this update, the dangling sign has been removed from the "verrel" output.

BZ#822073

The "brp-java-repack-jars" script was unable to correctly handle certain Java Archive (JAR) files. Those files set permissions on "exploded" directory hierarchies to non-standard permissions modes, such as "0000". With this update, standard user permissions are set correctly on the "exploded" directory hierarchy, which prevents certain errors from occurring, such as being unable to remove the directory tree when it is necessary to do so.

Enhancements

BZ#669638

Previously, the number of parallel compilation jobs suggested by the %_smp_mflags macro was limited to maximum of 16 CPUs. This update introduces the %_smp_ncpus_max macro, which makes the CPU limit adjustable.

BZ#869062

Previously, the /usr/lib/rpm/redhat/rpmrc file contained a leftover "macrofiles" line, which is ignored by later versions of RPM. With this update, the aforementioned line has been removed from rprmc to avoid confusion.

All users of redhat-rpm-config are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.211. RED HAT ENTERPRISE LINUX RELEASE NOTES

7.211.1. RHEA-2013:0439 — Red Hat Enterprise Linux 6.4 Release Notes

Updated packages containing the Release Notes for Red Hat Enterprise Linux 6.4 are now available.

Red Hat Enterprise Linux minor releases are an aggregation of individual enhancement, security and bug fix errata. The Red Hat Enterprise Linux 6.4 Release Notes documents the major changes made to the Red Hat Enterprise Linux 6 operating system and its accompanying applications for this minor release. Detailed notes on all changes in this minor release are available in the Technical Notes.

Refer to the Online Release Notes for the most up-to-date version of the Red Hat Enterprise Linux 6.4 Release Notes:

https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html-single/6.4_Release_Notes/index.html

NOTE

Starting with the 6.4 release of the online Release Notes, the "Device Drivers" chapter has been moved to the online Technical Notes:

https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/6.4_Technical_Notes/ch-device_drivers.html

7.212. RESOURCE-AGENTS

7.212.1. RHBA-2013:0288 — resource-agents bug fix and enhancement update

Updated resource-agents packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The resource-agents packages contain a set of scripts to interface with several services to operate in a High Availability (HA) environment for both the **Pacemaker** and **rgmanager** service managers.

Bug Fixes

BZ#714156

Previously, the `status` action in the **netfs** interface failed to write any output to the `/var/log/cluster/rgmanager.log` file. Consequently, it was not possible to verify if the status check of an NFS mount was successful. The bug has been fixed, and results of the status check are now properly stored in the log file.

BZ#728365

For **HA-LVM** to work properly, the `/boot/initrd.img` file, which is used during the boot process, must be synchronized with the `/etc/lvm/lvm.conf` file. Previously, the **HA-LVM** startup failed when `lvm.conf` was changed without updating `initrd.img`. With this update, this behavior has been modified. A warning message is now displayed, but the startup is no longer terminated in the described case.

BZ#729812

Prior to this update, occasional service failures occurred when starting the `clvmd` variant of the **HA-LVM** service on multiple nodes in a cluster at the same time. The start of an **HA-LVM** resource coincided with another node initializing that same **HA-LVM** resource. With this update, a patch has been introduced to synchronize the initialization of both resources. As a result, services no longer fail due to the simultaneous initialization.

BZ#817550

When the **oracledb.sh** script was called with the `status` argument, it restarted the database after checking its status without any notification to the **rgmanager** application. This bug has been fixed, and the unwanted restart no longer occurs.

BZ#822244

Previously, the /**usr**/**sbin**/**tomcat-6.sh** script parsed configuration files and set shell variables before starting the Apache Tomcat 6 servlet container. Consequently, the default configuration was ignored. This bug has been fixed and the aforementioned problem no longer occurs.

BZ#839181

Previously, an output of HA-LVM commands that contained more than one word, was not correctly parsed. Consequently, starting an HA-LVM service with the **`rg_test`** command occasionally failed with the following message:

```
too many arguments
```

With this update, the underlying source code has been modified to add quotation marks around variables that expand to more than one word. As a result, the aforementioned startup errors no longer occur.

BZ#847335

If the contents of the **`/proc/mounts`** file changed during a status check operation of the file system resource agent, the status check could incorrectly detect a missing mount and mark the service as failed. This bug has been fixed and **rgmanager**'s file system resource agent no longer reports false failures in the described scenario.

BZ#848642

Previously, **rgmanager** did not recognize CIFS (Common Internet File System) mounts in case their corresponding entries in the device field of the **`/proc/mounts`** file contained trailing slashes. With this update, a patch has been introduced to remove trailing slashes from device names when reading the contents of **`/proc/mounts`**. As a result, CIFS mounts are now recognized properly.

BZ#853249

Prior to this update, when running a file system depending on an LVM resource in a service, and that LVM resource failed to start, the subsequent attempt to unregister the file system resource failed. This bug has been fixed, and a file system resource can now be successfully unregistered after a failed mount operation.

BZ#860328

Previously, when using the **HA-LVM** resource agent in the **Pacemaker** cluster environment, several errors and failed actions occurred. With this update, several scripts have been added to prevent these errors. These scripts repair the treatment of whitespace within **HA-LVM** and the processing of non-zero codes in **rgmanager**. In addition, the **member_util** utility has been updated to use **Corosync** and **Pacemaker** when **rgmanager** is not present on the system.

BZ#860981

Previously, when a node lost access to the storage device, **HA-LVM** was unable to deactivate the volume group for the services running in that node. The underlying source code has been modified to allow services to migrate to other machines that still have access to storage devices, thus preventing this bug.

BZ#869695

Previously, SAP instances started by the **SAPInstance** cluster resource agent inherited limits on system resources for the root user. Higher limits were needed on the maximum number of open files (**`ulimit -n`**), the maximum stack size (**`ulimit -s`**), and the maximum size of data segments (**ulimit -d**). With this update, the **SAPInstance** agent has been modified to accept limits specified in the **/usr/sap/services** file. As a result, system resources limits can now be specified manually.

Enhancements

BZ#773478

With this update, the **/usr/share/cluster/script.sh** resource, used mainly by the **rgmanager** application, has been enhanced to provide more informative reports on causes of internal errors.

BZ#822053

With this update, the **nfsrestart** option has been added to both the **fs** and **clusterfs** resource agents. This option provides a way to forcefully restart NFS servers and allow a clean unmount of an exported file system.

BZ#834293

The pacemaker **SAPInstance** and **SAPDatabase** resource agents have been updated with the latest upstream patches.

BZ#843049

A new ***prefer_interface*** parameter has been added to the **rgmanager ip.sh** resource agent. This parameter is used for adding an IP address to a particular network interface when a cluster node has multiple active interfaces with IP addresses on the same subnetwork.

All users of resource-agents are advised to upgrade to these updated packages, which fix these bugs and add these enhancements

7.212.2. RHEA-2013:1494 — resource-agents enhancement update

Updated resource-agents packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The resource-agents packages contain a set of scripts to interface with several services to operate in a High Availability (HA) environment for both the Pacemaker and rgmanager service managers.

Enhancement

BZ#1001519

This update adds support for the Pacemaker resource agents under the Heartbeat OCF provider.

Users of resource-agents are advised to upgrade to these updated packages, which add this enhancement.

7.212.3. RHBA-2013:1007 — resource-agents bug fix and enhancement update

Updated resource-agents packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The resource-agents packages contain a set of scripts to interface with several services to operate in a High Availability (HA) environment for both the Pacemaker and rgmanager service managers.

Bug Fix

BZ#978775

Usage of lvm.sh with tags resulted in the stripping of cluster tags when the node rejoined the cluster. This was because the lvm.sh agent was unable to accurately detect the tag represented by a cluster node. Thus, the active logical volume on a cluster node failed when another node re-joined the cluster. This update properly detects whether tags represent a cluster node, the node-name, or, if fqdn is returned by the corosync-quorumtool -l output. When nodes re-join the cluster, tags are not stripped of LVM volume groups, and the volume group no longer fails on other nodes.

Enhancement

BZ#972931

Previous versions of the Oracle Resource Agent were only tested against Oracle 10. With this update, support for the Oracle Database 11g has been added to the oracledb, orainstance, and oralistener resource agents.

Users of resource-agents are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

7.213. RGMANAGER

7.213.1. RHBA-2013:0409 — rgmanager bug fix update

Updated rgmanager packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The rgmanager packages contain the Red Hat Resource Group Manager, which allows to create and manage high-availability server applications in the event of system downtime.

Bug Fixes

BZ#825375

Due to an unlocked access to internal DBus data structures from different rgmanager threads, rgmanager could terminate unexpectedly inside dbus library functions when running rgmanager without the "-q" flag (set as default). The underlying source code has been modified and rgmanager no longer fails in this situation.

BZ#831658

Previously, rgmanager preferred two nodes in a three-nodes cluster, which caused the third node being unused. The configuration has been changed and rgmanager now uses all nodes in the cluster as expected.

BZ#833347

Previously, the cpglockd init script was not included in the chkconfig configuration file. This updated adds cpglockd in this file.

BZ#853251

Resource Group Manager fails to stop a resource if it is located on an unmounted file system. As a result of this failure, rgmanager treated the resource as missing and marked the appropriate service as failed, which prevented the cluster from recovering the service. This update allows rgmanager to ignore this error if a resource has not been previously started with a service. The service can now be properly started on a different host.

BZ#861157

When rgmanager received a remote start message for a particular service while already in the process of starting that service locally, a deadlock could occur. This sometimes happened during the recovery of a service that had failed its start operation. This bug has been fixed and rgmanager works as expected.

BZ#879031

When a service is configured with a recoverable resource, such as nfsclient, a failure of that client correctly triggers the recovery function. However, even if recovery operation was successful, rgmanager still stopped and recovered the service. The underlying source code has been modified and rgmanager no longer stops successfully recovered clients.

All users of rgmanager are advised to upgrade to these updated packages, which fix these bugs.

7.214. RHN-CLIENT-TOOLS

7.214.1. RHBA-2013:0388 — rhn-client-tools bug fix and enhancement update

Updated rhn-client-tools packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

Red Hat Network Client Tools provide utilities for connecting to and receiving content from Red Hat Network.

Bug Fixes

BZ#784964

If a system used multiple network interfaces, the Satellite server might have discovered a different IP address from the one the user used to connect to Red Hat Network. This caused Red Hat Network to display incorrect information in the web UI. The underlying source code has been modified, so that the correct IP is now discovered and also the correct information displayed in the web UI.

BZ#842834

Multiple-server failover did not work properly; a socket error could occur when multiple servers were configured. This update ensures that the user can configure additional servers to try if the first option fails.

BZ#815695

Previously, the rhn-channel utility could ignore configured proxy servers when used with certain options, for example, "--available channels". This problem has been fixed and the specified proxy servers are used as expected in this scenario.

BZ#811641

Due to a bug in the source code, the rhn_register utility could throw a traceback during registration if a USB device was connected in the system. The bug has been fixed, and Red Hat Network registrations work correctly in this scenario.

BZ#839791

Previously, the rhn-profile-sync utility exited with an incorrect exit code if an error occurred. This update ensures that rhn-profile-sync exits with the correct exit code.

BZ#823551

Previously, the firstboot and rhn_register GUIs displayed confusing or conflicting information that did not reflect changes to Subscription Manager. The text has been updated to be clearer and specific.

BZ#830776

The rhn_check utility failed with a traceback if another instance of rhn_check was running. With this update, if the user attempts to run rhn_check while another instance is running, an appropriate error message will be displayed.

BZ#810315

An outdated example icon was displayed on the Set Up Software Update screen in firstboot. The icon has been replaced to provide an example that matches what users see on their system.

BZ#839935

Previously, attempting to subscribe to a non-existent channel using the rhn-channel utility failed with a traceback. With this update, an informative error message appears in this scenario.

BZ#786422

This update fixes a typo that previously existed in the text of the rhn_register user interface.

BZ#846359

The rhn-channel utility did not properly parse certain methods used for specifying command-line options. As a consequence, rhn-channel could fail with a traceback. This update ensures that rhn-channel can properly parse various ways that options are commonly specified in bash.

BZ#851657

Titles for some windows in the rhn_register GUI did not follow standard title capitalization; some titles were lowercase. This update ensures that the titles are uppercase where appropriate.

BZ#878758

When running the rhn_register utility, the "Enter your account information" page contained a link pointing to a non-existing web page. The link has been fixed and now points to the correct page.

Enhancement

BZ#859281

The "-b" option can now be specified for the rhn-channel utility to display the current base channel of the system.

All users of rhn-client-tools are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.215. RICCI

7.215.1. RHBA-2013:0453 — ricci bug fix and enhancement update

Updated ricci packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The ricci packages contain a daemon and a client for remote configuring and managing of clusters.

Bug Fixes

BZ#811702

Prior to this update, if the ricci daemon was not running on all nodes, executing the "ccs --stopall" command caused an attribute error to occur. With this update, the code has been fixed and the error no longer occurs in the aforementioned scenario.

BZ#815752

Previously, a segmentation fault occurred in both the ricci daemon and ccs_sync utility when processing a larger cluster.conf file. This was caused by an insufficient thread stack size in ricci. The ccs_sync utility terminated unexpectedly due to incorrect behavior of the PR_Write function. With this update, a patch has been introduced to fix both causes. As a result, the segmentation fault no longer occurs.

BZ#877381

Previously, a segmentation fault occurred in the ricci daemon when processing cluster.conf files with very large values. This was caused by allocating large amounts of memory not available on the stack. With this update, a patch has been introduced to allocate memory on the heap and provide an error if not enough memory is available. As a result, the segmentation fault no longer occurs.

BZ#818335

Previously, the "ccs_sync" command did not return a non-zero exit code if an error occurred or the ricci daemon was not running, even when running the command with the "-w" option to exit with a failure status if any warnings were issued. The underlying source code has been modified so that "ccs_sync" with the "-w" option now returns "1" on failure.

BZ#839039

With this update, a minor typographical error has been fixed in the ccs error message related to being unable to start a node, possibly due to lack of quorum.

BZ#841288

Previously, the "ccs --lsmisc" command did not properly display the alternate multicast address. The bug has been fixed, and the alternate multicast address is now reported correctly when --lsmisc is used.

BZ#867019

Previously, the ccs program failed to generate certificates when running on a read-only NFS. This bug has been fixed and ccs now generates certificates regardless of the type of the current working directory.

BZ#866894

Previously, the ccs program incorrectly handled the cluster.conf file when adding a resource into the file. Consequently, resulting cluster.conf was invalid. This bug has been fixed and ccs now works correctly in the described case.

BZ#842939

Previously, the ricci daemon would not properly handle yum output when it was split over multiple lines. Consequently, in certain circumstances the conga management system was unable to list or install packages. This bug has been fixed and ricci now works correctly in the described case.

Enhancement

BZ#878108

The cluster schema has been updated to match the current Red Hat Enterprise Linux 6.4 cluster packages.

All users of ricci are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.216. RPCBIND

7.216.1. RHBA-2013:0291 — rpcbind bug fix and enhancement update

Updated rpcbind packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The rpcbind utility maps RPC (Remote Procedure Call) services to the ports on which the services listen and allows the host to make RPC calls to the RPC server.

Bug Fixes

BZ#813898

Previously, the rpcbind(8) man page referred to rpcbind(3) for which no entry existed. This update adds the missing rpcbind(3) man page.

BZ#864056

Using Reverse Address Resolution Protocol (RARP) and the bootparams file for booting Solaris or SPARC machines did not work properly. The SPARC systems sent broadcast bootparams WHOAMI requests, but the answer was never sent back by rpcbind. This bug has been fixed and rpcbind no longer discards the bootparams WHOAMI requests in the described scenario.

Enhancement

BZ#731542

When using the rpcbind's insecure mode via the "-i" option, non-root local users are now allowed to set and unset calls from remote hosts.

All users of rpcbind are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.217. RPMDEVTOOLS

7.217.1. RHBA-2012:1313 — rpmdevtools bug fix update

Updated rpmdevtools packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The rpmdevtools packages contain scripts and (X)Emacs support files to aid in development of RPM packages.

Bug Fix

BZ#730770

Prior to this update, the sample spec files referred to a deprecated BuildRoot tag. The tag was ignored if it was defined. This update removes the BuildRoot tags from all sample spec files.

All users of rpmdevtools are advised to upgrade to these updated packages, which fix this bug.

7.218. RPM

7.218.1. RHBA-2013:0461 — rpm bug fix and enhancement update

Updated rpm packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The RPM Package Manager (RPM) is a powerful command-line driven package management system that can install, uninstall, verify, query and update software packages.

Bug Fixes

BZ#664696

Previously, PGP keys were loaded even if they were not needed. Consequently, under certain conditions, RPM could not be opened. With this update, the PGP keys are loaded only when needed and RPM no longer fails to start.

BZ#727872

The debuginfo packages contained only one symbolic link per build ID. When multiple identical binaries existed on the system, only one of them was linked. With this update, numbered symbolic links are created instead.

BZ#730473

Setting the %defattr macro in a package's spec file overrode the directory permissions given by the %attr macro so that directories were created with incorrect permissions during installation of the package. This update modifies the underlying RPM code to prevent the %defattr macro from overriding the %attr macro. The directories are now created with the correct permissions by RPM.

BZ#743229

The value of the %_host macro was set to "x86_64-unknown-linux-gnu" by default. With this update, the word "unknown" is replaced by "redhat" as is expected by several parts of the build chain.

BZ#773503

Previously, using the "rpmbuild" command caused the [patched].orig file to be created without any indication, which could confuse the user. This update modifies the underlying source code so that rpmbuild no longer runs the patch utility with the "-s" command line option.

BZ#802839

When a large package was sent to the standard input (stdin), the rpm2cpio utility terminated. With this update, the underlying source code has been modified and rpm2cpio works as expected in this situation.

BZ#825147

Previously, using the RPM API for parsing spec files caused macros defined in a spec file to remain in the RPM macro "environment" after the parsing routine exited. This behavior affected the parsing results if more than one spec file was parsed per process lifetime. To resolve the problem, this update backports the reloadConfig() method from RPM 4.10's Python API. Multiple spec files can now be safely processed within a single process.

BZ#829621

An attempt to import multi-key PGP armors caused the rpm utility to fail, which could lead to memory corruption or RPM database corruption. With this update, rpm has been modified to reject multi-key PGP armors. As a result, when importing multi-key PGP armors, the "unsupported=multikey packets/armors" error message is returned.

BZ#858731

Due to the lack of DWARF 3 and 4 format support, the rpmbuild utility was not able to produce usable debug packages with newer compilers. This update adds the required support for the debugedit utility to RPM, and DWARF 3 and 4 formats are now supported as expected.

BZ#869667

Previously, RPM returned the 0 exit code even if the import of a PGP key failed. The underlying source code has been modified to fix this bug and RPM no longer returns 0 if key import fails.

BZ#804049, BZ#845065

This update contains several minor fixes and corrections in the rpm(8) manual page.

Enhancements

BZ#825087

This enhancement improves RPM to support the dpkg-style tilde character ("~") in the package's version and the release string to signify lower priority in version comparison. Note that this enhancement could affect packages that already have the tilde character in their version or release and the updated version of RPM do not work with packages that were built with an old RPM version.

BZ#839126, BZ#845063

This update adds the description of the --eval, --setperms and --setugid parameters to the rpm(8) manual page.

All users of rpm are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.219. RSYSLOG

7.219.1. RHBA-2013:0450 — rsyslog bug fix update

Updated rsyslog packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The rsyslog packages provide an enhanced, multi-threaded syslog daemon. Rsyslog supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grain output format control.

Bug Fixes

BZ#838148

Prior to this update, the rsyslog packages depended on a newer selinux-policy which the rsyslog spec file did not reflect. The command "yum --security update" updated rsyslog but not the selinux-policy. As a consequence, rsyslog malfunctioned when booting and depending services failed, including login. This update modifies the spec file to prevent installation with an incompatible selinux-policy package and enforce its update if available.

BZ#847568

Prior to this update, the rule that was specified immediately before the "$IncludeConfig" directive to be reordered after the contents of the included configuration file due to handling problem with the configuration file parser. As a consequence, the order of processing was different from the intended one with the potential of message losses. This update modifies the underlying code so that the order of processing is the same as in the configuration file.

BZ#886004

Prior to this update, the Unix Socket Input plug-in for rsyslog did not consider the timestamp format specified by the RFC 5424 Syslog Protocol for timestamps derived from RFC 3339. As a consequence, messages sent to the syslog daemon via Unix sockets that used the RFC 3339-derived timestamp format were silently discarded. This update supports this timestamp format. Messages sent to the rsyslog system logging daemon via Unix sockets that use the RFC 3339-derived timestamp format are now accepted and processed properly.

All rsyslog users are advised to upgrade to these updated packages, which fix these bugs.

7.220. S390UTILS

7.220.1. RHBA-2013:0395 — s390utils bug fix and enhancement update

Updated s390utils packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The s390utils packages contain a set of user space utilities for Linux on IBM system z achitecture.

Bug Fixes

BZ#818599

The internal parsing logic of the ziomon utility previously relied on a Bash shell construct when identifying multipath devices. Changes in later versions of Bash caused the parsing logic to not work properly if the ziomon command was specified with more than one multipath device as an argument. Consequently, ziomon did not recognize all multipath devices and did not collect performance data for the respective devices. With this update, ziomon has been modified to use a bash-independent construct in the parsing logic. The ziomon utility now correctly recognizes all multipath devices and provides performance data as expected.

BZ#818877

Previously, the /etc/zipl.conf configuration file did not belong to any RPM package. This update corrects this problem and the /etc/zipl.conf file is now owned by the s390utils-base package.

BZ#828145

The "lsdasd -h" command always incorrectly returned an exit code of 1. Also, the lsdasd(8) man page was missing information about the "-b, --base" option. With this update, the lsdasd utility has been corrected to return the exit code 0 on success when issued to print help information. The lsdasd(8) man page has been updated and it now provides information on usage of the "-b" option as expected.

BZ#828146

Previously, the lsluns utility performed a SCSI generic (sg) functionality test before scanning for available LUNs or showing the attached LUNs. Consequently, the lsluns command failed and did not display any available or attached LUNs if there was no SCSI device available. This update modifies lsluns to perform a LUN scan first and execute an sg functionality test only if at least one SCSI device is found.

BZ#837311

The lsluns utility performed a SCSI registration test immediately after adding LUN0 and WLUN to the unit_add file. However, SCSI devices are not available immediately after adding LUNs to unit_add so lsluns did not recognize that LUN0 and WLUN are available. The lsluns command therefore failed with the "Cannot attach WLUN / LUN0 for scanning" error message. This update modifies lsluns so that the SCSI registration test is now performed several times allowing the SCSI mid-layer to complete SCSI device registration. The lsluns command now successfully displays LUNs as expected.

BZ#857815

Due to the way the kernel maintains caches for block devices, running the zipl boot loader could, under certain circumstances, lead to inconsistent cache contents in the first 4096 bytes on an FBA DASD device (a direct-access storage device with a fixed block architecture). This update modifies zipl so that the boot loader flushes disk buffers before installing the initial program load (IPL), which prevents cache corruption from occurring on FBA DASD devices.

Enhancements

BZ#847087

This update adds the necessary user space tools to allow Linux to access Storage Class Memory (SCM) as a block device on IBM System z systems using sub-channels of the Extended Asynchronous Data Mover (EADM) Facility.

BZ#847088

The lszcrypt utility has been modified to support the IBM Crypto Express 4 feature.

All users of s390utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.221. SAMBA4

7.221.1. RHSA-2013:0506 — Moderate: samba4 security, bug fix and enhancement update

Updated samba4 packages that fix one security issue, multiple bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Samba is an open-source implementation of the Server Message Block (SMB) or Common Internet File System (CIFS) protocol, which allows PC-compatible machines to share files, printers, and other information.

NOTE

The samba4 packages have been upgraded to upstream version 4.0.0, which provides a number of bug fixes and enhancements over the previous version. In particular, improved interoperability with Active Directory (AD) domains. SSSD now uses the libndr-krb5pac library to parse the Privilege Attribute Certificate (PAC) issued by an AD Key Distribution Center (KDC).

The Cross Realm Kerberos Trust functionality provided by Identity Management, which relies on the capabilities of the samba4 client library, is included as a Technology Preview. This functionality and server libraries, is included as a Technology Preview. This functionality uses the libndr-nbt library to prepare Connection-less Lightweight Directory Access Protocol (CLDAP) messages.

Additionally, various improvements have been made to the Local Security Authority (LSA) and Net Logon services to allow verification of trust from a Windows system. Because the Cross Realm Kerberos Trust functionality is considered a Technology Preview, selected samba4 components are considered to be a Technology Preview. For more information on which Samba packages are considered a Technology Preview, refer to Table 5.1, "Samba4 Package Support" in the Release Notes. (BZ#766333, BZ#882188)

Security Fix

CVE-2012-1182

A flaw was found in the Samba suite's Perl-based DCE/RPC IDL (PIDL) compiler, used to generate code to handle RPC calls. This could result in code generated by the PIDL compiler to not sufficiently protect against buffer overflows.

Bug Fix

BZ#878564

Prior to this update, if the Active Directory (AD) server was rebooted, Winbind sometimes failed to reconnect when requested by "wbinfo -n" or "wbinfo -s" commands. Consequently, looking up users using the wbinfo tool failed. This update applies upstream patches to fix this problem and now looking up a Security Identifier (SID) for a username, or a username for a given SID, works as expected after a domain controller is rebooted.

All users of samba4 are advised to upgrade to these updated packages, which fix these issues and add these enhancements. Warning: If you upgrade from Red Hat Enterprise Linux 6.3 to Red Hat Enterprise

Linux 6.4 and you have Samba in use, you should make sure that you uninstall the package named "samba4" to avoid conflicts during the upgrade.

7.222. SAMBA

7.222.1. RHBA-2013:0338 — samba bug fix and enhancement update

Updated samba packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Samba is an open-source implementation of the Server Message Block (SMB) and Common Internet File System (CIFS) protocol, which allows PC-compatible machines to share files, printers, and other information.

NOTE

The samba packages have been upgraded to upstream version 3.6, which provides a number of bug fixes and enhancements over the previous version. In particular, support for the SMB2 protocol has been added. SMB2 support can be enabled with the following parameter in the [global] section of the **/etc/samba/smb.conf** file:

```
max protocol = SMB2
```

Additionally, **Samba** now has support for AES Kerberos encryption. AES support has been available in Microsoft Windows operating systems since Windows Vista and Windows Server 2008. It is reported to be the new default Kerberos encryption type since Windows 7. Samba now adds AES Kerberos keys to the keytab it controls. This means that other Kerberos based services that use the Samba keytab and run on the same machine can benefit from AES encryption. In order to use AES session keys (and not only use AES encrypted ticket granting tickets), the Samba machine account in Active Directory's LDAP server needs to be manually modified. For more information, refer to the Microsoft Open Specifications Support Team Blog.

Also note that several *Trivial Database* (TDB) files have been updated and printing support has been rewritten to use the actual registry implementation. This means that all TDB files are upgraded as soon as you start the new **Samba** server daemon (**smbd**) version. You cannot downgrade to an older **Samba** version unless you have backups of the TDB files. (BZ#649479)

WARNING

The updated samba packages also change the way ID mapping is configured. Users are advised to modify their existing **Samba** configuration files. For more information, refer to the Release Notes for Samba 3.6.0, the **smb.conf** man page and the individual IDMAP backend man pages.

If you upgrade from Red Hat Enterprise Linux 6.3 to Red Hat Enterprise Linux 6.4 and you have **Samba** in use, you should make sure that you uninstall the package named samba4 to avoid conflicts during the upgrade.

Bug Fixes

BZ#760109

Previously, the **pam_winbind** utility returned an incorrect PAM error code if the **Winbind** module was not reachable. Consequently, users were not able to log in even if another PAM Module authenticated the user successfully. With this update, the error **`PAM_USER_UNKNOWN`** is always returned in case Winbind fails to authenticate a user. As a result, users successfully authenticated by another PAM module can log in as expected.

BZ#838893

Samba 3.6 failed to migrate existing printers from the *Trivial Database* (TDB) to the registry due to a *Network Data Representation* (NDR) alignment problem. Consequently, printers from 3.5 could not be migrated and the **Samba** server daemon (**`smbd`**) stopped with an error. The NDR parser has been fixed to correctly parse printing entries from Samba 3.5. As a result, printers are correctly migrated from 3.5 TDB to the 3.6 registry.

BZ#866412

Due to a regression, the previous release changed the behavior of resolving domain local groups and the **Winbind** daemon (**`winbindd`**) could not find them. The original behavior for resolving the domain local groups has been restored. As a result, the **`ID`** command resolves domain local groups in its own domain correctly again.

BZ#866570

The **net** utility improperly displayed the realm which it had joined in all lowercase letters. Consequently, a user might misunderstand the domain join and might use the lowercase format of the realm name. This update corrects the case and improves the wording of the message printed about a domain join. As a result, the user is correctly informed as to which **`DNS`** domain the system has joined.

BZ#875879

If a *Domain Controller* (DC) was rebuilding the *System Volume* (Sysvol) shared directory and turned off **netlogon**, users were not able to log in until it was finished, even if another working DC was available. Consequently, users could not log in and got strange errors if **netlogon** was available and then was turned off. With this update, **Samba** retries twice to open the **netlogon** connection and if it still does not work the DC is added to the negative connection cache and Samba will failover to the next DC. As a result, the user no longer sees any error messages in this scenario and can log in using another DC as expected.

Enhancements

BZ#748407

When joining an *Active Directory* domain and using Samba's support for using Kerberos keytabs, AES Kerberos keys were not added into the generated keytab. Consequently, **Samba** did not support the new AES encryption type for Kerberos. This update adds support for AES Kerberos keys to Samba and AES Kerberos Keys are now created in the keytab during the Domain join.

Users of samba are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.223. SCL-UTILS

7.223.1. RHBA-2013:0400 — scl-utils bug fix and enhancement update

Updated scl-utils packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The scl-utils packages provide a runtime utility and RPM packaging macros for packaging Software Collections. Software Collections allow users to concurrently install multiple versions of the same RPM packages on the system. Using the scl utility, users may enable specific versions of RPMs, which are installed into the /opt directory.

BZ#855999

The scl-utils packages have been upgraded to upstream version 20120927, which provides a number of bug fixes and enhancements over the previous version. The following list includes notable bug fixes:

- The fix has been provided for a double free or corruption error when reading commands from the standard input, which could have led to a segmentation fault under certain circumstances.
- The /usr/lib/rpm/redhat/brp-compress script now properly compresses man pages in %_mandir.

All users who require scl-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.224. SEABIOS

7.224.1. RHBA-2013:0307 — seabios bug fix and enhancement update

Updated seabios packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The seabios packages contain an open-source legacy BIOS implementation which can be used as a coreboot payload. It implements the standard BIOS calling interfaces that a typical x86 proprietary BIOS implements.

Bug Fixes

BZ#771616

In the QXL-VGA drive, the ram_size and vram_size variables were set to a default value that was too high. Consequently, the guest was not able to boot, and the "VM status: paused (internal-error)" message was returned. This update uses extended addressing for PCI address space and the guest can now boot successfully.

BZ#839674

Previously, the advertisement of S3 and S4 states in the default BIOS was disabled for which a separate BIOS binary file had been created. This update enables users to configurate S3 and S4 states per virtual machine in seabios and thus, the extra BIOS binary file is no longer necessary. Now, a single binary is used to enable these states.

BZ#851245

Prior to this update, the SeaBIOS component did not support the non-contiguous APIC IDs. This resulted in incorrect topology generation on SMP and NUMA systems; moreover, QEMU-KVM was unable to run on some of the host systems. A patch has been provided to fix this bug and Seabios now supports the non-contiguous APIC IDs.

BZ#854448

The seabios packages used the time-stamp counter (TSC) for timekeeping with a simple calibration loop. As a consequence, on a busy host, the magnitude calibration could be set incorrectly and could lead to boot failures. This update provides the power management timer (PMT) with a fixed frequency, which does not suffer from calibration errors due to a loaded host machine. As a result, timeouts work correctly under all circumstances.

Enhancements

BZ#827500

With this update, it is possible to configurate S3 and S4 states per virtual machine.

BZ#831273

The seabios packages are now able to reboot a VM even if no bootable device can be found.

Users of seabios are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.225. SELINUX-POLICY

7.225.1. RHBA-2013:0537 — selinux-policy bug fix update

Updated selinux-policy packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fix

BZ#912392

When multiple devices were added into the system, udev rules restarted ktune services for each new device, so there were several restarts in a short time interval. The multiple restarts triggered a race condition in the kernel which was not easily fixable. Currently, the tuned code is modified not to trigger more than one restart per 10 seconds and the race condition is avoided.

Users of selinux-policy are advised to upgrade to these updated packages, which fix this bug.

7.225.2. RHBA-2013:0314 — selinux-policy bug fix and enhancement update

Updated selinux-policy packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The selinux-policy contain the rules that govern how confined processes run on the system.

Bug Fixes

BZ#837815

With the Multi-Level Security (MLS) SELinux policy enabled, a user created with an SELinux MLS level could not login to the system through an **SSH** client. The SELinux policy rules have been updated to allow the user to log in to the system in the described scenario.

BZ#835923

When SELinux was in enforcing mode, an **OpenMPI** job, parallel universe in Red Hat Enterprise Linux MRG Grid, failed and was unable to access files in the **/var/lib/condor/execute/** directory. New SELinux policy rules have been added for **OpenMPI** jobs to allow a job to access files in this directory.

BZ#857352

When SELinux was in enforcing mode, a migration from one host to another using the Red Hat Enterprise Virtualization Manager was denied. This update fixes relevant SELinux policy rules and the migration now completes as expected in the described scenario.

BZ#865759

Due to a regression, the root user was able to log in when the **ssh_sysadm_login** variable was set to **OFF** in MLS. To fix this bug, the **ssh_sysadm_login** SELinux boolean has been corrected to prevent the root user to log in when this variable is set to **OFF**.

BZ#877108

When the user ran the **system-config-kdump** utility on the IBM System z architecture, the following error message was returned:

```
error opening /etc/zipl.conf for read: Permission denied
```

This error was caused by missing SELinux policy rules. With this update, the respective rules have been updated to allow **system-config-kdump** to access the **/etc/zipl.conf** file, and the error messages are no longer returned.

BZ#877932

Previously, **cron** daemon jobs were set to run in the **cronjob_t** domain when the SELinux MLS policy was enabled. As a consequence, users could not run their **cron** jobs. The relevant policy rules have been modified and **cron** jobs now run in the user domain, thus fixing this bug.

BZ#880369

When the user added a mount point to the **/var/lib/openshift** file and executed the **quotacheck -cmug /var/lib/openshift** command, the process resulted in AVC messages logged in the **/var/log/audit/audit.log** file. With this update, the quota system can manage **openshift_var_lib_t** directories to make the command work as expected.

BZ#867002

When the system was set up to use the **SSSD** system daemon to perform user authentication, the **passwd** utility was not allowed to read the **/var/lib/sss/mc/** directory. This update fixes the security context for **/var/lib/sss/mc/** to allow **passwd** to read this directory as expected.

BZ#878212

With SELinux in enforcing mode, during automatic testing of Red Hat Enterprise Linux in FIPS mode, PAM (Pluggable Authentication Modules) attempted to run prelink on the **/sbin/unix_chkpwd** file to verify its hash. Consequently, users could not log in to the system. The appropriate SELinux policy rules have been updated and a FIPS mode boolean has been added to resolve this bug.

BZ#887129

Previously, the **`system-config-kdump`** utility was unable to handle the **`kdump`** service when SELinux was in enforcing mode for 64-bit PowerPC. To fix this bug, the security context for the ***`/usr/lib/yaboot/addnote`*** binary file has been changed to the **bin_t** type. With this update, **`system-config-kdump`** handles **`kdump`** as expected.

BZ#869376

Due to a missing SELinux policy rule, certain services failed to start in enforcing mode. This update adds the **mount_t unlabeled_t:filesystem relabelfrom;** rule to make sure these services start as expected.

BZ#881413

Previously, if the user added the **includedir /var/lib/sss/pubconf/krb5.include.d/** directive to a **`krb5.conf`** file in Identity Manager and installed a server in permissive mode, it generated numerous AVC messages because a number of processes were not able to read the contents of the included directory. This update adds rules to allow domains that can read the **sssd_public_t** type to also list this directory.

BZ#859231

When the krb5 package was upgraded to version 1.9-33.el6_3.3 and Identity Management or FreeIPA was used, an attempt to start the **`named`** daemon terminated unexpectedly in enforcing mode. This update adapts the relevant SELinux policy to make sure the **`named`** daemon can be started in the described scenario.

BZ#858235

Previously, the **`rhnsd`** daemon was handled by the **`rhsmcertd`** SELinux domain, which caused an AVC denial message to be returned. With this update, **`rhnsd`** has its own SELinux policy domain called **`rhnsd_t`**, thus preventing these messages.

BZ#831908

When the **`SANLOCKOPTS="-w 0"`** option was enabled in the ***`/etc/sysconfig/sanlock`*** configuration file, AVC denial messages were generated by the **`service sanlock restart`** command. The SELinux rules have been updated to allow the **`sanlock`** daemon to be restarted correctly without any AVC messages.

BZ#855889

Previously, the **`libselinux`** library did not support setting the context based on the contents of ***`/etc/selinux/targeted/logins/$username/`*** directories. Consequently, central management of SELinux limits did not work properly. With this update, the ***`/etc/selinux/targeted/logins/`*** directory is now handled by the selinux-policy packages as expected.

BZ#854671

With SELinux in enforcing mode, the running the **`openswan`** service with FIPS enabled caused AVC denial messages to be logged to the ***`/var/log/audit/audit.log`*** file. This update fixes the relevant SELinux policy rules and **`openswan`** no longer produces AVC messages.

BZ#852763

With the SELinux MLS policy enabled, users could not mount a file via a loop device. This bug has been fixed, and users can mount a file via a loop device to the **/mnt/** directory successfully.

BZ#835936

When SELinux was running in enforcing mode, it was impossible to start a virtual machine on a disk located on a POSIX file system, such as GlusterFS. The relevant SELinux policy has been fixed and virtual machines can now be started in the described scenario as expected.

BZ#843814

In its current version, the **SSSD** daemon writes SELinux configuration files into the **/etc/selinux/<policy>/logins/** directory. The SELinux PAM module then uses this information to set the correct context for a remote user trying to log in. Due to a missing policy for this feature, **SSSD** could not write into this directory. With this update, a new security context for **/etc/selinux/<[policy]/logins/** has been added together with appropriate SELinux policy rules.

BZ#836311

Previously, the **heartbeat** subsystem was incorrectly treated by the **corosync** SELinux policy. Consequently, AVC messages were generated and **heartbeat** was unusable by default. To fix this bug, **heartbeat** is now handled by the **rgmanager** SELinux policy and AVC messages are no longer returned.

BZ#837138

With SELinux in enforcing mode, the **clamscan** utility did not work correctly as a backup server in the **amavisd-new** interface, which resulted in AVC messages to be returned if **clamscan** could not access **amavis** spool files. This update corrects the SELinux policy to grant **clamscan** the necessary permission in the described scenario.

BZ#887892

Previously, SELinux prevented the **ABRT** (Automatic Bug Reporting Tool) utility to use the **inotify** subsystem on the **/var/spool/abrt-upload/** directory. Consequently, when the user set up the **WatchCrashdumpArchiveDir** option in the **ABRT** utility, the **abrtd** daemon failed on restart. To fix this bug, a SELinux policy rule has been added to allow **ABRT** to use **inotify** on **/var/spool/abrt-upload/** with the daemon working correctly.

BZ#842818

With SELinux in enforcing mode, the **saslauthd** daemon process could not work properly if the **MECH=shadow** option was specified in the **/etc/sysconfig/saslauthd** file. This update fixes the relevant SELinux policy rules and allows **saslauthd** to use the **MECH=shadow** configuration option.

BZ#842905

Previously, when a process with the **user_r** SELinux role tried to use the **crontab** utility on an NFS (Network File System) home directory, AVC messages were written to the audit.log file. The relevant SELinux policy has been updated to allow **user_r** processes to run the **crontab** utility, thus fixing the bug.

BZ#842927, BZ#842968

When the **MAILDIR=$HOME/Maildir** option was enabled either in the **/etc/procmailrc** or in

dovecot configuration files, the **procmail** and **dovecot** services were not able to access a Maildir directory located in the home directory. This update fixes relevant SELinux policy rules to allow the **procmail**/**dovecot** service to read the configured **MAILDIR** option in **/etc/procmailrc**.

BZ#886874

When the **vsftpd** daemon is being stopped, it terminates all child **vsftpd** processes by sending the SIGTERM signal to them. When the parent process dies, the child process gets the SIGTERM signal. Previously, this signal was blocked by SELinux. This update fixes the relevant SELinux policy rules to allow **vsftpd** to terminate its child processes properly.

BZ#885518

Previously, the **/var/lib/pgsql/.ssh/** directory had an incorrect security context. With this update, the security context has been changed to the **ssh_home_t** label, which is required by the **PostgreSQL** system backup.

BZ#843543

Due to an incorrect SELinux policy, SELinux prevented the **libvirtd** daemon from starting the **dnsmasq** server with the **--pid-file=/var/run/libvirt/network/default.pid** option and AVC denial messages were returned. The updated SELinux rules allow the **libvirtd** daemon to start correctly with **dnsmasq** support.

BZ#843577

With the MLS SELinux policy enabled, an administrator in an SELinux domain, with the **sysadm_t** type at the **s0-s15:c0.c1023** level, was not able to execute the **tar --selinux -zcf wrk.tar.gz /wrk** command. These updated SELinux rules allow administrators to run the command in the described scenario.

BZ#843732

Due to a missing fcontext for the **/var/named/chroot/lib64/** directory, AVC messages could be returned when working with the **named** daemon. To fix this bug, the missing SELinux security context for **/var/named/chroot/lib64/** has been added.

BZ#836241

Due to an incorrect SELinux policy, the **dovecot-imap** and **dovecot-lda** utilities were not allowed access to the Maildir files and directories with the **mail_home_rw_t** security context. These updated SELinux rules allow **dovecot-imap** and **dovecot-lda** to access Maildir home directories.

BZ#844045

With SELinux in enforcing mode, the **automount** utility erroneously returned the **mount.nfs4: access denied by a server** error message when instructed to perform a mount operation, which included a ***context=*** parameter. Mount operations in NFS v3 were not affected. Now, SELinux policy rules have been updated to allow **automount** to work correctly in the described scenario.

BZ#809716

Due to an incorrect SELinux policy, the **smartd** daemon was not able to create the **megaraid_sas_ioctl_node** device with the correct SELinux security context. Consequently, monitoring of some disks on a MegaRAID controller using **smartd** was prevented. This update provides SELinux rules that allow monitoring of disks on a MegaRAID controller using **smartd**.

BZ#845201

Previously, the incorrect default label on the **`/etc/openldap/cacerts/`** and **`/etc/openldap/certs/`** directories was provided by SELinux policy, which caused various unnecessary AVCs to be returned. To fix this bug, these directories have been labeled with the **slapd_cert_t** SELinux security label. Now, no redundant AVCs are returned.

BZ#882348, BZ#850774

Previously, with SELinux in enforcing mode and the **`internal-sftp`** subsystem configured together with the **`Chroot`** option, users with the **unconfined_t** SELinux type were unable to connect using the **`sftp`** utility. This update fixes the SELinux policy to allow users to utilize **`sftp`** successfully in the described scenario.

BZ#849262

Previously, the **`snmpd`** daemon service was unable to connect to the **`corosync`** service using a Unix stream socket, which resulted in AVC messages being logged in the **`/var/log/audit/audit.log`** file. To fix this bug, a set of new rules has been added to the SELinux policy to allow the **`snmpd`** daemon to connect to **`corosync`**.

BZ#849671

With SELinux in enforcing mode, the **`/var/run/amavisd/clamd.pid`** file was empty, thus any attempt to restart the **`clamd.amavisd`** daemon failed. Stopping the service failed because of the empty PID file and starting it failed because the socket was already in use or still being used. These updated SELinux rules allow **`clamd.amavisd`** to write to the PID file as expected.

BZ#851113

Due to an incorrect SELinux policy, there was an incorrect label on the **`/var/run/cachefilesd.pid`** file. With this update, SELinux policy rules and the security context have been fixed to get the **cachefilesd_var_run_t** label for the file.

BZ#881993

Due to missing SELinux policy rules, the **`rsync`** daemon, which served an automounted home NFS directory, was not able to write files in this directory. To fix this bug, the **`rsync`** daemon has been changed into a home manager to allow the needed access permissions.

BZ#851289

Previously, the **8953**/**tcp** port used the **port_t** SELinux port type, which prevented the **unbound** service from working correctly. To fix this bug, the **8953**/**tcp** port has been associated with the **rndc_port_t** SELinux port type.

BZ#851483

The spice-vdagent package was rebased to the latest upstream version (BZ#842355). A part of this rebased spice-vdagent was moved to the **`syslog()`** function instead of using its own logging code (BZ#747894). To reflect this change, the SELinux policy rules have been updated for the spice-vdagent policy to allow the use of **`syslog()`**.

BZ#852731

Previously, when a user wanted to create a user home directory on a client which did not exist, they could do so on local volumes. However, this operation was blocked in enforcing mode when the **`pam_oddjob_mkhomedir.so`** module attempted to create a home directory on an NFS mounted volume. SELinux policy rules have been updated to allow **pam_oddjob_mkhomedir** to use NFS and user home directories can now be created in enforcing mode as well.

BZ#853453

When the **.forward** file was configured by the user on NFS, AVC messages were returned. Consequently, **Postfix** was not able to access the script in the aforementioned file. These updated SELinux rules allow to properly set up **.forward** in the described scenario.

BZ#811319

Previously, the **fence_virtd** daemon was unconfined by SELinux, which caused the service to run in the **initrc_t** type SELinux domain. To fix this bug, the **fenced_exec_t** security context has been added for the **fence_virtd** daemon, and this service now runs in the **fenced_t** SELinux domain.

BZ#871038

Previously, with SELinux in enforcing mode, the **setroubleshootd** daemon was not able to read the **/proc/irq** file. Consequently, AVC messages were returned. This update provides SELinux rules, which allow **setroubleshootd** to read **/proc/irq**, and AVC messages are no longer returned.

BZ#833463

With SELinux running in enforcing mode, the **fence_vmware_soap** binary did not work correctly. Consequently, fencing failed, services did not failover, and AVC denial messages were written to the **audit.log** file. This update fixes the relevant policy to make the **fence_vmware_soap** binary work correctly.

BZ#832998

Prior to this update, a proper security context for the **/usr/lib/mozilla/plugins/libflashplayer.so** file was missing. Consequently, executing the **mozilla-plugin-config -i** command caused the following error to be returned:

```
*** NSPlugin Viewer  *** ERROR:
/usr/lib/mozilla/plugins/libflashplayer.so: cannot restore segment prot
after reloc: Permission denied
```

The security context has been updated, and the command now works as expected.

BZ#821887

A missing SELinux policy prevented the Red Hat Enterprise Virtualization Hypervisors to recreate the **/etc/mtab** file with a correct security context. To fix this bug, a new SELinux transition from the **virtd_t** to **mount_t** SELinux domain has been added.

BZ#858406

Due to missing SELinux policy rules, Point-In-Time Recovery (PITR) implementation with the support for the **SSH** and **RSync** protocols failed to work with PostgreSQL. To resolve this bug, the **postgresql_can_rsync** SELinux boolean has been added to allow PostgreSQL to run the **rsync** utility and interact with SSH.

BZ#858784

With SELinux in enforcing mode, the **pulse** utility failed to start the Internet Protocol Video Security (**IPVS**) sync daemon at startup. SELinux policy rules have been updated to allow **pulse** start the daemon as expected.

BZ#829274

Previously, the SELinux Multi-Level Security (MLS) policy did not allow the **sysadm_r** SELinux role to use the **`chkconfig SERVICE on/off`** commands to enable or disable a service on the system. This update fixes the relevant SELinux policy to allow the **sysadm_r** SELinux role to use these commands to enable or disable the service.

BZ#860666

Due to missing SELinux policy rules, the rebased krb5 package version 1.10 returned the following AVC message:

```
type=AVC msg=audit(1348602155.821:530): avc:  denied  { write } for
pid=23129 comm="kadmind" path="anon_inode:[eventfd]" dev=anon_inodefs
ino=3647 scontext=unconfined_u:system_r:kadmind_t:s0
tcontext=system_u:object_r:anon_inodefs_t:s0 tclass=file
```

With this update, the **`kadmind`** utility has been allowed to access **anon_inode** file descriptors to fix the AVC message.

BZ#868959

Previously, the cluster-cim package was allowed to be used in enforcing mode. However, AVC messages connected with access to the /**var**/**run**/**clumond.sock** and /**var**/**run**/**cman_client** Unix sockets were identified. To fix this bug, new SELinux policy rules have been provided to allow the **`cimprovag`** utility to connect to the **cman_client** socket.

BZ#861011, BZ#901565

Previously, the **`/var/nmbd/`** directory was labeled as **`var_t`**, which caused issues with Samba services which needed to access this directory. The security context has been updated and Samba can now access this directory as expected. Furthermore, SELinux can prevent the **`nmbd`** service from writing into the **`/var/`** repository, which causes problems with NetBIOS name resolution and leads to SELinux AVC denial messages.

BZ#867001

In the previous update, the rsyslog-gssapi package allowed the **`rsyslog`** utility to use the Generic Security Services Application Program Interface (GSSAPI). However, AVC messages were returned as a consequence. This update fixes relevant SELinux policy rules to allow the **`rsyslog`** utility to use Kerberos tickets on the client side.

BZ#865567

With SELinux in enforcing mode, when the **`fail2ban`** service was restarted and **`fail2ban`** was not able to execute the **`ldconfig`** and **`iptables`** commands, it resulted in SELinux AVC denial messages being returned. This update fixes the relevant SELinux policy rules to allow **`fail2ban`** to execute **`ldconfig`** and also fix security contexts for **`iptables`** binaries.

BZ#841950

Due to an incorrect security context for the **`/opt/sartest`** file, data could not be written to this location by the **`sadc`** utility running from a root **`cron`** daemon job. The security context has been updated and now **`sadc`** running from a root **`cron`** job can write data to this location.

BZ#860858

Previously, when the **clamdscan** utility was called by a Sendmail filter, the **clamd** daemon was not able to scan all files on the system. This update adds the **clamscan_can_scan_system** variable to allow all antivirus programs to scan all files on the system.

BZ#825221

Due to missing SELinux policy rules, the **restorecon** utility disregarded custom rules for symbolic links. These updated SELinux rules allow **restorecon** to properly handle custom rules for symlinks.

BZ#863407

Due to missing SELinux policy rules, the **freshclam** utility was not able to update databases through the **HTTP proxy** daemon when run by the **cron** daemon. To fix this bug, the relevant SELinux policy rules have been updated. As a result, **freshclam** now updates databases as expected in the described scenario.

BZ#864546, BZ#886619

Previously, SELinux prevented the puppet master from running passenger web application. To fix this bug, security context for the Passenger Apache module has been updated to reflect latest passenger paths to executables to make sure all applications using Passenger web applications run with the correct SELinux domain.

BZ#860087

When a user set up the Red Hat Enterprise Linux 6 system as a VPN server with the **IPSec+L2TP** VPN, SELinux prevented the **pppd** daemon from accessing some needed components after connecting to the VPN server with the following error message:

```
pppd needs to be allowed also to "read" and "write" operations on
l2tpd_t:socket
```

This update adds the missing SELinux policy to make sure all **pppd** actions are enabled by SELinux.

BZ#823647

Previously, some patterns in the **/etc/selinux/targeted/contexts/files/file_contexts** file contained typo errors. Some patterns matched the 32-bit path, but the same pattern for the 64-bit path was missing. Consequently, different security contexts were assigned to these paths. With this update, the relevant file context specifications have been corrected so that there are no more differences between these paths.

BZ#831068

Previously, when a user tried to change a password in the GNOME user account dialog window, the attempt was blocked by SELinux in enforcing mode due to missing SELinux rules for the **passwd_t** SELinux domain. With this update, SELinux policy rules have been added to allow users to change their passwords in the GNOME user account dialog window.

BZ#871106, BZ#882850

Previously, there were problems to hook certain monitoring plug-ins to the **munin** plug-in domain with SELinux in enforcing mode. To fix this bug, the **unconfined_munin_plugin_t** SELinux type has been added to the SELinux policy to cover all unconfined **munin** plug-ins. As a result, **munin** plug-ins can now run unconfined.

BZ#871816

With SELinux in enforcing mode, the **ipactl** restart command caused AVC denial messages to be returned. This update fixes the relevant SELinux policy rules and the command no longer produces AVC messages.

BZ#855286

While installing an ISO image on a virtual machine (VM) from Red Hat Enterprise Virtualization Manager, AVC messages were generated. These AVC were returned due to the **sanlock** utility which could not access files and directories on the FUSE file system. To fix this bug, the **sanlock_use_fusefs** SELinux boolean variable has been added and installing from an ISO image on a VM now succeeds.

BZ#853970

Previously, a Red Hat Cluster Suite node did not auto-join a cluster ring after power fencing due to missing SELinux policy rules for the **corosync** utility. Consequently, **corosync** failed to reboot. To fix this bug, **corosync** has been allowed to use **1229/udp** and **1228/udp** ports to make auto-join a cluster ring after power fencing. As a result, a machine re-joins the cluster after fencing and reboots as expected.

BZ#853852

Previously, the SELinux boolean variable for NFS failed to prevent an NFS client from accessing a share. Consequently, the NFS client could mount an NFS share and read or write files. Because the NFS server runs as a kernel process, the **nfs_export_all_rw** boolean variable was needed no longer and has been removed from the policy, thus fixing the bug. NFS clients now cannot access shares in the described scenario.

BZ#879266

When the user was installing Red Hat Cluster Suite packages from Red Hat Network, the installation process became unresponsive and the cluster suite was not installed. With this update, the relevant policy has been added and Red Hat Cluster Suite packages from RHN can now be installed as expected.

BZ#880407

Previously, if the user ran the **restorecon** utility on **/ect/multipath*** directories and files, the security context was reset. This update fixes relevant SELinux policy rules and adds updated SELinux security context for these directories and files.

BZ#846069

Previously, the **piranha-web** utility was unable to connect to the **windbind** daemon using Unix stream sockets. Consequently, AVC messages were returned. To fix this bug, a set of new rules has been added to the SELinux policy to allow the **piranha-web** service to connect to **windbind**.

BZ#883143

Due to the incorrect **git_read_generic_system_content_files()** interface, the **git-daemon** and **httpd** daemons could not serve the same directory. To fix this bug, the **git_read_generic_system_content_files()** interface has been updated to allow **git-daemon** and **httpd** to serve the same directory.

BZ#809877

Previously, due to incorrect file context specifications, the policy did not always have a correct label for files in the **/var/log/** directory which were processed by the **logrotate** utility. To fix this bug, the file context specifications have been updated and the files and directories processed by **logrotate** now have correct labels.

BZ#844448

Previously, the **munin-node** agent lacked necessary SELinux rules for reading Exim log files. Consequently, multiple bundled exim plug-ins were prevented from working and **munin-node** terminated unexpectedly. This update fixes the relevant SELinux policy rules to allow **munin-node** to read exim log files to make exim Munin plug-ins working correctly.

BZ#843455

Previously, when the user tried to use the **munin_stats** Munin plug-in, it caused AVC messages to be returned. To fix this bug, updated SELinux policy rules have been provided and **munin_stats** now works as expected.

BZ#886563

If a user tried to use a post-login script in the **dovecot** utility, an AVC message was returned. This update fixes relevant SELinux policy rules and adds updated SELinux rules to allow **dovecot** to start the **/bin/bash** file. Now, AVC messages are no longer returned.

BZ#841329

Due to an incorrect SELinux policy, confined SELinux users could not decrypt S/MIME (Secure/Multipurpose Internet Mail Extensions) emails by preventing the **gpg-agent** daemon from reading the **/dev/random** file. The **claws-mail** client using the **smime** utility was affected by this bug. Now, SELinux policy rules have been updated to allow SELinux confined users to decrypt S/MIME emails.

BZ#770065

Previously, when a user tried to use the **check_icmp** Munin plug-in, AVC messages were returned. With this update, a corrected SELinux policy has been provided for **check_icmp**, thus fixing the bug.

BZ#890687

When a user attempted to configure the **rsync** daemon to log directly to a specific file, missing SELinux policy rules let the user create the log file, but did not allow to append to it. With this update, SELinux policy rules have been added to allow **rsync** to append to a specific log file.

BZ#821483

With SELinux in enforcing mode, running a **spamd** daemon process updating Razor configuration files resulted in a permission to be denied and an AVC message to be generated. This update fixes relevant SELinux policy rules to allow **spamd** processes to update Razor configuration files in the described scenario.

BZ#869304

With SELinux in enforcing mode, on a Red Hat Enterprise Linux 6.3 hypervisor, SELinux prevented the QEMU-KVM **getattr()** function access when starting VMs from Red Hat Enterprise Virtualization Manager hosted on a Red Hat Storage (RHS) storage domain. This update fixes relevant SELinux policy rules to allow the QEMU-KVM **getattr()** access.

BZ#867628

Prior to this update, the manual pages did not reflect actual state of SELinux policy rules. To fix this bug, the actual policy has been included in the selinux-policy package. Furthermore, all auto-generated manual pages are now regenerated on the system using the **`sepolicy`** utility from Fedora to provide better SELinux manual pages for each SELinux domain.

BZ#887793

The **`wdmd`** watchdog daemon used the **`/etc/wdmd.d/checkquorum.wdmd`** script, both provided by the sanlock package, for checking out the cluster state. Consequently, with SELinux enabled, this detection failed resulting in a self-resetting loop. To fix this bug, the SELinux support for the **`watchdog`** script from the **`sanlock`** utility has been added, and the detection no longer fails.

Enhancements

BZ#739103

On Red Hat Enterprise Linux 6, root privileges are required to start a KVM guest with bridged networking. The **`libvirt`** library in turn launches a QEMU process as the unprivileged **`qemu`** user. New **`qemu:///session`** URIs introduced to **`libvirt`** attempted to allow the unprivileged user to start KVM guests and have the QEMU process execute as the same unprivileged user but failed since the **`CAP_NET_ADMIN`** capability is required to use TUN/TAP networking. To fix this bug from the SELinux perspective, a new SELinux policy has been added for a networking helper program that QEMU can invoke.

BZ#801493

This update provides a new SELinux policy for the **`pacemaker`** service.

BZ#807157

This update provides a new SELinux policy for the **`numad`** service.

BZ#807678

This update provides a new SELinux policy for the **`bcfg2-server`** service.

BZ#836034

This update provides a new SELinux policy for the OpenStack Essex cloud computing framework.

BZ#834994

This update provides a new SELinux policy for the **`rhnsd`** service.

BZ#839250, BZ#838260

A new SELinux *antivirus policy* module has been introduced in this release. This module contains the **antivirus_db_t** file type and the **`antivirus`** attribute to consolidate all anti-virus programs on the system. The module also allows to manage files and directories labeled with the **antivirus_db_t** file type.

BZ#833557

This update provides a new SELinux policy for the **`xl2tpd`** service.

BZ#827389

This update adds SELinux support for the Gitolite v.3 utility, which allows users to set up hosting of Git repositories on a central server.

BZ#811361

This update provides a new SELinux policy for the **`svnserve`** service.

BZ#811304

This update provides a new SELinux policy for the **`glusterd`** daemon.

BZ#848915

This update provides a new SELinux policy for the **`slpd`** daemon.

BZ#845417

This update provides a new SELinux policy for the **`ovs-vswitchd`** and **`ovs-brcompatd`** Open vSwitch services.

BZ#845033

This update provides a new SELinux policy for the **iucvtty** application provides full-screen terminal access to a Linux instance running as a z/VM Inter-User Communication Vehicle (IUCV).

BZ#839831

The QEMU emulator now provides a new **`qemu-ga`** (guest agent) daemon. This daemon runs on the guest and executes commands on behalf of processes running on the host. This update provides a new SELinux policy for a new **`qemu-ga`** (guest agent) daemon.

BZ#848918

This update provides a new SELinux policy for the **`sencord`** service.

BZ#851128, BZ#888164

SELinux support has been added for the **`rpc.rstatd`** and **`rpc.rusersd`** daemons to prevent them from running in the **`initrc_t`** SELinux domain. Now, these services run in the **`rpcd_t`** SELinux domain.

BZ#851241

This update provides a new SELinux policy for the **`cpglockd`** service.

BZ#885432

Support for the **`/usr/share/ovirt-guest-agent/ovirt-guest-agent.py`** file has been added to these updated packages.

BZ#875839

Support for OpenShift Enterprise Policy has been added to Red Hat Enterprise Linux 6.4.

Users of selinux-policy are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.226. SETROUBLESHOOT

7.226.1. RHBA-2013:0387 — setroubleshoot bug fix update

Updated setroubleshoot packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

This package provides a set of analysis plugins for use with setroubleshoot. Each plugin has the capacity to analyze SELinux AVC (Access Vector Cache) data and system data to provide user friendly reports describing how to interpret SELinux AVC denial messages.

Bug Fixes

BZ#788196

Prior to this update, the "sealert -a /var/log/audit/audit.log -H" command did not work correctly. When opening the audit.log file, the sealert utility returned an error when the "-H" option was used. The relevant source code has been modified and the "-H" sealert option is no longer recognized as a valid option.

BZ#832143

Previously, SELinux Alert Browser did not display alerts even if SELinux denial messages were present. This was caused by the sedispatch utility, which did not handle audit messages correctly, and users were not able to fix their SELinux issues according to the SELinux alerts. Now, SELinux Alert Browser properly alerts the user in the described scenario.

BZ#842445

Under certain circumstances, sealert produced the " 'tuple' object has no attribute 'split' " error message. A patch has been provided to fix this bug. As a result, sealert no longer returns this error message.

BZ#851824

The sealert utility returned parse error messages if an alert description contained parentheses. With this update, sealert has been fixed and now, the error messages are no longer returned in the described scenario.

BZ#864429

Previously, improper documentation content was present in files located in the /usr/share/doc/setroubleshoot/ directory. This update removes certain unneeded files and fixes content of others.

Users of setroubleshoot are advised to upgrade to these updated packages, which fix these bugs.

7.227. SETUP

7.227.1. RHBA-2012:1367 — setup bug fix update

Updated setup packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The setup packages provide a set of important system configuration and setup files, such as passwd, group, and profile.

Bug Fixes

BZ#791140

Prior to this update, the "/etc/profile" script used a non-portable method for undefining the pathmunge() function. As a consequence, the script could encounter problems when using the korn shell (ksh). This update modifies the undefining method of the function to work more efficiently with alternative shells.

BZ#839410, BZ#860221

Prior to this update, the accounts for the haproxy system user, the jbosson-agentsystem user, and the jbosson system group were created with dynamic uid/gid assignment, which is not recommended for network daemons and for sensitive data. With this update, the static uid/gid pair 188:188 can be used to create these users and groups.

All users of setup are advised to upgrade to these updated packages, which fix these bugs.

7.228. SLAPI-NIS

7.228.1. RHBA-2013:0370 — slapi-nis bug fix update

An updated slapi-nis package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The slapi-nis package contains the NIS server plug-in and the Schema Compatibility plug-in for use with the 389 directory server.

Bug Fixes

BZ#840926

While updating their internal data caches after the server had processed an LDAP modify request, the modules leaked a small amount of memory after every modify request. This bug has been fixed and no memory is now leaked in the described scenario.

BZ#829502

At build-time, the slapi-nis package attempted to detect if it was being built for a version of the directory server which included support for backend transactions. If this support was detected, the plug-in enabled its own optional logic for supporting transactions in order to allow it to interact properly with the server and other plug-ins. Some time after this support was added to slapi-nis, the recommended strategy for integrating with a transaction-enabled server was revised, rendering changes in slapi-nis incorrect. This update explicitly disables that support in these plug-in, thus preventing this support from interfering with normal directory server operations.

Users of slapi-nis are advised to upgrade to this updated package, which fixes these bugs.

7.229. SLF4J

7.229.1. RHBA-2012:1239 — slf4j bug fix update

Updated slf4j packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The Simple Logging Facade (SLF4J) for Java serves as a simple facade for various logging APIs allowing the end-user to plug in the desired implementation at deployment time.

Bug Fix

BZ#831933, BZ#828644

The slf4j packages contained a non-functional dummy API implementation which was not supposed to be used. This dummy implementation was always selected instead of other implementations and UnsupportedOperationException was thrown. The dummy API implementation has been removed, so that user-supplied implementation is now always chosen, and slf4j works as expected.

All users of slf4j are advised to upgrade to these updated packages, which fix this bug.

7.230. SMARTMONTOOLS

7.230.1. RHBA-2013:0365 — smartmontools bug fix and enhancement update

Updated smartmontools packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The smartmontools packages provide the smartctl tool and the smartd daemon to control and monitor storage systems using the Self-Monitoring, Analysis and Reporting Technology System (SMART) built into most modern ATA and SCSI hard disks.

NOTE

The smartmontools packages have been upgraded to upstream version 5.43, which provides a number of bug fixes and enhancements over the previous version. (BZ#826144)

All users of smartmontools are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.231. SOS

7.231.1. RHBA-2013:0474 — sos bug fix and enhancement update

Updated sos packages that fix a number of bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The sos packages contain a set of tools that gather information from system hardware, logs and configuration files. The information can then be used for diagnostic purposes and debugging.

Bug Fixes

BZ#859142

The previous versions of the sos packages used a built-in module to collect data from Red Hat Network Satellite Server and Red Hat Network Proxy Server. As a consequence, data captured by the **`sos`** utility was incomplete or in a different format than expected by RHN Satellite developers. The module has now been extended to use the RHN Satellite script (**`spacewalk-debug`**) to collect information when present, and the RHN Satellite components now supply a debug script that is able to collect more detailed diagnostic data.

BZ#821323

Previous versions of sos did not include any support for capturing RHUI (Red Hat Update

Infrastructure) configuration and diagnostic data. Consequently, no diagnostic information for the RHUI components was available in generated reports. A new module has been added to capture this information. As a result, full logs and configuration data are now included when run on hosts with RHUI components installed.

BZ#849546

The previous version of **`gluster`** module made use of **`gluster`** CLI commands to obtain state dump information. This caused cluster-wide locks to be taken, potentially blocking other nodes for the duration of data collection. The module has been set to directly issue a signal to the local **`gluster`** processes and collect the generated files. Now, full state dump data is collected without causing side effects to other hosts in the environment.

BZ#850542

Previous versions of the sos **`psacct`** (BSD Process Accounting) module collected all process accounting files present on the system, which could, under certain configurations, lead to a very large number of archived files in the process accounting directory. This has been fixed by changing **`psacct`** collecting only the most recent accounting file by default. The **`all`** option has been added to the module which allows the user to request the original behavior if required. As a result, reports generated on hosts with many archived accounting files no longer include this large set of additional data.

BZ#817093

Previous versions of the device-mapper-multipath packages stored path binding data directly in the **`/etc/`** or **`/var/lib/`** directories. Consequently, the previous versions of sos did not capture files stored in this location. The **`devicemapper`** module has been extended to include the **`/etc/multipath/`** directory contents as well, to allow more consistent SELinux labeling of multipath files. The complete bindings file is now captured on hosts using the new directory layout.

BZ#834594

Prior to this update, the **`sosreport`** networking module collected various data from the **`sysctl`** configuration found in the **`/proc/sys/net/`** directory. Certain legacy paths in this directory have been deprecated upstream and scheduled for removal in future releases but are maintained for compatibility reasons. Nevertheless, running **`sosreport`** on systems having deprecated **`sysctls`** configuration generated warning messages as the **`sos`** utility accessed these paths. This bug has been fixed by including **`sos`** to a blacklist for forbidden paths of this directory. Now, diagnostic information is no longer lost as the content of these files is now provided under different parameter names that are already included in the report. Thus, full diagnostic information is now collected from the **`/proc/sys/net/`** directory without generating unnecessary warning messages in system logs.

BZ#833170

Previously, the **`sosreport`** utility did not recognize interfaces named by BIOS, using the **`biosdevname`** utility. Consequently, Ethernet network devices were constrained to the conventional **`ethN`** naming scheme and the **`ifconfig`** command, in some cases, did not identify correctly interface types. To address this issue, the **`sos`** networking module was set to use the **`ip`** command from the iproute package to generate lists of network interfaces. As a result, information for these network interfaces is now correctly captured and is available in generated reports.

BZ#850433

Prior to this update, the Python runtime's pipe communication interface added an additional trailing newline (“\n”) character to output read by an external program. Consequently, files stored in the reports that were generated by running an external command included additional trailing whitespace that could interfere with attempts to compare file contents. The **sosreport** command has been modified to remove this additional character when present, thus fixing this bug. File capture is now consistent between sos versions in Red Hat Enterprise Linux 5 and 6, thus simplifying comparison of diagnostic data captured on these two releases.

BZ#822174

Previous versions of sos did not sanitize special characters in system hostnames when using the name in file system paths. Consequently, inserting special characters in the system hostname could cause **sos** to generate invalid file system paths and fail to generate a report. With this update, invalid characters are filtered out of system hostnames and the **sosreport** command now works correctly on systems having characters disallowed in file system paths present in the hostname, thus fixing this bug.

BZ#822113

Previous versions of the **sos** utility failed to validate the ***--name*** parameter correctly. Consequently, the report was generated with a file name containing an empty name field. To fix this bug, a default name has been substituted when the provided report name is empty or invalid and files are now generated with names following a consistent pattern.

BZ#824378

Due to changes in the logging design in earlier releases, the **sos** utility did not log errors when attempting to collect output from external commands. Consequently, no message was written to the **sos** log file when an external command could not be executed. This update ensures that the logging is carried out in the **core** plug-in code and a failure to execute an external program is now correctly logged.

BZ#821005

Previous versions of the **sos** utility passed an unescaped double tilde (~~) character sequence to a command executed by the system shell. On some systems, the expansion of this sequence resulted in an error message when the shell home directory expansion attempted a lookup for an account named ~. The sequence is now correctly double-quoted to disable shell expansion of the string and no spurious account lookup or log message is triggered in the described scenario.

BZ#850779

The sanlock package is a new component that provides disk based leases and uses the **watchdog** device to protect their recovery. Previous versions of sos did not include support for collecting **sanlock** diagnostic data. A new module has been added to collect configuration and log files for this component so that diagnostic information relating to the **sanlock** service would be captured in generated reports.

BZ#852049

PostgreSQL is a popular open-source database in Red Hat Enterprise Linux. Prior versions of sos did not include support for collecting information about installed **postgres** instances, and thus no diagnostic information was collected for this component. The **psql** module that obtains information from the database has been included in this release. Now, when **psql** is enabled, diagnostic data is captured on appropriately configured systems, and optional parameters such as database name and authentication may be specified in order to collect more detailed information.

BZ#809727

The **pagetypeinfo** file contains additional information relevant to external fragmentation of kernel memory. Previous versions of sos only collected the related **buddyinfo** data. Consequently, less detailed information was available regarding the fragmentation state of the kernel page allocator. The **pagetypeinfo** file has been included in the generated report and detailed fragmentation debugging data is now collected by default, thus avoiding manual effort to obtain this information.

Enhancements

BZ#840975

Previous releases of sos captured only the **/proc/ioports** file detailing registered I/O port regions in use. The **/proc/iomem** file additionally describes regions of physical system memory and their use of memory, firmware data, and device I/O traffic. As this data may be important in debugging certain hardware and device-driver problems, both **ioports** and **iomem** data have been made available within generated reports.

BZ#825968, BZ#826312

The RHSM (Red Hat Subscription Manager) provides a new method for managing Red Hat subscriptions and entitlements on installed hosts. This update adds support for capturing the **subscription-manager** utility output for diagnostic purposes. The output of **subscription-manager** is now included in generated reports.

Users of sos are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.232. SPICE-GTK

7.232.1. RHBA-2013:0343 — spice-gtk bug fix and enhancement update

Updated spice-gtk packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The spice-gtk packages provide a **GTK2** widget for SPICE clients. Both the **virt-manager** and **virt-viewer** utilities can make use of this widget to access virtual machines using the SPICE protocol.

NOTE

The spice-gtk packages have been upgraded to upstream version 0.14, which provides a number of bug fixes and enhancements over the previous version. The following list includes notable enhancements:

- Windows USB redirection support
- Seamless migration
- Better multi-monitor or resolution setting support
- Improved handling of key-press and key-release events in high latency situations

BZ#842354

Bug Fixes

BZ#834283

When part of a key combination matched the grab sequence, the last key of the combination was sometimes not sent to the guest. As a consequence, the Left Ctrl+Alt+Del key combination was not passed to guests. This update ensures that all the keys are sent to the SPICE server even if they are part of a combination. Now, when a key combination matches the grab sequence, the procedure works as expected.

BZ#813865

Previously, when a Uniform Resource Identifier (URI) contained an IPv6 address, errors occurred when parsing URIs in **remote-viewer**. As a consequence, **remote-viewer** could not be started from the command line with an IPv6 URI. Parsing of URIs containing IPv6 addresses is now fixed and it is possible to connect to an IPv6 address when starting remote-viewer from the command line.

BZ#812347

High network jitter caused some key strokes to enter multiple characters instead of one. Improvements on the SPICE protocol have been made to avoid unwanted character repetition.

BZ#818848

When the **QEMU** application was started with the **`--spice-disable-effects`** option and an invalid value, **spice-gtk** did not print any error message, which could confuse users. This bug is now fixed and **QEMU** exits when an invalid value is encountered.

BZ#881072

Previously, an attempt to close connection to a display failed until one of the remaining windows got resized. Consequently, a previously closed window could be opened again without user's intention. Reopening of the closed display is now fixed and closing the **remote-viewer** windows works as expected.

BZ#835997

Previously, SPICE motion messages were not properly synchronized between client and server after migration. As a consequence, mouse cursor state could get out of sync after migration. This update ensures SPICE motion messages are synchronized between client and server and mouse cursor state no longer gets out of sync.

BZ#846666

Previously, the following error code was returned in various scenarios:

```
main-1:0: SSL_connect: error:00000001:lib(0):func(0):reason(1)
```

This code made debugging of connections failures cumbersome. With this update, the corresponding error message is printed for each of the different scenarios.

BZ#818847

When using the **`--spice-color-value`** option with an invalid value, an error message is displayed. However, previously, the message was not clear enough. After the update, when using the **`--spice-color-value`** option with an invalid value, SPICE returns an error message including a suggestion of the value.

BZ#843134

After connecting to an agent-less guest with 16-bit color depth, the initial screen was black and got drawn on change only. This bug is now fixed and the guest screen is rendered fully upon connection to an agent-less guest with 16-bit color depth.

BZ#867885

Disabling client-side mouse acceleration temporarily when the pointer was in server mode and grabbed caused the mouse pointer to "jump" over the guest desktop at any faster movement. This bug is now fixed and the mouse pointer moves in a guest as supposed in a physical client.

BZ#851090

Previously, the Ctrl+Shift composite key did not work, resulting in the same actions being triggered by different composite keys. This bug is now fixed and Ctrl+Shift works as expected.

BZ#858228

Previously, when no host subject was specified, the **remote-viewer** tool failed to connect with the following error message:

```
Spice-Warning **: ssl_verify.c:484:openssl_verify: ssl: subject ''
verification failed
```

With this update, when no host subject is specified, **remote-viewer** treats it like an empty host subject and verifies a common name **`CN=`** from the subject field with hostname.

BZ#858232

Under certain circumstances, an unclear warning message was returned, incorrectly suggesting that a needless network connection was attempted. The error message has been improved to correctly reflect the state.

BZ#859392

Previously, for security reasons, users were prompted to enter the root password when trying to redirect a USB device from a Red Hat Enterprise Linux 6.4 client to a SPICE guest. However, regular users do not have the root password. As this behavior is controlled by PolicyKit, changes in the ***`/usr/share/polkit-1/actions/org.spice-space.lowlevelusbaccess.policy`*** file have been made to allow access to the raw USB device without prompting for a password. A warning about the security implications of this have been included in the documentation.

BZ#807771

Previously, implementation of the CONTROLLER_SEND_CAD event was missing in the **spice-gtk** controller. As a consequence, checking the box the "Pass Ctrl+Alt+Del to virtual machine box" in the user interface did not produce any result. Implementation for CONTROLLER_SEND_CAD has been added to the underlying source code and users can now tick the checkbox for Ctrl+Alt+Del to be intercepted on the virtual guest.

BZ#861332

After a non-seamless migration of virtual machines with redirected USB devices, SPICE did not evaluate the USB state correctly. With this update, the related functions called from the **`channel_reset()`** function can rely on the state accurately, reflecting the USB state.

BZ#804187

When there was no device to redirect, the redirection dialogue window did not provide clear enough information. With this update, a help message indicating that there is no device to redirect is included in the dialogue window as well as additional related guidance.

BZ#868237

In some situations, SPICE attempted to send the **`00`** scan codes to virtual machines, which resulted in the **`unknown key pressed`** error messages being printed by the client. After this update, SPICE no longer sends the **`00`** scan codes to the **spice-server**.

Enhancements

BZ#846911

The previous SPICE migration pathway was almost equivalent to automatically connecting the client to the migration target and starting the session from scratch. This pathway resulted in unrecoverable data loss, mainly USB, smartcard or copy-paste data that was on its way from the client to the guest and vice versa, when the non-live phase of the migration started. This update prevents data loss and the migration process completes successfully in this scenario.

BZ#842411

RandR multi-monitor support for Linux guests and arbitrary resolution support for Linux and Windows guests have been added to the spice-gtk package. It is now possible to dynamically add new screens while using a virtual machine. Also, after resizing the window of the SPICE client, the resolution of the guest is automatically adjusted to match the size of the window.

BZ#820964

Auto-discovery of already plugged-in USB devices on Red Hat Enterprise Linux clients by the USB Redirector has been added to the spice-gtk package.

BZ#834504

This update adds more informative error messages to the spice-gtk package; the messages deal with host subject mismatch when invalid SSL certificates or SSL options are passed to **QEMU** to the spice-gtk package.

Users of spice-gtk are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.232.2. RHSA-2013:1273 — Important: spice-gtk security update

Updated spice-gtk packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The spice-gtk packages provide a GIMP Toolkit (GTK+) widget for SPICE (Simple Protocol for Independent Computing Environments) clients. Both Virtual Machine Manager and Virtual Machine Viewer can make use of this widget to access virtual machines using the SPICE protocol.

Security Fix

CVE-2013-4324

spice-gtk communicated with PolicyKit for authorization via an API that is vulnerable to a race condition. This could lead to intended PolicyKit authorizations being bypassed. This update modifies spice-gtk to communicate with PolicyKit via a different API that is not vulnerable to the race condition.

All users of spice-gtk are advised to upgrade to these updated packages, which contain a backported patch to correct this issue.

7.233. SPICE-PROTOCOL

7.233.1. RHBA-2013:0510 — spice-protocol bug fix and enhancement update

Updated spice-protocol packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The spice-protocol packages provide header files to describe the SPICE protocol and the QXL para-virtualized graphics card. The SPICE protocol is needed to build newer versions of the spice-client and the spice-server packages.

NOTE

The spice-protocol package has been upgraded to upstream version 0.12.2, which provides a number of enhancements over the previous version, including support for USB redirection. (BZ#842352)

Enhancement

BZ#846910

This update adds support for seamless migration to the spice-protocol packages.

All users who build spice packages are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.234. SPICE-SERVER

7.234.1. RHBA-2013:0529 — spice-server bug fix and enhancement update

Updated spice-server packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol for virtual environments. SPICE users can access a virtualized desktop or server from the local system or any system with network access to the server. SPICE is used in Red Hat Enterprise Linux for viewing virtualized guests running on the Kernel-based Virtual Machine (KVM) hypervisor or on Red Hat Enterprise Virtualization Hypervisors.

NOTE

The spice-server package has been upgraded to upstream version 0.12.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#842353)

Bug Fixes

BZ#787694

Previously, when the "-spice" command line option of the qemu-kvm command contained invalid parameters, the SPICE server terminated unexpectedly. This behavior has been modified, and SPICE server now returns a proper error value when incorrect parameters are passed.

BZ#824384

Previously, resolution changes run in a loop on a guest virtual machine led the qemu-kvm process to fail with the SIGABRT signal. This was caused by calling the ring _remove() function twice by the red_worker script. This bug has been fixed, and qemu-kvm no longer crashes in the described case.

BZ#864982

Previously, non-RGB images with masks were omitted when rendering the guest user interface with the spice-server package. Consequently, certain icons were rendered incorrectly. This bug has been fixed, and the rendering errors no longer occur.

BZ#876685

Using the LZ compression for server self-created images resulted in incorrect stride values, which caused SPICE server to abort. With this update, the LZ compression is no longer used for these images to prevent SPICE server termination.

BZ#881980

Previously, messages from a client to the spice-vdagent agent were received by SPICE server, even after the agent had already disconnected from the server. These messages were mishandled and in certain circumstances could cause SPICE server to terminate unexpectedly. Now, these messages are dropped by the server, thus preventing this bug.

BZ#891326

When trying to change the settings of the "3D Flying Objects" screen saver, SPICE server was forced to access already freed pointers. Consequently, SPICE server terminated unexpectedly with a segmentation fault. With this update, the sequence of operations has been reordered to prevent the segmentation fault.

Enhancements

BZ#836123

With this update, a seamless migration of the SPICE server has been enabled to ensure the full data transfer. This change required modifications in the QUEMU emulator and the libvirt library. The "seamless-migration=on" argument has been added to SPICE's QUEMU arguments. In case this argument is not set, SPICE returns to the old migration pathway.

BZ#842310

This update adds support for multiple monitors and arbitrary screen resolutions.

All users of spice-server are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.234.2. RHSA-2013:1473 — Important: spice-server security update

An updated spice-server package that fixes one security issue is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol for virtual environments. SPICE users can access a virtualized desktop or server from the local system or any system with network access to the server. SPICE is used in Red Hat Enterprise Linux for viewing virtualized guests running on the Kernel-based Virtual Machine (KVM) hypervisor or on Red Hat Enterprise Virtualization Hypervisors.

Security Fix

CVE-2013-4282

A stack-based buffer overflow flaw was found in the way the reds_handle_ticket() function in the spice-server library handled decryption of ticket data provided by the client. A remote user able to initiate a SPICE connection to an application acting as a SPICE server could use this flaw to crash the application.

This issue was discovered by Tomas Jamrisko of Red Hat.

All spice-server users are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

7.235. SPICE-VDAGENT

7.235.1. RHEA-2013:0311 — spice-vdagent enhancement update

Updated spice-vdagent packages that add various enhancements are now available for Red Hat Enterprise Linux 6.

The spice-vdagent packages provide a SPICE agent for Linux guests.

NOTE

The spice-vdagent packages have been upgraded to upstream version 0.12.0, which provides a number of enhancements over the previous version. (BZ#842355)

Enhancements

BZ#747894

The spice-vdagent agent now uses the syslog standard for logging. Syslog provides previously missing information on time stamps and severity marks of the logged events.

BZ#842298

With this update, support for dynamic multiple monitors and arbitrary window resolution has been added to the spice-vdagent agent.

All users of spice-vdagent are advised to upgrade to these updated packages, which add these enhancements.

7.236. SPICE-XPI

7.236.1. RHBA-2013:0459 — spice-xpi bug fix update

Updated spice-xpi packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The spice-xpi packages provide the Simple Protocol for Independent Computing Environments (SPICE) extension for Mozilla that allows the SPICE client to be used from a web browser.

Bug Fixes

BZ#805602

Previously, spice-xpi did not check port validity. Consequently, if an invalid port number was provided, spice-xpi sent it to the client. With this update, spice-xpi checks validity of provided port numbers, warns about invalid ports, and does not run the client if both ports are invalid.

BZ#810583

Previously, the disconnect() function failed to terminate a SPICE client when invoked. The underlying source code has been modified and disconnect() now works as expected in the described scenario.

All users of spice-xpi are advised to upgrade to these updated packages, which fix these bugs.

7.237. SQUID

7.237.1. RHSA-2013:0505 — Moderate: squid security and bug fix update

Updated squid packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Squid is a high-performance proxy caching server for web clients that supports FTP, Gopher, and HTTP data objects.

Security Fixes

CVE-2012-5643

A denial of service flaw was found in the way the Squid Cache Manager processed certain requests. A remote attacker who is able to access the Cache Manager CGI could use this flaw to cause Squid to consume an excessive amount of memory.

Bug Fixes

BZ#805879

Due to a bug in the **ConnStateData::noteMoreBodySpaceAvailable()** function, child processes of Squid terminated upon encountering a failed assertion. An upstream patch has been provided and Squid child processes no longer terminate.

BZ#844723

Due to an upstream patch, which renamed the HTTP header controlling persistent connections from **Proxy-Connection** to **Connection**, the NTLM pass-through authentication does not work, thus preventing login. This update adds the new **http10** option to the **squid.conf** file, which can be used to enable the change in the patch. This option is set to **off** by default. When set to **on**, the NTLM pass-through authentication works properly, thus allowing login attempts to succeed.

BZ#832484

When the IPv6 protocol was disabled and Squid tried to handle an HTTP GET request containing an IPv6 address, the Squid child process terminated due to signal **6**. This bug has been fixed and such requests are now handled as expected.

BZ#847056

The old "stale if hit" logic did not account for cases where the stored stale response became fresh due to a successful re-validation with the origin server. Consequently, incorrect warning messages were returned. Now, Squid no longer marks elements as stale in the described scenario.

BZ#797571

When squid packages were installed before samba-winbind, the **wbpriv** group did not include Squid. Consequently, NTLM authentication calls failed. Now, Squid correctly adds itself into the wbpriv group if samba-winbind is installed before Squid, thus fixing this bug.

BZ#833086

In FIPS mode, Squid was using private MD5 hash functions for user authentication and network access. As MD5 is incompatible with FIPS mode, Squid could fail to start. This update limits the use of the private MD5 functions to local disk file hash identifiers, thus allowing Squid to work in FIPS mode.

BZ#782732

Under the high system load, the squid process could terminate unexpectedly with a segmentation fault during reboot. This update provides better memory handling during reboot, thus fixing this bug.

BZ#798090

Squid incorrectly set the timeout limit for client HTTP connections with the value for server-side connections, which is much higher, thus creating unnecessary delays. With this update, Squid uses a proper value for the client timeout limit.

BZ#861062

When the GET method requested a fully-qualified domain name that did not contain the **AAAA** record, Squid delayed due to long DNS requesting time. This update introduces the **dns_v4_first** option to **squid.conf**. If the **dns_timeout** value of this option is properly set, Squid sends the **A** and **AAAA** queries in parallel and the delays no longer occur.

BZ#758861

Squid did not properly release allocated memory when generating error page contents, which caused memory leaks. Consequently, the Squid proxy server consumed a lot of memory within a short time period. This update fixes this memory leak.

BZ#797884

Squid did not pass the `ident` value to a URL rewriter that was configured using the `url_rewrite_program` directive. Consequently, the URL rewriter received the dash character (`-`) as the user value instead of the correct user name. Now, the URL rewriter receives the correct user name in the described scenario.

BZ#720504

Squid, used as a transparent proxy, can only handle the HTTP protocol. Previously, it was possible to define a URL in which the access protocol contained the asterisk character (`*`) or an unknown protocol namespace URI. Consequently, an `Invalid URL` error message was logged to `access.log` during reload. This update ensures that `http://` is always used in transparent proxy URLs, and the error message is no longer logged in this scenario.

Users of squid are advised to upgrade to these updated packages, which resolve this issue and fix these bugs.

7.238. SSSD

7.238.1. RHSA-2013:0508 — Low: sssd security, bug fix and enhancement update

Updated sssd packages that fix two security issues, multiple bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The System Security Services Daemon (SSSD) provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable back-end system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects such as FreeIPA.

NOTE

The sssd packages have been upgraded to upstream version 1.9.2, which provides a number of bug fixes and enhancements over the previous version. BZ#827606

Security Fixes

CVE-2013-0219

A race condition was found in the way SSSD copied and removed user home directories. A local attacker who is able to write into the home directory of a different user who is being removed could use this flaw to perform symbolic link attacks, possibly allowing them to modify and delete arbitrary files with the privileges of the root user.

CVE-2013-0220

Multiple out-of-bounds memory read flaws were found in the way the autofs and SSH service responders parsed certain SSSD packets. An attacker could spend a specially-crafted packet that, when processed by the autofs or SSH service responders, would cause SSSD to crash. This issue only caused a temporary denial of service, as SSSD was automatically restarted by the monitor process after the crash.

The CVE-2013-0219 and CVE-2013-0220 issues were discovered by Florian Weimer of the Red Hat Product Security Team.

Bug Fixes

BZ#854619

When SSSD was built without sudo support, the ldap_sudo_search_base value was not set and the namingContexts LDAP attribute contained a zero-length string. Consequently, SSSD tried to set ldap_sudo_search_base with this string and failed. Therefore, SSSD was unable to establish a connection with the LDAP server and switched to offline mode. With this update, SSSD considers the zero-length namingContexts value the same way as if no value is available; thus preventing this bug. Note that this issue was primarily affecting Novell eDirectory server users.

BZ#840089

When the ldap_chpass_update_last_change option was enabled, the shadowLastChange attribute contained a number of seconds instead of days. Consequently, when shadowLastChange was in use and the user was prompted to update their expiring password, shadowLastChange was not updated. The user then continued to get an error until they were locked out of the system. With this update, the number of days is stored in shadowLastChange attribute and users are able to change their expiring passwords as expected.

BZ#847039

When the kpasswd server was configured but was unreachable during authentication, SSSD considered it the same way as if the KDC server was unreachable. As a consequence, the user failed to authenticate. Now, SSSD considers an unreachable kpasswd server as a fatal error only when performing a password change and users can log in successfully.

BZ#847043

Previously, canceling a pthread which was in the midst of any SSS client usage could leave the client mutex locked. As a consequence, the next call to any SSS function became unresponsive, waiting for the mutex to unlock. With this update, a more robust mutex is used, and canceling such a pthread no longer keeps the client mutex locked.

BZ#872324

When SSSD created an SELinux login file, it erroneously kept the file descriptor of this file opened. As a consequence, the number of the file descriptors used by SSSD increased every time a user logged in. SSSD now closes the file descriptor when it is no longer needed, thus protecting it from leaking.

BZ#801719

Previously, reverse DNS lookup was not performed to get the Fully Qualified Domain Name (FQDN) of a host specified by an IP address. As a consequence, SSH host public key lookup was incorrectly attempted with the textual IP address as an FQDN. Reverse DNS lookup is now performed to get the FQDN of the host before the SSH host public key lookup. SSH host public key lookup now functions correctly using the FQDN of the host.

BZ#857108

Kerberos options were loaded separately in the krb5 utility and the IPA provider with different code paths. The code was fixed in krb5 but not in the IPA provider. Consequently, a Kerberos ticket was not renewed in time when IPA was used as an authentication provider. With this update, Kerberos options are loaded using a common API and Kerberos tickets are renewed as expected in the described scenario.

BZ#849081

When SSSD was configured to use SSL during communication with an LDAP server and the initialization of SSL failed, SSSD kept the connection to the LDAP server opened. As a consequence, the number of connections to the LDAP server was increased with every request via SSSD, until the LDAP server ran out of available file descriptors. With this update, when the SSL initialization fails, SSSD closes the connection immediately and the number of connections does not grow.

BZ#819057

If the LDAP provider was configured to use GSSAPI authentication but the first configured Kerberos server to authenticate against was offline, then SSSD did not retry the other, possibly working servers. The failover code was amended so that all Kerberos servers are tried when GSSAPI authentication is performed in the LDAP provider. The LDAP provider is now able to authenticate against servers that are only configured as failover.

BZ#822404

Previously, SSSD did not use the correct attribute mapping when a custom schema was used. As a consequence, if the administrator configured SSSD with a custom attribute map, the autofs integration did not work. The attribute mapping was fixed and SSSD now works with a custom attribute schema.

BZ#826192, BZ#827036

In some cases, the SSSD responder processes did not properly close the file descriptors they used to communicate with the client library. As a consequence, the descriptors leaked, and, over time, caused denial of service because SSSD reached the limit of open file descriptors defined in the system. SSSD now proactively closes file descriptors that were not active for some time, making the file descriptor usage consistent.

BZ#829742

The SSSD back-end process kept a pointer to the server it was connected to in all cases, even when the server entry was about to expire. Most customers encountered this issue when SRV resolution was enabled. As a consequence, when the server entry expired while SSSD was using it, the back-end process crashed. An additional check has been added to SSSD to ensure the server object is valid before using it. SSSD no longer crashes when using SRV discovery.

BZ#829740

When the SSSD daemon was in the process of starting, the parent processes quit right after spawning the child process. As a consequence, the init script printed [OK] after the parent process terminated, which was before SSSD was actually functional. After this update, the parent processes are not terminated until all worker processes are up. Now, the administrator can start using SSSD after the init script prints [OK].

BZ#836555

Previously, SSSD always treated the values of attributes that configure the "shadow" LDAP password policy as absolute. As a consequence, an administrator could not configure properties of the "shadow" LDAP password policy as "valid forever". The LDAP "shadow" password attributes are now extended to also allow "-1" as a valid value and an administrator can use the reserved value of "-1" as a "valid forever".

BZ#842753

When a service with a protocol was requested from SSSD, SSSD performed access to an unallocated memory space, which caused it to occasionally crash during service lookup. Now, SSSD does not access unallocated memory and no longer crashes during service lookups.

BZ#842842

When the LDAP user record contained an empty attribute, the user was not stored correctly in the SSSD cache. As a consequence, the user and group memberships were missing. After this update, empty attributes are not considered an error and the user is stored correctly in the SSSD cache. As a result, the user is present and the group membership can be successfully evaluated.

BZ#845251

When multiple servers were configured and SSSD was unable to resolve the host name of a server, it did not try the next server in the list. As a consequence, SSSD went offline even when a working server was present in the configuration file after the one with the unresolvable hostname. SSSD now tries the next server in the list and failover works as expected.

BZ#847332

Previously, the description of ldap_*_search_base options in the sssd-ldap(5) man page was missing syntax details for these options which made it unclear how the search base should be specified. The description of ldap_*_search_base options in sssd-ldap(5) man page has been amended so that the format of the search base is now clear.

BZ#811984

If the krb5_canonicalize option was set to True or not present at all in the /etc/sssd/sssd.conf file, the client principal could change as a result of the canonicalization. However, SSSD still saved the original principal. As the incorrect principal was saved, the GSSAPI authentication failed. The Kerberos helper process that saves the principals was amended so that the canonicalized principal is saved if canonicalization is enabled. The GSSAPI binds now work correctly even for cases where the principal is changed as a result of the canonicalization.

BZ#886038

Previously, SSSD kept the file descriptors to the log files open. Consequently on occasions like moving the actual log file and restarting the back end, SSSD still kept the file descriptors open. After this update, SSSD closes the file descriptor after child process execution. As a result, after successful start of the back end, the file descriptor to log files is closed.

BZ#802718

Previously, the proxy domain type of SSSD allowed looking up a user only by its "primary name" in the LDAP server. If SSSD was configured with a "proxy domain" and the LDAP entry contained more name attributes, only the primary one could be used for lookups. For this update, the proxy provider was enhanced to also handle aliases in addition to primary user names. An administrator can now look up a user by any of his names when using the proxy provider.

BZ#869013

The sudo "smart refresh" operation was not performed if the LDAP server did not contain any rule when SSSD was started. As a consequence, newly created sudo rules were found after a longer period of time than the "ldap_sudo_smart_refresh_interval" option displayed. The sudo "smart refresh" operation is now performed and newly created sudo rules are found within the ldap_sudo_smart_refresh_interval time span.

BZ#790090

The SSSD "local" domain (id_provider=local) performed a bad check on the validity of the access_provider value. If the access_provider option was set with "permit", which is a correct value, SSSD failed with an error. The check for the access_provider option value has been corrected and SSSD now allows the correct access_provider value for domains with id_provider=local.

BZ#874579

Previously, SELinux usermap contexts were not ordered correctly if the SELinux mappings were using HBAC rules as a definition of what users to apply the mapping to and if the Identity Management server was not reachable at the same time. As a consequence, an invalid SELinux context could be assigned to a user. SELinux usermap contexts are now ordered correctly, and the SELinux context is assigned to a user successfully.

BZ#700805

If SSSD was configured to locate servers using SRV queries, but the default DNS domain was not configured, SSSD printed a DEBUG message. The DEBUG message, which contained an "unknown domain" string, could confuse the user. The DEBUG messages were fixed so that they specifically report that the DNS domain is being looked up, and only print known domains.

BZ#871424

Previously, the chpass_provider directive was missing in the SSSD authconfig API. As a consequence, the authconfig utility was unable to configure SSSD if the chpass_provider option was present in the SSSD configuration file. The chpass_provider option has been included in the SSSD authconfig API and now the authconfig utility does not consider this option to be incorrect.

BZ#874618

Previously, the sss_cache tool did not accept fully qualified domain names (FQDN). As a consequence, the administrator was unable to force the expiration of a user record in the SSSD cache with a FQDN. The sss_cache tool now accepts an FQDN and the administrator is able to force the expiration of a user record in the SSSD cache with an FQDN.

BZ#870039

Previously, when the sss_cache tool was run after an SSSD downgrade, the cache file remained the same as the one used for the previous version of SSSD. The sss_cache tool could not manipulate the cache file and a confusing error message was printed. The "invalid database version" error message was improved in the sss_cache tool. Now, when an invalid cache version is detected, the sss_cache tool prints a suggested solution.

BZ#882923

When the proxy provider did not succeed in finding a requested user, the result of the search was not stored in the negative cache (which stores entries that are not found when searched for). A subsequent request for the same user was not answered by the negative cache, but was rather looked up again from the remote server. This bug had a performance impact. The internal error codes were fixed, allowing SSSD to store search results that yielded no entries into the negative cache. Subsequent lookups for non-existent entries are answered from the negative cache and, by effect, are very fast.

BZ#884600

Previously, during LDAP authentication, SSSD attempted to contact all of the servers on the server list if every previous server failed. However, SSSD tried to connect to the next server only if the current connection timed out. SSSD now tries to contact the next server on any error and connection attempts work as expected.

BZ#861075

When the sssd_be process was forcefully terminated, the SSSD responder processes failed to reconnect if the attempt was performed before the sssd_be process was ready. This caused the responder to be restarted. Occasionally, the responder restarted several times before sssd_be was ready, hitting the maximum number of restarts threshold, after which it was terminated completely. As a consequence, the SSSD responder was not gracefully restarted. After this update, each restart of the SSSD responder process is done with an increasing delay, so that the sssd_be process has enough time to recover before a responder is restarted.

BZ#858345

Previously, the sssd_pam responder was not properly configured to recover from a back end disconnection. The PAM requests that were pending before the disconnection were not canceled. Thus, new requests for the same user were erroneously detected as similar requests and piled up on top of the previous ones. This caused the PAM operation to time out with the following error:

```
Connection to SSSD failed: Timer Expired
```

As a consequence, the user could not log in. After this update, pending requests are canceled after disconnection and the user is able to log in when the pam responder reconnects.

BZ#873032

Previously, the sss_cache utility was not included in the main SSSD package and users were unaware of it, unless they installed the sssd-tools package. After this update, the sss_cache utility has been moved to the sssd package.

BZ#872683

When the anonymous bind was disabled and enumeration was enabled, SSSD touched an invalid array element during enumeration because the array was not NULL terminated. This caused the sssd_be process to crash. The array is now NULL terminated and the sssd_be process does not crash during enumeration when the anonymous bind is disabled.

BZ#870505

When SSSD was configured with multiple domains, the sss_cache tool searched for an object only in the first configured domain and ignored the others. As a consequence, the administrator could not use the sss_cache utility on objects from an arbitrary domain. The sss_cache tool now searches all domains and the administrator can use the tool on objects from an arbitrary domain.

Enhancements

BZ#768168, BZ#832120, BZ#743505

A new ID mapping library that is capable of automatically generating UNIX IDs from Windows Security Identifiers (SIDs) has been added to SSSD. An administrator is now able to use Windows accounts easily in a UNIX environment. Also, a new Active Directory provider that contains the attribute mappings tailored specifically for use with Active Directory has been added to SSSD. When id_provider=ad is configured, the configuration no longer requires setting the attribute mappings manually. A new provider for SSSD has been implemented and the administrator can now set up an Active Directory client without having to know the specific Active Directory attribute mappings. The performance of the Active Directory provider is better than the performance of the LDAP provider, especially during login.

BZ#789470

When SSSD failed over to another server in its failover list, it stuck with that server as long as it worked. As a result, if the SSSD failed over to a server in another region, it did not reconnect to a closer server until it was restarted or until the backup server stopped working. The concept of a "backup server" has been introduced to SSSD and if SSSD fails over to a server which is listed as a backup server in the configuration, it periodically tries to reconnect to one of the primary servers.

BZ#789473

A new sss_seed utility has been introduced in SSSD. An administrator can save a pre-seeded user entry into the SSSD cache which is used until the user can actually refresh the entry with a non-pre-seeded entry from the directory.

BZ#768165

Active Directory uses a nonstandard format when a large group that does not fit into a single "page" is returned. By default, the single page size contains 1500 members and if the response exceeds the page size, the range extension is used. If a group was stored on an Active Directory server which contained more than 1500 members, the response from Active Directory contained the proprietary format which SSSD could not parse. SSSD was improved so that it is able to parse the range extension and can now process groups with more than 1500 group members coming from the Active Directory.

BZ#766000

Previously, administrators were forced to distribute SELinux mappings via means that were error prone. Therefore, a centralized store of SELinux mappings was introduced to define which user gets which context after logging into a certain machine. SSSD is able to read mappings from an Identity Management server, process them according to a defined algorithm and select the appropriate SELinux context which is later consumed by the pam_selinux module. The Identity Management server administrator is now able to centrally define SELinux context mappings and the Identity Management clients process the mappings when a user logs in using his Identity Management credentials.

BZ#813327

The automounter can be configured to read autofs maps from a centralized server such as an LDAP server. But when the network is down or the server is not reachable, the automounter is unable to serve maps. A new responder has been introduced to SSSD that is able to communicate with the automounter daemon. Automounter can now request the maps via SSSD instead of going directly to the server. As a result, the automounter is able to serve maps even in case of an outage of the LDAP server.

BZ#761573

A new sudo responder has been implemented in SSSD as well as a client library in sudo itself. SSSD is able to act as a transparent proxy for serving sudo rules for the sudo binary. Now, when the centralized sudo rules source is not available, for instance when the network is down, SSSD is able to fall back to cached rules, providing transparent access to sudo rules from a centralized database.

BZ#789507

Prior to this update, even if a user entry was cached by SSSD, it had to be read from the cache file on the disk. This caused the cache readings to be slow in some performance-critical environments. A new layer of cache, stored in the memory was introduced, greatly improving the performance of returning cached entries.

BZ#771412

The pam_pwd_expiration_warning option can be used to limit the number of days a password expiration warning is shown for. However, SSSD did not allow to unconditionally pass any password warning coming from the server to the client. The behavior of pam_pwd_expiration_warning was modified so that if the option is set to 0, it is always passed on to the client, regardless of the value of the warning. As a result, after setting the pam_pwd_expiration_warning option to 0, the administrator will always see the expiration warning if the server sends one.

BZ#771975

The force_timeout option has been made configurable and the administrator can now change the force_timeout option for environments where SSSD subprocesses might be unresponsive for some time.

All users of sssd are advised to upgrade to these updated packages, which correct these issues, fix these bugs and add these enhancements.

7.239. STRACE

7.239.1. RHBA-2013:0282 — strace bug fix and enhancement update

Updated strace packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The strace packages provide a utility to intercept and record the system calls called and received by a running process. The strace utility can print a record of each system call, its arguments and its return value. The strace utility is useful for diagnosing, debugging and instructional purposes.

Bug Fixes

BZ#759569

Prior to this update, the strace utility extracted arguments for the "semtimedop" system call from the wrong location on the IBM System z platforms. As a consequence, arguments for the "semtimedop" system call were incorrectly displayed. This update modifies strace to extract the arguments from the correct memory location so that the arguments for the "semtimedop" system call are displayed as expected.

BZ#837183

Prior to this update, the strace utility used special breakpoints to trace fork/vfork/clone system calls. As a consequence, sometimes strace could cause applications to crash when following fork/vfork/clone system calls. This update modifies strace to use PTRACE_SETOPTIONS to set the behavior at fork/vfork/clone system calls and applications no longer crash.

Enhancement

BZ#809917

Prior to this update, strace incorrectly decoded system calls when tracing a 32-bit process on a 64-bit machine, because strace on IBM System z platforms is not multi-arch aware. This update provides an additional strace executable (strace32) which can be used to trace 32-bit processes on 64-bit machines.

All users of strace are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.240. SUBSCRIPTION-MANAGER-MIGRATION-DATA

7.240.1. RHBA-2013:0360 — subscription-manager-migration-data bug fix and enhancement update

An updated subscription-manager-migration-data package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The new Subscription Management tooling allows users to understand the specific products, which have been installed on their machines, and the specific subscriptions, which their machines consume.

NOTE

The subscription-manager-migration-data package has been upgraded to upstream version 1.12.2.5, which provides a number of bug fixes and new product certificates over the previous version. (BZ#860304, BZ#825603, BZ#872959, BZ#875760)

All users of subscription-manager-migration-data are advised to upgrade to this updated package, which fixes these bugs adds these enhancements.

7.241. SUBSCRIPTION-MANAGER

7.241.1. RHBA-2013:0350 — subscription-manager bug fix and enhancement update

Updated subscription-manager packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The subscription-manager packages provide programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat Entitlement platform.

NOTE

The subscription-manager packages have been upgraded to upstream version 1.1.15, which provides a number of bug fixes and enhancements over the previous version. (BZ#860291)

Bug Fixes

BZ#785265

The dbus packages, which contain the D-BUS communication system, are not included in the minimal installation of Red Hat Enterprise Linux. However, the subscription-manager utility depends on dbus, which could previously cause subscription-manager to terminate unexpectedly with a traceback during the registration process. The system was registered successfully but the rhsmcertd daemon was not able to communicate with subscription manager servers, such as candlepin, Subscription Asset Manager, or katello. With this update, subscription-manager exits without a traceback when dbus is not present on the system. To ensure proper communication with the subscription manager servers, install dbus manually by running "yum install dbus".

BZ#865954

Due to an incorrect error handling of invalid system names, the system could be left in unusable state during the first boot process. The handling of invalid system names has been fixed and first boot proceeds properly as expected.

Enhancements

BZ#874749

With this update, the subscribe-manager "unsubscribe" command has been renamed to "remove".

BZ#874776, BZ#874804

With this update, the subscribe-manager "subscribe" command has been renamed to "attach". This change includes also the references to the "subscribe" command, such as "--auto-subscribe", which has been renamed to "--auto-attach".

All users of subscription-manager are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.242. SUDO

7.242.1. RHBA-2013:0363 — sudo bug fix and enhancement update

Updated sudo packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The **sudo** (super user do) utility allows system administrators to give certain users the ability to run commands as root.

NOTE

The sudo package has been upgraded to upstream version 1.8.6p3, which provides a number of bug fixes and enhancements over the previous version. The following list includes highlights, important fixes, or notable enhancements:

- Plug-in API has been added, provided by the new sudo-devel subpackage.
- New **`/etc/sudo.conf`** configuration file for the **sudo** utility front-end configuration (plug-in path, coredumps, debugging and so on) has been added.
- It is possible to specify the sudoer's path, UID, GID, and file mode as options to the plug-in in the **`/etc/sudo.conf`** file.
- Support for using the System Security Services Daemon (SSSD) as a source of sudoers data has been provided.
- The **`-D`** flag in the **sudo** utility has been replaced with a more general debugging framework that is configured in the **`/etc/sudo.conf`** file.
- The deprecated **`noexec_file`** sudoers option is no longer supported.
- The **`noexec`** functionality has been moved out of the sudoers policy plug-in and into the **sudo** utility front end, which matches the behavior documented in the plug-in writer's guide. As a result, the path to the **`/user/libexec/sudo_noexec.so`** file is now specified in the **`/etc/sudo.conf`** file instead of the **`/etc/sudoers`** file.
- If the user fails to authenticate, and the user's executed command is rejected by the rules defined in the **`sudoers`** file, the **`command now allowed`** error message is now logged instead of the previously used **`<N> incorrect password attempts`**. Likewise, the **`mail_no_perms sudoers`** option now takes precedence over the **`mail_badpass`** option.
- If the user is a member of the exempt group in the **`sudoers`** file, he will no longer be prompted for a password even if the **`-k`** option is specified with the executed command. This makes the **`sudo -k`** command consistent with the behavior one would get if running the **`sudo -k`** command immediately before executing another command.
- If the user specifies a group via the **sudo** utility's **`-g`** option that matches the target user's group in the password database, it is now allowed even if no groups are present in the **`Runas_Spec`**.
- A group ID (**`%#gid`**) can now be specified in the **`User_List`** or **`Runas_List`** files. Likewise, for non-Unix groups the syntax is **`%:#gid`**.
- The **visudo** utility now fixes the mode on the sudoers file even if no changes are made, unless the **`-f`** option is specified.

(BZ#759480)

Bug fixes

BZ#823993

The controlling **tty** of a suspended process was not saved by the **sudo** utility. Thus, the code handling the resume operation could not restore it correctly. Consequently, resume was not enabled to a suspended process run through the **sudo** utility. This bug has been fixed by rebasing to a new upstream version. As a result, suspending and resuming works correctly again.

BZ#840980

A change in the internal execution method of commands in the **sudo** utility was the cause of creating a new process and executing the command from there. To fix this bug, new **defaults** option was added to restore the old behavior. Since the execution method has been implemented to correctly handle PAM session handling, I/O logging, SELinux support, and the plug-in policy close functionality, these features do not work correctly if the newly-implemented option is used. To apply this option, add the following line to the **/etc/sudoers** file:

```
Defaults cmnd_no_wait
```

As a result, if the newly-implemented option is used, commands will be executed directly by the **sudo** utility.

BZ#836242

The **sudo** utility set the core dump size limit to 0 to prevent the possibility of exposing the user password in the core dump file in case of an unexpected termination. However, this limit was not reset to the previous state before executing a command and the core dump size hard limit of a child process was eventually set to 0. Consequently, it was not possible to set the core dump size limit by processes run through the **sudo** utility. This bug was fixed by rebasing to a new upstream version; thus, setting the core dump size limit by processes run through the **sudo** utility works as expected.

BZ#804123

When initializing the global variable holding the PAM (Pluggable Authentication Modules) handle from a child process, which had a separate address space, a different PAM handle was passed to PAM API functions where the same handle was supposed to be used. Thus, the initialization had no effect on the parent's PAM handle when the **pam_end_sessions()** function was called. As a consequence, dependent modules could fail to iniciate at session close in order to release resources or make important administrative changes. This bug has been fixed by rebasing to a newer upstream version, which uses the PAM API correctly (for example, initializes one PAM handle and uses it in all related PAM API function calls). As a result, PAM sessions are now closed correctly.

BZ#860397

Incorrect file permissions on the **/etc/sudo-ldap.conf** file and missing examples in the same file led to an inconsistency with documentation provided by Red Hat. With this update, file permissions have been corrected and example configuration lines have been added. As a result, **/etc/sudo-ldap.conf** is now consistent with the documentation.

BZ#844691

When the **sudo** utility set up the environment in which it ran a command, it reset the value of the **RLIMIT_NPROC** resource limit to the parents value of this limit if both the soft (current) and hard (maximum) values of **RLIMIT_NPROC** were not limited. An upstream patch has been provided to address this bug and **RLIMIT_NPROC** can now be set to "unlimited".

BZ#879675

Due to different parsing rules for comments in the **/etc/ldap.conf** file, the hash ('#') character could not be used as part of a configuration value, for example in a password. It was understood as a beginning of a comment and everything following the # character was ignored. Now, the parser has been fixed to interpret the # character as a beginning of a comment only if it is at the beginning of a line. As a result, the '#' character can be used as part of a password, or any other value if needed.

BZ#872740

White space characters included in command arguments were not escaped before being passed to the specified command. As a consequence, incorrect arguments were passed to the specified command. This bug was fixed by rebasing to a new upstream version where the escape of command arguments is performed correctly. As a result, command arguments specified on the command line are passed to the command as expected.

Enhancements

BZ#789937

The **sudo** utility is able to consult the `/etc/nsswitch.conf` file for sudoers entries and look them up in files or via LDAP (Lightweight Directory Access Protocol). Previously, when a match was found in the first database of sudoers entries, the look-up operation still continued in other databases. In Red Hat Enterprise Linux 6.4, an option has been added to the `/etc/nsswitch.conf` file that allows users to specify a database after which a match of the sudoer's entry is sufficient. This eliminates the need to query any other databases; thus improving the performance of sudoer's entry look up in large environments. This behavior is not enabled by default and must be configured by adding the `[SUCCESS=return]` string after a selected database. When a match is found in a database that directly precedes this string, no other databases are queried.

BZ#846117

This update improves sudo documentation in the section describing wildcard usage, describing what unintended consequences a wildcard character used in the command argument can have.

Users of sudo should upgrade to these updated packages, which fix these bugs and add these enhancements.

7.243. SYSFSUTILS

7.243.1. RHBA-2012:1453 — sysfsutils bug fix update

Updated sysfsutils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The sysfsutils packages provide a suite of daemons to manage access to remote directories and authentication mechanisms. The sysfsutils suite provides an NSS and PAM interface toward the system and a pluggable backend system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.

Bug Fix

BZ#671554

Prior to this update, sysfs directories were not closed as expected. As a consequence, the libsysfs library could leak memory in long running programs that frequently opened and closed sysfs directories. This update modifies the underlying code to close sysfs directories as expected.

All users of sysfsutils are advised to upgrade to these updated packages, which fix this bug.

7.244. SYSLINUX

7.244.1. RHBA-2013:0473 — syslinux bug fix update

Updated syslinux packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The syslinux utility is responsible for booting the operating system kernel.

Bug Fix

BZ#812034

A Coverity test revealed several static overruns in the creation of "hybrid" ISO images, which could lead to incorrect images being created. This bug has been fixed to correctly produce "hybrid" ISO images.

All users of syslinux are advised to upgrade to these updated packages, which fix this bug.

7.245. SYSTEM-CONFIG-KDUMP

7.245.1. RHBA-2013:0292 — system-config-kdump bug fix and enhancement update

Updated system-config-kdump packages that fix three bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The system-config-kdump packages provide a graphical tool to configure kernel crash dumping via kdump and kexec.

Bug Fixes

BZ#811104

An attempt to use system-config-kdump on the IBM System z machines caused an error message to appear. As a consequence, users were unable to choose the specific kernel. This bug has been fixed and the user can choose the required kernel in this situation.

BZ#829386

On IBM PowerPC computers, the system-config-kdump tool used the first crashkernel parameter instead of the last one and a traceback was returned when crashkernel value was set to "auto". With this update, system-config-kdump uses the last crashkernel parameter and allows this parameter to be set to "auto". As a result, tracebacks are no longer returned in the described scenario.

BZ#858280

Because some actions take longer time to finish, and the return timeout value was set too low, the front end did not receive an answer in an appropriate time, and displayed an error message. The return timeout has been set to 5 minutes and system-config-kdump works as expected now.

Enhancement

BZ#852766

This enhancements adds support for firmware-assisted dump (fadump) for IBM PowerPC computers. The user is now also allowed to choose between kdump and fadump.

All users of system-config-kdump are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.246. SYSTEM-CONFIG-KICKSTART

7.246.1. RHEA-2013:0470 — system-config-kickstart enhancement update

An updated system-config-kickstart package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

The system-config-kickstart package contains Kickstart Configurator, a graphical tool for creating kickstart files.

Enhancement

BZ#819813

This update contains a complete Assamese translation of the system-config-kickstart package.

Users requiring Assamese translation of system-config-kickstart are advised to upgrade to this updated package, which adds this enhancement.

7.247. SYSTEM-CONFIG-LANGUAGE

7.247.1. RHBA-2012:1213 — system-config-language bug fix update

An updated system-config-language package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The system-config-language is a graphical user interface that allows the user to change the default language of the system.

Bug Fix

BZ#819811

When using system-config-language in a non-English locale, some of the messages in the GUI were not translated. Consequently, non-English users were presented with untranslated messages. With this update, all message strings have been translated.

All users of system-config-language are advised to upgrade to this updated package, which fixes this bug.

7.248. SYSTEM-CONFIG-LVM

7.248.1. RHBA-2013:0385 — system-config-lvm bug fix update

Updated system-config-lvm packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The system-config-lvm packages contain a utility for configuring logical volumes (LVs) using a graphical user interface.

Bug Fixes

BZ#852864

When there was a RAID1 mirrored volume created using the lvm utility, system-config-lvm did not start correctly. The underlying source code has been modified to prevent system-config-lvm from terminating unexpectedly. The RAID1 volumes are now shown properly, however, they are visible as its underlying logical volumes.

BZ#820539

During an attempt to work with a mirror log, the system-config-lvm utility failed on start. This bug has been fixed and mirrored volumes are now supported as expected.

BZ#840070

Due to a bug in the best_fit() function, which tried to fit all existing logical volumes (LVs) into the display area, system-config-lvm did not start correctly on systems with large amount of existing LVs. This bug has been fixed and system-config-lvm is fully functional even on systems with more then 350 LVs.

All users of system-config-lvm are advised to upgrade to these updated packages, which fix these bugs.

7.249. SYSTEM-CONFIG-USERS

7.249.1. RHBA-2012:1387 — system-config-users bug fix update

Updated system-config-users packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

The system-config-users packages provide a graphical utility for administrating users and groups.

Bug Fixes

BZ#736037

Prior to this update, expiration dates at or before January 1, 1970 were not correctly calculated. As a consequence, the system-config-users utility stored expiration dates off by one day into /etc/shadow. This update modifies the underlying code so that account expiration dates are calculated and stored correctly.

BZ#801652

Prior to this update, a string in the user interface was not correctly localized into Japanese. This update modifies the string so that the text is now correct.

BZ#841886

Prior to this update, the system-config-users utility determined incorrectly whether to set an account as inactive if an expired password was not reset during a specified period. This update modifies the underlying code to check for this condition by hard-coding the value which indicates this condition.

All users of system-config-users are advised to upgrade to these updated packages, which fix these bugs.

7.250. SYSTEMTAP

7.250.1. RHBA-2013:0345 — systemtap bug fix and enhancement update

Updated systemtap packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

SystemTap is a tracing and probing tool to analyze and monitor activities of the operating system, including the kernel. It provides a wide range of filtering and analysis options.

NOTE

The systemtap packages have been upgraded to upstream version 1.8, which provides a number of bug fixes and enhancements over the previous version. (BZ#843123)

Bug Fixes

BZ#746334

Many of the SystemTap examples for memory used tracepoints which did not exist in some versions of kernel. Consequently, if the user tried to run the mmanonpage.stp, mmfilepage.stp, or mmwriteback.stp files, this process failed. The examples have been updated to work with the memory tracepoints available in Red Hat Enterprise Linux 6 and SystemTap now works as expected.

BZ#822503

Previously, support for the IPv6 protocol was missing. Consequently, an attempt to execute a script that evaluates a tapset variable containing an IPv6 address, or call a tapset function returning an IPv6 address was unsuccessful, and the address field was filled with the "Unsupported Address Family" message instead of a valid IPv6 address. This update adds the support for the IPv6 protocol.

BZ#824311

Previously, changes in the include/trace/events/sunrpc.h file were referenced, but were not defined by the #include directive. As a consequence, the rpc tracepoint was missing. This tracepoint has been defined using #include and SystemTap works correctly in this situation.

BZ#828103

In previous kernels and versions of SystemTap, the nfsd.open probe-alias in the nfsd tapset referred to the "access" parameter, which was later renamed to "may_flags" in the kernel. Consequently, the semantic errors occurred and then the stap command failed to execute. This update allows the nfsd.open probe-alias check under both names for setting the "access" script-level variable, and stap now works as expected in the described scenario.

BZ#884951

Recent kernel updates required updates to some of the NFS tapset definitions to find certain context variables. With this update, the tapset aliases now search both old and new locations.

All users of systemtap are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.251. TAR

7.251.1. RHBA-2012:1372 — tar bug fix update

Updated tar packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The tar packages provide the GNU tar program. Gnu tar can allows to save multiple files in one archive and can restore the files from that archive. This update fixes the following bug:

BZ#841308

Prior to this update, tar failed to match and extract given file names from an archive when this archive was created with the options "--sparse" and "--posix". This update modifies the underlying code to match and extract the given name as expected.

All users of tar are advised to upgrade to these updated packages, which fix this bug.

7.251.2. RHBA-2013:0489 — tar bug fix update

Updated tar packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The tar packages provide the GNU tar utility, which allows the user to save multiple files in one archive and can restore the files from that archive.

Bug Fixes

BZ#875727

When the "--strip-components" command-line parameter was used, the tar utility was unable to correctly match a file name that had to be extracted and the action failed. This bug has been fixed and tar now matches file names as expected in the described scenario.

BZ#877769

When the "--listed-incremental" command-line parameter was used and a file was specified multiple times, tar terminated unexpectedly with a segmentation fault. The underlying source code has been modified and tar no longer crashes under these circumstances.

All users of tar are advised to upgrade to these updated packages, which fix these bugs.

7.252. TBOOT

7.252.1. RHBA-2013:0524 — tboot bug fix update

Updated tboot packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The tboot packages provide the Trusted Boot (tboot) open source pre-kernel/VMM module. This module uses Intel Trusted Execution Technology (Intel TXT) to initialize the launch of operating system kernels and virtual machines.

Bug Fixes

BZ#885684

Due to an error in the underlying source code, a buffer overflow could occur and an attempt to boot the kernel with tboot enabled could fail with the following error:

Kernel panic - not syncing: Too many boot init vars at `numbers,'

This update applies an upstream patch that corrects this error, and the kernel now boots as expected.

BZ#834323

Prior to this update, the installed README file incorrectly identified the supported kernels. This update corrects this file and ensures that it no longer contains incorrect information.

All users of tboot are advised to upgrade to these updated packages, which fix these bugs.

7.253. TCSH

7.253.1. RHBA-2013:0446 — tcsh bug fix update

Updated tcsh packages that fix multiple bugs are now available for Red Hat Enterprise Linux 6.

The tcsh packages provide an enhanced and compatible version of the C shell (csh) command language interpreter, which can be used as an interactive login shell, as well as a shell script command processor.

Bug Fixes

BZ#769157

Prior to this update, the tcsh command language interpreter could run out of memory because of random "sbrk()" failures in the internal "malloc()" function. As a consequence, tcsh could abort with a segmentation fault. This update uses "system malloc" instead and tcsh no longer aborts.

BZ#814069

Prior to this update, aliases were inserted into the history buffer when saving the history in loops if the alias included a statement that did not work in the loop. This update no longer allows to save the history in loops. Now, only the first line of loops and the "if" statement are saved in the history. Aliases now work as expected.

BZ#821796

Prior to this update, casting was removed when calling a function in the history file locking patch. As a consequence, multibyte tests failed. This update reverts the status before the patch and tests no longer fail.

BZ#847102

Prior to this update, the tcsh logic did not handle file sourcing as expected. As a consequence, source commands failed when using a single-line "if" statement. This update modifies the underlying code to handle source commands as expected.

BZ#884937

Prior to this update, the SIGINT signal was not blocked when the tcsh command language interpreter waited for the child process to finish. As a consequence, tcsh could be aborted with the key combination Ctrl+c. This update blocks the SIGINT signal and tcsh is no longer aborted.

All users of tcsh are advised to upgrade to these updated packages, which fix these bugs.

7.254. TIGERVNC

7.254.1. RHBA-2013:0478 — tigervnc bug fix and enhancement update

Updated tigervnc packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

Virtual Network Computing (VNC) is a remote display system which allows you to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. This package contains a client which will allow you to connect to other desktops running a VNC server.

Bug Fixes

BZ#688624

When the Xvnc server was started by the vncserver init script, but no password file existed, the initscript failed without displaying a message. This bug is now fixed and the "VNC password for user is not configured" message appears when the password is not configured for the Xvnc session.

BZ#843714

Previously, the user was not allowed to change the value of the AcceptPointerEvents parameter while Xvnc was running. As a consequence, when the "vncconfig -set AcceptPointerEvents=1" command was used to enable and "vncconfig -set AcceptPointerEvents=0", to disable mouse input for VNC session, it failed with an error message, similar to the following:

Setting param AcceptPointerEvents=0 failed

Now the user is allowed to change the value of the AcceptPointerEvents parameter and the mouse input for a VNC session can be enabled or disabled while Xvnc is running.

Enhancement

BZ#844486

The tigervnc packages have been updated to match the latest X server version.

Users of tigervnc are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.255. TOG-PEGASUS

7.255.1. RHBA-2013:0418 — tog-pegasus bug fix and enhancement update

Updated tog-pegasus packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

OpenPegasus Web-Based Enterprise Management (WBEM) Services for Linux enables management solutions that deliver increased control of enterprise resources. WBEM is a platform and resource independent of Distributed Management Task Force (DMTF) standard that defines a common information model and communication protocol for monitoring and controlling resources from diverse sources.

NOTE

The tog-pegasus package has been upgraded to upstream version 2.12.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#739118, BZ#825471)

Bug Fixes

BZ#812892

Previously, non-array properties of CMPI instances were not checked for NULL values in the cimserver daemon (OpenPegasus CIM server). This led to an unexpected termination of cimserver. This update provides an upstream patch for cimserver. Now, cimserver correctly returns instances with non-array properties including those containing NULL values.

BZ#869664

Prior to this update, all connections to cimserver were considered local host. Consequently, cimsever could not discern between local and remote connections and between granted and denied access. A patch has been provided to fix this bug. Now, cimserver is again capable of recognizing whether, firstly, connections are local or remote and, secondly, whether the access per user will be granted or denied.

Enhancement

BZ#716474

The cimserver daemon uses all of well-known ports based on CIM/WBEM technology for network communication. This update provides the user with an option to configure, which interfaces have to be used and to restrict cimserver to listen only on selected network interfaces.

Users of tog-pegasus are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.256. TOMCAT6

7.256.1. RHBA-2013:0480 — tomcat6 bug fix update

Updated tomcat6 packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The tomcat6 packages provide Apache Tomcat 6, which is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

Bug Fixes

BZ#576540

On Red Hat Enterprise Linux, Apache Tomcat initscripts should be located in the /etc/rc.d/init.d directory. However, the comman initscript was previously located in the /etc/init.d directory due to a mistake in the package specs file. With this update, the specs file has been updated and the conman script is located in the /etc/rc.d/init.d directory along with other initscripts as expected.

BZ#847288

When a web application used its own class loader, a deadlock in Tomcat WebappClassLoader could occur when compiling JSPs due to a synchronization bug. This update fixes the synchronization bug and external class loaders no longer interfere with WebappClassLoader.

BZ#798617

The service status returned an incorrect tomcat6 status when TOMCAT_USER in the /etc/tomcat6/tomcat6.conf file was changed to a user whose UID differed from the user GID due to incorrect logic in retrieving the process details. With this update, the code has been modified and the correct service status is now returned in this scenario.

BZ#785954

When Tomcat attempted to import a non-existing page with JavaScript fragments in the URL parameters, it returned a message that the resource was not available. This update adds HTML filtering to Tomcat and the servlet container now correctly returns the message that the resource is missing in this scenario.

Users of tomcat6 are advised to upgrade to these updated packages, which fix these bugs.

7.256.2. RHSA-2013:0869 — Important: tomcat6 security update

Updated tomcat6 packages that fix two security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

Security Fixes

CVE-2013-1976

A flaw was found in the way the tomcat6 init script handled the tomcat6-initd.log log file. A malicious web application deployed on Tomcat could use this flaw to perform a symbolic link attack to change the ownership of an arbitrary system file to that of the tomcat user, allowing them to escalate their privileges to root.

CVE-2013-2051

Note: With this update, tomcat6-initd.log has been moved from /var/log/tomcat6/ to the /var/log/ directory.

It was found that the RHSA-2013:0623 update did not correctly fix CVE-2012-5887, a weakness in the Tomcat DIGEST authentication implementation. A remote attacker could use this flaw to perform replay attacks in some circumstances. Additionally, this problem also prevented users from being able to authenticate using DIGEST authentication.

Red Hat would like to thank Simon Fayer of Imperial College London for reporting the CVE-2013-1976 issue.

Users of Tomcat are advised to upgrade to these updated packages, which correct these issues. Tomcat must be restarted for this update to take effect.

7.256.3. RHSA-2013:0623 — Important: tomcat6 security update

Updated tomcat6 packages that fix multiple security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with the description below.

Apache Tomcat is a servlet container.

Security Fixes

CVE-2012-3546

It was found that when an application used FORM authentication, along with another component that calls request.setUserPrincipal() before the call to FormAuthenticator#authenticate() (such as the Single-Sign-On valve), it was possible to bypass the security constraint checks in the FORM authenticator by appending "/j_security_check" to the end of a URL. A remote attacker with an authenticated session on an affected application could use this flaw to circumvent authorization controls, and thereby access resources not permitted by the roles associated with their authenticated session.

CVE-2012-4534

A flaw was found in the way Tomcat handled sendfile operations when using the HTTP NIO (Non-Blocking I/O) connector and HTTPS. A remote attacker could use this flaw to cause a denial of service (infinite loop). The HTTP blocking IO (BIO) connector, which is not vulnerable to this issue, is used by default in Red Hat Enterprise Linux 6.

CVE-2012-5885, CVE-2012-5886, CVE-2012-5887

Multiple weaknesses were found in the Tomcat DIGEST authentication implementation, effectively reducing the security normally provided by DIGEST authentication. A remote attacker could use these flaws to perform replay attacks in some circumstances.

Users of Tomcat should upgrade to these updated packages, which correct these issues. Tomcat must be restarted for this update to take effect.

7.257. TRACE-CMD

7.257.1. RHBA-2013:0423 — trace-cmd bug fix and enhancement update

Updated trace-cmd packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The trace-cmd packages contain a command-line tool that interfaces with the ftrace utility in the kernel.

Bug Fixes

BZ#746656

The trace-cmd extract command read a buffer multiple times even after an EOF condition. Consequently, the output of the trace-cmd command contained duplicate data. With this update, the trace-cmd utility has been modified to respect the EOF condition and avoid duplication of data in its output.

BZ#879792

When using the latency tracer, the start_threads() function was not called. Calling the stop_threads() function without first calling start_threads() caused the trace-cmd record command to terminate with a segmentation fault because PIDs were not initialized. Consequently, the trace.dat file was not generated. With this update, stop_threads() is not called unless start_threads() is called first. As a result, the segmentation fault no longer occurs.

Enhancement

BZ#838746

Previously, the trace-cmd record command was able to filter ftrace data based on a single PID only. With this update, multiple PIDs can be specified by using the "-P" option.

Users of trace-cmd are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.258. TUNED

7.258.1. RHBA-2013:0538 — tuned bug fix update

Updated tuned packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The tuned packages contain a daemon that tunes system settings dynamically. It does so by monitoring the usage of several system components periodically.

Bug Fixes

BZ#907856

Previously, the ktune service did not save readahead values. On startup, it multiplied the current value by a constant and divided the value by the same constant on stop. This could result in a wrong value being set on devices that were added after ktune had been started. Now, the previous readahead values are stored for all devices and the correct values are restored on ktune stop.

BZ#907768

Previously, when multiple devices were added into the system, a udev rule restarted ktune for each new device. This could lead to many restarts in a short period of time. The multiple restarts could trigger a race condition in the kernel, which cannot be currently fixed. The tuned daemon code has been modified not to trigger more than one restart per 10 seconds, thus preventing the race condition from occurring.

Users of tuned are advised to upgrade to these updated packages, which fix these bugs.

7.258.2. RHBA-2013:0386 — tuned bug fix update

Updated tuned packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The tuned packages contain a daemon that tunes system settings dynamically. It does so by monitoring the usage of several system components periodically.

Bug Fixes

BZ#714180

Red Hat Enterprise Linux 6.1 and later enters processor power-saving states more aggressively. This could result in a small performance penalty on certain workloads. With this update, the pmqos-static.py daemon has been added to the tuned packages, which allows to set the requested latency using the kernel Power Management QoS interface. It is run when the "latency-performance" profile is activated and it sets cpu_dma_latency=0, which keeps the CPU in C0 state, thus making the system as responsive as possible.

BZ#784308

When the ELEVATOR_TUNE_DEVS option was set to a disk device in the /etc/sysconfig/ktune file instead of providing a disk scheduler control file, the scheduler setting was not written to a disk scheduler control file but directly into the disk device file. Consequently, contents of the disk could become corrupted. With this update, the value of ELEVATOR_TUNE_DEVS is checked and only the disk scheduler control file is allowed for writing. As a result, an invalid value of ELEVATOR_TUNE_DEVS is detected in the described scenario so that the disk contents damage can be prevented.

BZ#801561

When the tuned daemon run with the "enterprise-storage" profile enabled and a non-root, non-boot disk partition from a device with write-back cache was mounted, tuned remounted the partition with the "nobarriers" option. If a power failure occurred at that time, the file system could become corrupted. With this update, tuned can detect usage of write-back cache on devices communicating with kernel via SCSI. In these cases, "nobarriers" is now disabled, thus preventing this bug in the described scenario.

BZ#845336

Previously, when the tuned service was started, the tuned PID file was created with world-writable permissions. This bug has been fixed and the /var/run/tuned/tuned.pid file is now created with correct permissions as expected.

BZ#847445

On a machine with hot-plug disk devices with the "enterprise-storage" profile activated, a new disk device could be added into the system, or the disk could be removed and inserted back. In such a scenario, the scheduler and read-ahead settings from the profile were not applied on the newly-added disks. With this update, a new udev rule has been added, which restarts the ktune daemon whenever a new disk device is added, thus fixing this bug.

BZ#887355

The transparent hugepage kernel thread could interfere with latency-sensitive applications. To lower the latency, the transparent hugepages are now disabled in the latency-performance tuned profile.

BZ#886956

Previously, non-root, non-boot partitions were re-mounted using the "nobarrier" option to improve performance. On virtual guests, this could lead to data corruption if power supply was suddenly interrupted, because there was usually a host cache in transfer. This bug has been fixed and the virtual-guest profile no longer re-mounts partitions using "nobarrier".

Users of tuned are advised to upgrade to these updated packages, which fix these bugs.

7.259. UDEV

7.259.1. RHBA-2013:0435 — udev bug fix and enhancement update

Updated udev packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The udev packages implement a dynamic device directory, providing only the devices present on the system. This dynamic directory is managed in user space, dynamically creates and removes devices, provides consistent naming, and a user-space API.

Bug Fixes

BZ#784697

Previously, the /dev/disk/by-id file contained all expected symbolic links for cciss devices, but only one device link was present in the /dev/disk/by-path/ directory. This bug has been fixed and this file now contains all symbolic links as expected.

BZ#790321

The udev(7) man page did not document the hex encoding of blacklisted characters used in the device or symbolic link names. This update adds a paragraph about character encoding into the SYMLINK section of the udev(7) man page.

BZ#829188

Due to a bug in the binutils linker, the libudev library lost the ExecShield (GNU_RELRO) section and was not protected by the ExecShield security mechanism. This update contains libudev with the ExecShield (GNU_RELRO) section included.

BZ#838451

When using multipath devices, the udev utility tried to make a UUID symbolic link for all the different paths, but only the first one succeeded. Consequently, udev wrote several "File exists" error messages to the system log. This update provides a patch to change these messages from being logged as an error message to being logged as an informational message.

BZ#847925

When no medium was inserted in a drive, the cdrom_id utility, which is an udev helper tool, could not read DV and CD-ROM drive profiles. Consequently, the udev properties for the device node of the drive may not have contained all properties describing the capabilities of the drive, which could prevent other software using the udev database from offering all functionality for the drive. This bug has been fixed and all udev properties for the drive, which cdrom_id detects via drive's properties, are now stored for the device as expected.

Enhancement

BZ#826396

Previously, kernel messages showed device names instead of persistent device names provided by udev. As a consequence, device names could point to different devices every boot. This enhancement adds a new feature, which stores the mapping of device names, such as sda or sdb, and persistent device names to kernel messages.

All users of udev are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.260. USBREDIR

7.260.1. RHBA-2013:0346 — usbredir bug fix and enhancement update

Updated usbredir packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The usbredir packages provide a protocol for redirection of USB traffic from a single USB device to a different virtual machine then the one to which the USB device is attached. The usbredir packages contain a number of libraries to help implement support for usbredir.

NOTE

The usbredir packages have been upgraded to upstream version 0.5.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#842356)

Bug Fixes

BZ#834560

Due to a bug in the libusbredirhost library, handling of timeouts for bulk transfers did not work correctly. Consequently, traffic of USB ACM serial port devices, such as PSTN modems and SmartCard readers, could not be properly redirected. With this update, no timeout is set on the usb-host side for these devices and the traffic redirection works as expected.

BZ#855737

The usbredir code was allocating an unlimited amount of write buffers. Consequently, when a USB webcam produced data faster then it could be written out, the write queue grew boundlessly and the remote-viewer utility used an enormous amount of RAM. The underlying source code has been modified so that usbredir now checks how large the write queue is and drops isochronous data packets when the queue is too long.

Enhancement

BZ#842316

Support for live migration of SPICE USB redirection requires support for state serialization. This update adds this missing support to the libusbredirparser library.

All users of usbredir are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.261. UTIL-LINUX-NG

7.261.1. RHSA-2013:0517 — Low: util-linux-ng security, bug fix and enhancement update

Updated util-linux-ng packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The util-linux-ng packages contain a large variety of low-level system utilities that are necessary for a Linux operating system to function.

Security Fix

CVE-2013-0157

An information disclosure flaw was found in the way the `mount` command reported errors. A local attacker could use this flaw to determine the existence of files and directories they do not have access to.

Bug Fixes

BZ#790728

Previously, the **blkid** utility ignored swap area UUIDs if the first byte was zero. As a consequence, the swap areas could not be addressed by UUIDs; for example, from the `/etc/fstab` file. The libblkd library has been fixed and now swap partitions are labeled with a valid UUID value if the first byte is zero.

BZ#818621

Previously, the **lsblk** utility opened block devices to check if the device was in read-only mode, although the information was available in the `/sys` file system. This resulted in unexpected SELinux alerts and unnecessary `open()` calls. Now, the **lsblk** utility does not perform unnecessary opening operations and no longer reads the information from the `/sys` file system.

BZ#736245

On a non-uniform CPU configuration, for example on a system with two sockets with a different number of cores, the `lscpu` command failed unexpectedly with a segmentation fault and a core dump was generated. After this update, when executing the `lscpu` command on such a configuration, the correct result is printed and no core dump is generated.

BZ#837935

On a system with a large number of active processors, the `lscpu` command failed unexpectedly with a segmentation fault and a core dump was generated. This bug is now fixed and the `lscpu` command now works as expected on this configuration.

BZ#819945

Executing the `hwclock --systz` command to reset the system time based on the current time zone caused the clock to be incorrectly adjusted by one hour. This was because **hwclock** did not adjust the system time during boot according to the "warp clock" semantic described in the `settimeofday(2)` man page. With this update, **hwclock** correctly sets the system time when required.

BZ#845477

When SElinux options were specified both in the `/etc/fstab` file and on the command line, mounting failed and the kernel logged the following error upon running **dmesg**:

```
SELinux:  duplicate or incompatible mount options
```

The handling of SElinux options has been changed so that options on the command line now replace options given in the **/etc/fstab** file and as a result, devices can be mounted successfully.

BZ#845971

Due to a change in the search order of the mount utility, while reading the **/etc/fstab** file, the **mount** command returned a device before a directory. With this update, the search order has been modified and **mount** now works as expected.

BZ#858009

Previously, any new login or logout sequence by a telnet client caused the **/var/run/utmp** file to increase by one record on the telnetd machine. As a consequence, the **/var/run/utmp** file grew without a limit. As a result of trying to search though a huge **/var/run/utmp** file, the machine running **telnetd** could experience more severe side-effects over time. For example, the **telnetd** process could become unresponsive or the overall system performance could degrade. The **telnetd** now creates a proper record in **/var/run/utmp** before starting the logging process. As a result, the **/var/run/utmp** does not grow without a limit on each new login or logout sequence of a telnet session.

BZ#730891, BZ#783514, BZ#809139, BZ#820183, BZ#839281

Man pages of several utilities included in the package have been updated to fix minor mistakes and add entries for previously undocumented functionalities.

Enhancements

BZ#719927

A new **--compare** option for **hwclock** to compare the offset between system time and hardware clock has been added due to a discontinued distribution of **adjtimex** in Red Hat Enterprise Linux 6.0 and later, which had previously provided this option.

BZ#809449

The **lsblk** command now supports a new option, **--inverse**, used to print dependencies between block devices in reverse order. This feature is required to properly reboot or shut down systems with a configured cluster.

BZ#823008

The **lscpu** utility, which displays detailed information about the available CPUs, has been updated to include numerous new features. Also, a new utility, **chcpu**, has been added, which allows the user to change the CPU state (online or offline, standby or active, and other states), disable and enable CPUs, and configure specified CPUs. For more information about these utilities, refer to the **lscpu(1)** and **chcpu(8)** man pages.

Users of util-linux-ng are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.262. VALGRIND

7.262.1. RHBA-2013:0347 — valgrind bug fix and enhancement update

Updated valgrind packages that fix several bugs and add an enhancement are now available for Red Hat Enterprise Linux 6.

The valgrind packages provide a programming utility for debugging memory, detecting memory leaks, and profiling.

NOTE

The valgrind packages have been upgraded to upstream version 3.8.1, which provides a number of bug fixes over the previous version. (BZ#823005)

Bug Fixes

BZ#730303

When running a large program under valgrind, the "Valgrind: FATAL: VG_N_SEGNAMES is too low." error messages could be returned. With this update, the compile time constants have been increased (VG_N_SEGMENTS to 50000, VG_N_SEGNAMES to 25000) and these errors no longer occur.

BZ#862795

Previously, the valgrind gdbserver did not properly report exit or a fatal-signal process termination to the gdb debugger. Consequently, the "Remote connection closed" error messages were returned. This bug has been fixed in the code and the process termination is now properly reported in gdb.

BZ#816244

On IBM S/390 architecture, valgrind could report a "Conditional jump or move depends on uninitialized value(s)" warning message for the tsearch() function in glibc. This update includes a standard suppression for these warning messages, which are no longer reported.

Enhancement

BZ#672959

The embedded gdbserver has been added to allow integration of valgrind with the gdb debugger.

Users of valgrind are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.263. VGABIOS

7.263.1. RHBA-2013:0487 — vgabios bug fix update

An updated vgabios package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The vgabios package provides a GNU Lesser General Public License (LPGL) implementation of a BIOS for video cards. The vgabios package contains BIOS images that are intended to be used in the Kernel Virtual Machine (KVM).

Bug Fix

BZ#840087

Previously, an attempt to boot a Red Hat Enterprise Virtualization Hypervisor ISO in a virtual machine was unsuccessful. The boot menu appeared but then stopped responding. The underlying source code has been modified and the virtual machine now works as expected in the described scenario.

All users of vgabios are advised to upgrade to this updated package, which fixes this bug.

7.264. VIRTIO-WIN

7.264.1. RHBA-2013:0441 — virtio-win bug fix and enhancement update

Updated virtio-win packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The virtio-win packages provide paravirtualized network drivers for most Microsoft Windows operating systems. Paravirtualized drivers are virtualization-aware drivers used by fully virtualized guests running on Red Hat Enterprise Linux. Fully virtualized guests using the paravirtualized drivers gain significantly better I/O performance than fully virtualized guests running without the drivers.

Bug Fixes

BZ#750421

Prior to this update, a Windows Server 2003 guest could become suspended when rebooting if the balloon size was changed before, due to a lack of free memory. This update releases the memory to the guest before processing the power management request.

BZ#760022

Prior to this update, the **virtio-win** floppy disk did not contain NDIS drivers for Windows XP and Windows 7 platforms due to a lack of free space on VFD media. This update modifies the underlying code and switches to 2.88 MB media instead of 1.44 MB.

BZ#768795

Prior to this update, the work items processed the **`inflate`** and **`deflate`** requests. As a consequence, a stop error could occur when several requests were executed simultaneously. This update uses a dedicated thread instead of work items to process the **`inflate`** and **`deflate`** requests in sequence.

BZ#805423

Prior to this update, the port surprise-removal handler did not stop and purge the **`write`** and **`read`** queues. As a consequence, requests could be send to already removed devices. This update modifies the underlying code to stop and purge the **`write`** and **`read`** queues as expected and requests are no longer sent to removed devices.

BZ#807967, BZ#875155

Prior to this update, the initialization sequence of the **virtio-net** driver did not work properly after disabling and enabling **virtio-net**, or when resetting the power management. As a consequence, the first packets that were sent through the DHCP client could, under certain circumstances, become suspended in the queue and the DHCP client did not receive the IP address. With this update, the initialization sequence has been fixed and **virtio-net** now works as expected in the described scenario.

BZ#814896

Prior to this update, the **virtio** queue was not correctly reinitialized during the **`resume`** routine. As a consequence, ports could not handle the **`read`** requests correctly. This update adds the correct virtual queue for re-initialization when resuming after hibernation.

BZ#815295

On Microsoft Windows 7 operating system, a driver disregarded platform requests to indicate only a certain number of packets during one DPC (Deferred Procedure Call). As a consequence, the Windows Hardware Quality Labs (WHQL) test failed and the platform did not moderate the driver workload for the RX path. This update modifies the underlying code to implement packet indication moderation and the WHQL certification now passes in the described scenario.

BZ#824814

Prior to this update, the **`viostor`** driver did not handle configuration change events as expected. Consequently, when a relevant image was resized on-line, **`viostor`** left it unattended. This update modifies the underlying code to reset the bus sequence when changing the configurations and the driver can now recognize that media has been resized.

BZ#831570

Prior to this update, the work items processed the **`inflate`** and **`deflate`** requests. As a consequence, the **`inflate`** and **`deflate`** requests could be executed simultaneously with PnP and Power management (PM) handlers. This update uses a dedicated thread instead of work items to process the PnP and PM requests only after all other pending requests are completed.

BZ#839143

Prior to this update, the **`balloon`** driver failed to keep the current balloon size between hibernation-resume cycles and restarts. This update keeps the current balloon size between restarts and hibernation-resume cycles and adjusts the balloon size according to this value.

Enhancements

BZ#782268

This update introduces the **vioscsi.sys** driver to virtio-win packages to provide **virtio-scsi** functionality to Microsoft Windows platforms.

BZ#828275

This update adds support for the **virtio** control queue to offload RX filtering to the host.

BZ#834175

This update supports all possible offload combinations and offload parities between IPv4 and IPv6 for Windows certification 2012 and Windows 8 certification.

BZ#838005

This update adds offloads for IPv6 to virtio packages.

BZ#908163

This update adds virtual floppy drive drivers for Windows Server 2008 R2 guests to virtio packages.

Users of virtio-win are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.265. VIRT-MANAGER

7.265.1. RHBA-2013:0451 — virt-manager bug fix and enhancement update

Updated virt-manager packages that fix three bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

Virtual Machine Manager (virt-manager) is a graphical tool for administering virtual machines for KVM, Xen, and QEMU. The virt-manager utility uses the libvirt API and can start, stop, add or remove virtualized devices, connect to a graphical or serial console, and view resource usage statistics for existing virtualized guests on local or remote machines.

Bug Fixes

BZ#802639

Previously, the live migration dialog box of the virt-manager tool incorrectly described the unit of bandwidth as "Mbps" instead of "MB/s". With this update, the migration dialog has been changed to provide correct information on bandwidth units.

BZ#824275

Prior to this update, an unnecessary reboot occurred after the virt-manager tool created a new guest virtual machine by importing an existing disk image. With this update, a backported upstream patch has been provided, and virt-manager no longer restarts after importing an existing disk image.

BZ#872611

Due to differences in dependency solving between the yum and rpm programs, the virt-manager package failed to update from "noarch" to newer architecture version. With this update, a patch has been provided to mark the noarch version as obsolete. As a result, the noarch package can now be updated without complications.

Enhancement

BZ#878946

The "Delete Associated storage files" option is enabled by default in the virt-manager tool. A warning message is displayed prior to file deletion to notify the user about this configuration.

All users of virt-manager are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.266. VIRT-TOP

7.266.1. RHBA-2013:0391 — virt-top bug fix and enhancement update

Updated virt-top packages that fix two bugs and add three enhancements are now available for Red Hat Enterprise Linux 6.

The virt-top utility displays statistics of virtualized domains and uses many of the same keys and command-line options as the top utility.

Bug Fixes

BZ#807176

Prior to this update, the "-o" (sort) option was not properly described in the output of the "virt-top --help" command. Four of the possible sort parameters were not mentioned in the description. This bug has been fixed and the full range of sort parameters is now shown in the virt-top --help message.

BZ#834208

Previously, the column names of the virt-top summary table were not explained in the virt-top man page. The manual page has been updated, and the headings are now properly documented in the "COLUMN HEADINGS" section.

Enhancements

BZ#825627

The copyright information has been updated in the virt-top man pages and help documents.

BZ#835547

This update adds a separate man page for the processcsv.py script, which was previously documented only in the virt-top man page.

BZ#841759

With this update, the "virt-top -1" command has been enhanced to separately display the usage of virtual CPUs. Two numbers are now shown under each domain column; the first is the percentage of the physical CPU used by the domain and the hypervisor together, the second is the percentage used just by the domain. This information is important for performance tuning and other tasks.

All users of virt-top are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.267. VIRT-V2V

7.267.1. RHBA-2013:0477 — virt-v2v bug fix and enhancement update

Updated virt-v2v packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The virt-v2v packages provide a tool for converting virtual machines to use the Kernel-based Virtual Machine (KVM) hypervisor or Red Hat Enterprise Virtualization. The tool modifies both the virtual machine image and its associated libvirt metadata. Also, virt-v2v can configure a guest to use VirtIO drivers if possible.

Bug Fixes

BZ#794680

The virt-v2v packages used to rename block devices in various guest configuration files during conversion, including the /etc/fstab file. Consequently, the virt-v2v utility returned a redundant warning message when a guest's /etc/fstab file referenced to the /etc/fd0 file as the block device did not know it. To fix this bug, warning messages concerning floppy devices have been explicitly suppressed and virt-v2v no longer returns warning messages in this situation.

BZ#803629

When reading a libvirt guest, virt-v2v uses libvirt metadata to determine the on-disk format, considering only those of "dir", "fs", and "netfs" types as meaningful. If a guest used a different type of storage pool, virt-v2v interpreted these data as a format type, which was unable to convert by libvirt guests. To address this bug, virt-v2v now only uses volume format metadata from storage pools of type "dir", "fs", and "netfs", but also all other storage pools can only hold raw data, so the format is assumed to be "raw". As a result, virt-v2v can now convert libvirt guests using any supported storage pool type.

BZ#838057

When creating a new libvirt guest, virt-v2v failed to disable caching for disks as recommended. As a consequence, guests created by virt-v2v used caching for their disks, unless explicitly disabled by the user after conversion. To address this bug, virt-v2v now explicitly disables caching for all disks when creating a new libvirt guest, and guests created by virt-v2v now have caching disabled for all disks. The user can enable it again if required after conversion.

BZ#868405

Virt-v2v failed when attempting to perform an on-disk format conversion when reading a guest using the libvirtxml input method. A patch has been provided to fix this bug and virt-v2v can now perform format conversions on guests using libvirtxml.

Enhancement

BZ#682945

With this update, virt-v2v can do an on-disk format conversion while converting a remote libvirt guest. Note that when doing this kind of format conversion, virt-v2v must make an intermediate copy of the guest storage data on the conversion server. Other types of conversion do not require any intermediate storage on the conversion server. The user must ensure that the TMPDIR temporary directory has sufficient space for this intermediate copy.

Users of virt-v2v are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.268. VIRT-VIEWER

7.268.1. RHBA-2013:0361 — virt-viewer bug fix and enhancement update

Updated virt-viewer packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The virt-viewer packages provide Virtual Machine Viewer, which is a lightweight interface for interacting with the graphical display of a virtualized guest. Virtual Machine Viewer uses `libvirt` and is intended as a replacement for traditional VNC or SPICE clients.

Bug Fixes

BZ#814150

The **`remote-viewer`** and the **`virt-viewer`** tools, both use the same constant to print their usage message. Consequently, when the user used an unknown command option with the **`remote-viewer`** command, the error message referred to the **`virt-viewer --help`** command instead of the **`remote-viewer --help`** command. With this update, the **`remote-viewer`** and **`virt-viewer`** code has been modified so that the commands now return the correct error message when used with an unknown option.

BZ#822794

When connected to a guest using the **`virt-viewer -v`** command and the console was closed, the command prompt was printed at the end of the last line instead of the new line. This update fixes this bug and the command prompt is printed correctly.

BZ#832121

If the XML listen attribute contained a string consisting of the colon (":") and zero ("0") characters, **`virt-viewer`** did not treat the string as a wildcard address and did not create an appropriate remote host address as expected. Consequently, an attempt to connect to a remote host with such an address led to the connection failure. This update modifies the underlying source code to treat the aforementioned characters as wildcards and **`virt-viewer`** now successfully connects to a remote host in the described scenario.

BZ#854318

Due to changes in the latest upstream version of the spice-gtk packages, **`virt-viewer`** stopped working with the new **`spice-gtk`** module. With this update, the virt-viewer packages have been rebuilt to work properly with this new version of **`spice-gtk`**.

BZ#856610

Previously, the automatic window resize option did not work correctly with the **`remote-viewer`** client. When disabling and then re-enabling the automatic window size, the resized window was smaller then expected. This update provides a patch to fix this bug and the automatic window resize option now works properly.

BZ#856678

Within certain non-US keyboard layouts, keyboard shortcuts using the "Alt" key and another character worked even if they were disabled in a virtual machine. This update applies a patch that fixes this bug and keyboard shortcuts are now disabled as expected.

BZ#864929

Previously, when the **`virt-viewer`** client was sized to the full screen, the virt-viewer size resolution could not be set to a higher resolution than the monitor's native resolution. With this update, the user is now able to set a higher resolution than the monitor's native resolution.

BZ#867248

When connecting to a SPICE guest and the user input an incorrect graphic password first, a later attempt to connect using the correct password was unsuccessful, and the **`virt-viewer`** tool terminated unexpectedly. This update modifies the underlying code so that **`virt-viewer`** no longer crashes in the described scenario.

BZ#867459

When connecting to the Red Hat Enterprise Virtualization portal and the **`remote-viewer`** client was started from the **`XPI`** plug-in, the client terminated unexpectedly with a segmentation fault. This update modifies the underlying code and applies a patch to fix this bug so that **remote-viewer** now works as expected in this situation.

BZ#881020

Previously, when using **remote-viewer** to display multiple screens of a virtual machine with multiple physical displays, under certain circumstances, **remote-viewer** could display only one screen in single **remote-viewer** window and the other screens were disconnected. With this update, the underlying code has been modified so that all physical displays are now properly displayed in the respective **remote-viewer** windows.

Enhancements

BZ#828339

This enhancement provides the new **--title** option which allows the user to specify a title displayed in the remote-viewer window title bar.

BZ#842305

With this update, the **virt-viewer** tool supports the **SpiceMonitorsConfig** display message.

BZ#865793

The **virt-viewer** tool is now able to handle requests from the Red Hat Enterprise Virtualization portal to enable or disable passing of the Ctrl+Alt+Delete key combination to the guest operating system.

BZ#875126

Screenshots can be currently saved only in the PNG format. With this update, the ".png" suffix is automatically added to the screenshot file name if is it missing.

All users of virt-viewer are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.269. VIRT-WHAT

7.269.1. RHEA-2013:0483 — virt-what enhancement update

Updated virt-what packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The virt-what packages provide a command-line tool that is used to detect whether the operating system is running inside a virtual machine.

Enhancement

BZ#829427

This enhancement adds support for the Virtage hardware partitioning system to the virt-what utility.

All users of virt-what are advised to upgrade to these updated packages, which add this enhancement.

7.270. VIRT-WHO

7.270.1. RHBA-2013:0374 — virt-who bug fix and enhancement update

Updated virt-who packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The virt-who packages provide an agent that collects information about virtual guests present in the system and reports them to the Red Hat Subscription Manager tool.

Bug Fixes

BZ#825215

Previously, when running the virt-who service, unregistering a Red Hat Enterprise Virtualization Hypervisor host from the Subscription Asset Manager (SAM) server caused the service to be terminated with the following message:

```
SubscriptionManagerError: No such file or directory
Error in communication with candlepin, trying to recover
Unable to read certificate, system is not registered or you are not root
```

Only the last line of the aforementioned message should have been displayed. This bug has been fixed, and the traceback errors are now saved to the log file and not printed on the screen.

BZ#866890

When a snapshot of a virtual machine (VM) was created in Microsoft Hyper-V Server, the virt-who agent replaced the UUID of the VM file with the UUID of the snapshot. This bug has been fixed, and the UUID is not changed in the described case. Additionally, in certain cases, the virt-who agent running with the "--hyperv" command-line option terminated with the following message:

```
AttributeError: HyperV instance has no attribute 'ping'
```

This bug has been fixed and the aforementioned error no longer occurs.

BZ#869960

Previously, the virt-who agent failed to function correctly when a URL, which was set in the VIRTWHO_ESX_SERVER parameter, was missing the initial "https://" string. With this update, virt-who has been modified, and "https://" is no longer required in VIRTWHO_ESX_SERVER.

Enhancements

BZ#808060

With this update, the virt-who agent has been modified to start as a foreground process and to print error messages or debugging output (the "-d" command-line option) to the standard error output. Moreover, the following command-line options have been enhanced: the "-o" option provides the one-shot mode and exits after sending the list of guests; the "-b" option and the "service virt-who start" command equivalently start on the background and send data to the /var/log/ directory.

BZ#846788

The virt-who agent has been modified to support Red Hat Enterprise Virtualization Manager polling.

BZ#860854

With this update, the virt-who agent has been modified to correctly recognize guest virtual machines, which are installed on top of Microsoft Hyper-V Server.

BZ#868149

The virt-who manual pages and the output of the "virt-who --help" command have been enhanced with clarifying information. In addition, a typographical error has been corrected in both texts.

All users of virt-who are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.271. WDAEMON

7.271.1. RHBA-2013:0293 — wdaemon bug fix and enhancement update

Updated wdaemon packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The wdaemon packages contain a daemon to wrap input driver hotplugging in the X.Org implementation of the X Window System server. The wdaemon packages emulate virtual input devices to avoid otherwise non-persistent configuration of Wacom tablets to persist across device removals.

Bug Fix

BZ#852332

Due to the broken %postun scriptlet, an attempt to uninstall wdaemon caused an error message to appear. This error message also occurred during the wdaemon update because the old package is removed during the update. Consequently, the wdaemon service was not restarted after the update. The %postun scriptlet has been fixed and wdaemon works as expected in this situation.

Enhancement

BZ#838752

This enhancement adds support for emulation of the Wacom Intuos5 tablet series.

All users of wdaemon are advised to upgrade to these updated packages which fix this bug and add this enhancement.

7.272. WGET

7.272.1. RHBA-2012:1353 — wget bug fix update

Updated wget packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The wget packages provide the GNU Wget file retrieval utility for HTTP, HTTPS, and FTP protocols. Wget provides various useful features, such as the ability to work in the background while the user is logged out, recursive retrieval of directories, file name wildcard matching or updating files in dependency on file timestamp comparison.

Bug Fixes

BZ#754168

Prior to this update, the wget package contained a redundant URL to the wget upstream project. This update modifies the specification file to list the correct http://www.gnu.org/software/wget/.

BZ#814208

Prior to this update, the wget utility did not previously work as intended with the "-T, --timeout" option set when http server did not answer the SSL handshake. Wget source code has been patched, to ensure that wget aborts the connection when using --timeout option correctly.

BZ#714893

Prior to this update, the wget utility source code was lacking check of the HTTP response parsing function return value. In some cases, when HTTP response header was malformed (fuzzed), the parsing function returned error. Because the returned value was not checked, it then resulted in Segmentation Fault. This update adds check of the HTTP response parsing function return value in the wget source code. Now when HTTP response header is malformed (fuzzed) and the parsing function returns error, the following error message is thrown and wget retries the request:

```
2012-10-01 10:13:44 ERROR -1: Malformed status line.
```

All users of wget are advised to upgrade to these updated packages, which fix this bug.

7.273. WPA_SUPPLICANT

7.273.1. RHBA-2013:0431 — wpa_supplicant bug fix and enhancement update

Updated wpa_supplicant packages that fix multiple bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The wpa_supplicant packages contain a WPA (Wi-Fi Protected Access) Supplicant utility for Linux, BSD, and Windows with support for WPA and WPA2 (IEEE 802.11i/RSN). The supplicant is an IEEE 802.1X/WPA component that is used in client workstations. It implements key negotiation with a WPA Authenticator and it controls the roaming and IEEE 802.11 authentication and association of the WLAN driver.

Bug Fixes

BZ#813579

When roaming from one Access Point (AP) to another and the connection was disrupted, NetworkManager did not always automatically reconnect. This update includes a number of backported upstream patches to improve Proactive Key Caching (PKC), also known as Opportunistic Key Caching (OKC). As a result, WPA connections now roam more reliably.

BZ#837402

Previously, the supplicant would attempt to roam to slightly stronger access points, increasing the chance of a disconnection. This bug has been fixed and the supplicant now only attempts to roam to a stronger access point when the current signal is significantly degraded.

Enhancement

BZ#672976

The "wpa_gui" program was removed from "wpa_supplicant" in the 6.0 release as per BZ#553349, however, the man page was still being installed. This upgrade removes the man page.

All users of wpa_supplicant are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.274. X3270

7.274.1. RHBA-2013:0383 — x3270 bug fix update

Updated x3270 packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The x3270 packages provide an emulator for the IBM 3278 (monochrome) and 3279 (color) terminals.

Bug Fix

BZ#801139

Prior to this update, the x3270 emulator failed to support the double-byte character set (DBCS). As a consequence, the character sets option for Japanese was disabled. This update modifies the underlying code to enable DBCS and adds the icu packages as a dependency. Now, Japanese character sets are again available.

All users of x3270 are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.275. XFSDUMP

7.275.1. RHBA-2013:0482 — xfsdump bug fix update

Updated xfsdump packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The xfsdump packages provide several utilities for managing XFS file systems, including xfsrestore and xfsdump.

Bug Fix

BZ#860454

With Red Hat Enterprise Linux 6.4, XFS has been enhanced to allow the use of the 32-bit project quota ID feature. However, the top 16 bits of a 32-bit project quota ID were not properly saved and restored using the xfsdump and xfsrestore utilities. This caused the data to be saved and restored with an incorrect 16-bit project quota ID. With this update, the underlying source code has been fixed so that all 32 bits of the project quota ID are properly saved and restored by xsfdump and xfsrestore.

All users of xfsdump are advised to upgrade to these updated packages, which fix this bug.

7.276. XFSPROGS

7.276.1. RHBA-2013:0481 — xfsprogs bug fix and enhancement update

Updated xfsprogs packages that fix three bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The xfsprogs packages contain a set of commands to use the XFS file system, including the mkfs.xfs command to construct an XFS system.

Bug Fixes

BZ#730433

When the manual geometry of the mkfs.xfs utility was specified for striping as well as calculating of the allocation group counts and size, mkfs.xfs could emit confusing error messages on failure. With this update, more standardized and informative error messages are returned.

BZ#836433

When the sector size was not specified by the "-f" option, the mkfs.xfs utility used the 512 byte sector size by default even for drives with 4 Kb physical sectors. With this update, mkfs.xfs correctly recognizes the sector size in the described scenario, which fixes this bug.

BZ#878859

When attempting to set a 32-bit quota project ID on an XFS file system which did not have this feature enabled, the command returned success, but truncated the project ID to the lower 16 bits. With this update, a project ID of more than 16 bits cannot be set unless the 32-bit project ID feature is enabled.

Enhancement

BZ#827186

With this update, mkfs.xfs can enable 32-bit project quota IDs on a file system with the "-i projid32bit=1" parameter specified. Without this parameter, mkfs.xfs defaults to 16-bit project quota IDs. The 32-bit project quota IDs can be enabled on existing file systems by using the "xfs_admin -p" command.

All users who use the XFS file system are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.276.2. RHBA-2013:0987 — xfsprogs bug fix update

Updated xfsprogs packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The xfsprogs packages contain a set of commands to use the XFS file system, including the mkfs.xfs command to construct an XFS file system.

Bug Fixes

BZ#971698

When stripe geometry was specified manually to the mkfs.xfs utility, mkfs.xfs did not properly select "multidisk mode" as it does when stripe geometry is automatically detected. As a result, a less than optimal number of allocation groups were created. With this update, multidisk mode is selected properly, and a larger number of allocation groups are created.

BZ#976217

Previously, xfs_repair was unable to properly handle fragmented multiblock version 2 directories (Multiblock dir2 is only enabled with the "-n size=" mkfs.xfs option, where the size is greater than the file system block size). With this update, xfs_repair can operate on fragmented dir2 directories without errors.

Users of xfsprogs are advised to upgrade to these updated packages, which fix these bugs.

7.277. XINETD

7.277.1. RHSA-2013:0499 — Low: xinetd security and bug fix update

An updated xinetd package that fixes one security issue and two bugs is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The xinetd package provides a secure replacement for inetd, the Internet services daemon. xinetd provides access control for all services based on the address of the remote host and/or on time of access, and can prevent denial-of-access attacks.

Security Fix

CVE-2012-0862

When xinetd services are configured with the "TCPMUX" or "TCPMUXPLUS" type, and the tcpmux-server service is enabled, those services are accessible via port 1. It was found that enabling the tcpmux-server service (it is disabled by default) allowed every xinetd service, including those that are not configured with the "TCPMUX" or "TCPMUXPLUS" type, to be accessible via port 1. This could allow a remote attacker to bypass intended firewall restrictions.

Red Hat would like to thank Thomas Swan of FedEx for reporting this issue.

Bug Fixes

BZ#790036

Prior to this update, a file descriptor array in the service.c source file was not handled as expected. As a consequence, some of the descriptors remained open when xinetd was under heavy load. Additionally, the system log was filled with a large number of messages that took up a lot of disk space over time. This update modifies the xinetd code to handle the file descriptors correctly and messages no longer fill the system log.

BZ#809271

Prior to this update, services were disabled permanently when their CPS limit was reached. As a consequence, a failed bind operation could occur when xinetd attempted to restart the service. This update adds additional logic that attempts to restart the service. Now, the service is only disabled if xinetd cannot restart the service after 30 attempts.

All users of xinetd are advised to upgrade to this updated package, which contains backported patches to correct these issues.

7.278. X.ORG LEGACY INPUT DRIVERS

7.278.1. RHEA-2013:0295 — X.Org X11 legacy input drivers enhancement update

Updated xorg-x11-drv-acecad, xorg-x11-drv-aiptek, xorg-x11-drv-hyperpen, xorg-x11-drv-elographics, xorg-x11-drv-fpit, xorg-x11-drv-mutouch, xorg-x11-drv-penmount, and xorg-x11-drv-void packages that add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-keyboard and xorg-x11-drv-mouse packages contain the legacy X.Org X11 input drivers for keyboards and mice.

The xorg-x11-drv-acecad, xorg-x11-drv-aiptek, xorg-x11-drv-hyperpen, xorg-x11-drv-elographics, xorg-x11-drv-fpit, xorg-x11-drv-mutouch, xorg-x11-drv-penmount, and xorg-x11-drv-void packages contain the X.Org X11 input drivers for legacy devices.

The following packages have been upgraded to their respective upstream versions, which provide a number of enhancements over the previous versions:

Table 7.3. Upgraded packages

PACKAGE NAME	UPSTREAM VERSION	BZ NUMBER
xorg-x11-drv-acecad	1.5.0	835212
xorg-x11-drv-aiptek	1.4.1	835215
xorg-x11-drv-elographics	1.4.1	835222
xorg-x11-drv-fpit	1.4.0	835229
xorg-x11-drv-hyperpen	1.4.1	835233
xorg-x11-drv-keyboard	1.6.2	835237
xorg-x11-drv-mouse	1.8.1	835242
xorg-x11-drv-mutouch	1.3.0	835243
xorg-x11-drv-penmount	1.5.0	835248
xorg-x11-drv-void	1.4.0	835264

Users of X.Org X11 legacy input drivers are advised to upgrade to these updated packages, which add these enhancements.

7.279. XORG-X11-DRV-ATI

7.279.1. RHBA-2013:0302 — xorg-x11-drv-ati bug fix and enhancement update

Updated xorg-x11-drv-ati packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-ati packages provide a driver for ATI graphics cards for the X.Org implementation of the X Window System.

NOTE

The xorg-x11-drv-ati packages have been upgraded to upstream version 6.99.99, which provides a number of bug fixes and enhancements over the previous version. (BZ#835218)

All users of xorg-x11-drv-ati are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.280. XORG-X11-DRV-EVDEV

7.280.1. RHBA-2013:0297 — xorg-x11-drv-evdev bug fix and enhancement update

Updated xorg-x11-drv-evdev packages that fix several bugs add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-evdev packages contain the X.Org X11 input drivers for keyboards and mice.

NOTE

The xorg-x11-drv-evdev package has been upgraded to upstream version 2.7.3, which provides a number of bug fixes and enhancements over the previous version. (BZ#835225)

All users of xorg-x11-drv-evdev are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.281. XORG-X11-DRV-INTEL

7.281.1. RHBA-2013:0303 — xorg-x11-drv-intel bug fix and enhancement update

Updated xorg-x11-drv-intel packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-intel packages contain an Intel integrated graphics video driver for the X.Org implementation of the X Window System.

NOTE

The xorg-x11-drv-intel packages have been upgraded to upstream version 2.20.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#835236)

All users of xorg-x11-drv-intel are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

7.282. XORG-X11-DRV-NOUVEAU

7.282.1. RHBA-2013:0304 — xorg-x11-drv-nouveau bug fix and enhancement update

Updated xorg-x11-drv-nouveau packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-nouveau package provides the X.Org X11 noveau video driver for NVIDIA graphics chipsets.

NOTE

The xorg-x11-drv-nouveau package has been upgraded to upstream version 1.0.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#835245)

Users of xorg-x11-drv-nouveau are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.283. XORG-X11-DRV-QXL

7.283.1. RHBA-2013:0308 — xorg-x11-drv-qxl bug fix and enhancement update

Updated xorg-x11-drv-qxl packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-qxl packages provide an X11 video driver for the QEMU QXL video accelerator. This driver makes it possible to use Red Hat Enterprise Linux 6 as a guest operating system under the KVM kernel module and the QEMU multi-platform emulator, using the SPICE protocol.

NOTE

The xorg-x11-drv-qxl packages have been upgraded to upstream version 0.1.0, which adds support for multiple monitors and continuous resolution. It aslo provides a number of bug fixes and enhancements over the previous version. (BZ#835249, BZ#787160)

Bug Fixes

BZ#883578

Due to overlapping memory areas, remote-viewer became unresponsive after a migration of a guest playing a video. This update adjusts the monitors_config pointer to fix this issue, and migration of a guest, which is displaying video, works as expected.

BZ#896005

This update disables "surfaces" by default due to a performance regression with the rendering support.

All users of xorg-x11-drv-qxl are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.284. XORG-X11-DRV-SYNAPTICS

7.284.1. RHBA-2013:0298 — xorg-x11-drv-synaptics bug fix and enhancement update

Updated xorg-x11-drv-synaptics packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-synaptics packages contain the X.Org X11 input drivers for Synaptics touchpads.

NOTE

The xorg-x11-drv-synaptics packages have been upgraded to upstream version 1.6.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#835257)

Users of xorg-x11-drv-synaptics are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.285. XORG-X11-DRV-VMMOUSE

7.285.1. RHBA-2013:0300 — xorg-x11-drv-vmmouse bug fix and enhancement update

Updated xorg-x11-drv-vmmouse packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-vmmouse packages contain the X.Org X11 input drivers for the VMware vSphere Hypervisor.

NOTE

The xorg-x11-drv-vmmouse package has been upgraded to upstream version 12.9.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#835262)

Users of xorg-x11-drv-vmmouse are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.286. XORG-X11-DRV-WACOM

7.286.1. RHBA-2013:0296 — xorg-x11-drv-wacom bug fix and enhancement update

Updated xorg-x11-drv-wacom packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-drv-wacom packages contain the X.Org X11 input drivers for Wacom graphics tablets.

NOTE

The xorg-x11-drv-wacom package has been upgraded to upstream version 0.16.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#835266)

Bug Fixes

BZ#859851

Due to a bug in the input driver, covering the Expresskeys on the Wacom Intuos5 graphics tablet caused a spurious stylus jump to the upper left corner (0,0). This bug has been fixed and the described issue no longer occurs.

BZ#862939

Previously, the xorg.conf configuration file with two devices containing the same input node caused a double free error and subsequent failure of the X server. With this update, xorg.conf has been fixed, and the server crash is now prevented.

Enhancements

BZ#838751

With this update, support for the Wacom Intuos5 series graphics tablets has been added to the xorg-x11-drv-wacom package.

BZ#857088

With this update, support for the Wacom Cintiq 22HD series graphics tablets has been added to the xorg-x11-drv-wacom package.

All users of xorg-x11-drv-wacom are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.287. XORG-X11-SERVER

7.287.1. RHBA-2013:0299 — xorg-x11-server bug fix and enhancement update

Updated xorg-x11-server packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11-server packages provide the X.Org sample implementation of a server for the X Window System and the rendering services necessary for graphical user environments, such as GNOME and KDE.

NOTE

Updated xorg-x11-server packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The xorg-x11-server packages have been upgraded to upstream version 1.13.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#833212)

Bug Fixes

BZ#608076

When the GNOME sound volume applet was configured to pop up after pressing the "mute", "volume up", or "volume down" hardware buttons, doing so caused a graphical glitch to appear in a dual monitor configuration. Now, the screen glitch no longer appears.

BZ#745033

When spice-client was opened in full-screen mode, the client screen contained a static image which was not refreshed until it was switched back to window mode. Now, the static image no longer appears when opened in full-screen mode.

BZ#816347

When the screen saver started to fade, pressing keys did not interrupt the fade and did not immediately display the unlock screen. Now, pressing keys stops the screen from fading.

BZ#829321

A NULL pointer dereference caused X.Org to terminate unexpectedly with a segmentation fault on certain servers. The error is fixed and X.Org no longer crashes on those servers.

BZ#837073

An invalid pointer dereference in the server caused the server to unexpectedly terminate with a segmentation fault when the mouse was moved over the VNC window. Crashes no longer occur when moving the mouse over the VNC window.

BZ#853236

The KVM process could not access the X server because the "/usr/bin/Xorg" binary was unreadable for non-root users. Now, all users can read the binary and KVM guests can access host operating systems.

BZ#858005

A transformation matrix is used to bind a device to a specific area on the screen. An uninitialized device transformation matrix caused the pointer to jump to the top-left corner of the screen on some devices. With this update, the transformation matrix is properly initialized and pointer device movement works as expected.

BZ#863913

An X Input Extension (XI 1.x) grab on a disabled device led to a NULL pointer dereference error which caused the server to terminate unexpectedly. Currently, the XI 1.x grab functions normally and the X server no longer crashes.

BZ#864054

When screens are reconfigured, the server updates some internal fields to adjust input device coordinate scaling if the device is bound to a specific screen. The NVIDIA binary driver did not have access to these internal methods, and was not able to update these fields when it changed output configurations. A new API is now exported for the driver and the NVIDIA driver is now able to update the server-internal fields.

BZ#868054

Pointer screen crossings for non-Xinerama setups caused the mouse pointer to wrap around on the first screen instead of moving to the second screen. Now, the mouse pointer can move between both screens on non-Xinerama setups.

BZ#883206

Running xrestop on servers that used Intel, ATI or Nouveau drivers caused the server to terminate unexpectedly with a segmentation fault. Now, users are able to run xrestop on those servers without crashes.

Users of xorg-x11-server are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.287.2. RHSA-2013:1426 — Important: xorg-x11-server security update

Updated xorg-x11-server packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

X.Org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

Security Fix

CVE-2013-4396

A use-after-free flaw was found in the way the X.Org server handled ImageText requests. A malicious, authorized client could use this flaw to crash the X.Org server or, potentially, execute arbitrary code with root privileges.

Red Hat would like to thank the X.Org security team for reporting this issue. Upstream acknowledges Pedro Ribeiro as the original reporter.

All xorg-x11-server users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue.

7.288. XORG-X11

7.288.1. RHEA-2013:0301 — xorg-x11 drivers enhancement update

Updated xorg-x11 drivers packages that add numerous enhancements are now available for Red Hat Enterprise Linux 6.

The xorg-x11 drivers packages allow the OS installation software to install all drivers all at once, without having to track which individual drivers are present on each architecture. By installing these packages, it forces all of the individual driver packages to be installed.

The following xorg-x11 drivers packages have been upgraded to their upstream versions to update several legacy GPU drivers:

Table 7.4. Upgraded packages

Package name	Upstream version	BZ number
xorg-x11-drv-apm	1.2.5	835216
xorg-x11-drv-ast	0.97.0	835217
xorg-x11-drv-cirrus	1.5.1	835219
xorg-x11-drv-dummy	0.3.6	835220
xorg-x11-drv-fbdev	0.4.3	835228
xorg-x11-drv-geode	2.11.13	835230
xorg-x11-drv-glint	1.2.8	835231
xorg-x11-drv-i128	1.3.6	835234
xorg-x11-drv-i740	1.3.4	835235
xorg-x11-drv-mach64	6.9.3	835239
xorg-x11-drv-mga	1.6.1	835240
xorg-x11-drv-neomagic	1.2.7	835244
xorg-x11-drv-nv	2.1.20	835246
xorg-x11-drv-openchrome	0.3.0	835247
xorg-x11-drv-r128	6.9.1	835250
xorg-x11-drv-rendition	4.2.5	835251
xorg-x11-drv-s3virge	1.10.6	835252
xorg-x11-drv-savage	2.3.6	835253
xorg-x11-drv-siliconmotion	1.7.7	835254
xorg-x11-drv-sis	0.10.7	835255
xorg-x11-drv-sisusb	0.9.6	835256
xorg-x11-drv-tdfx	1.4.5	835258
xorg-x11-drv-v4l	0.2.0	835260

Package name	Upstream version	BZ number
xorg-x11-drv-trident	1.3.6	835259
xorg-x11-drv-vesa	2.3.2	835261
xorg-x11-drv-vmware	12.0.2	835263
xorg-x11-drv-voodoo	1.2.5	835265
xorg-x11-drv-xgi	1.6.0	835267
xorg-x11-drivers	7.3	835285

Users of xorg-x11-drv are advised to upgrade to these updated packages, which add various enhancements.

7.289. XORG-X11-XKB-UTILS

7.289.1. RHBA-2013:0305 — xorg-x11-xkb-utils bug fix and enhancement update

Updated xorg-x11-xkb-utils packages that fix several bugs and add various enhancements are now available.

The x11-xkb-utils packages provide a set of client-side utilities for XKB, the X11 keyboard extension.

NOTE

The x11-xkb-utils packages have been upgraded to upstream version 7.7, which provides a number of bug fixes and enhancements over the previous version. (BZ#835282, BZ#872057)

All users of x11-xkb-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.290. YABOOT

7.290.1. RHBA-2013:0476 — yaboot bug fix and enhancement update

Updated yaboot packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The yaboot packages provide a boot loader for Open Firmware based PowerPC systems. Yaboot can be used to boot IBM eServer System p machines.

Bug Fix

BZ#871579

Prior to this update, the yaboot loader used by default a maximum block size of 512 bytes in the fdisk partition table. As a consequence, yaboot could not load a kernel in a disk that was formatted using 4 kilobytes partitions. This update extends the MAX_BLOCK_SIZE value to 4 kilobytes to allow for disks that use the advanced format.

Enhancement

BZ#822657

This update adds VLAN Tag support for network boot and installation to allow multiple VLANs in a bridged network to share the same physical network link but maintain isolation.

All users of yaboot are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

7.291. YPBIND

7.291.1. RHBA-2013:0426 — ypbind bug fix update

Updated ypbind packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The ypbind packages provide the ypbind daemon to bind NIS clients to an NIS domain. The ypbind daemon must be running on any machines that run NIS client programs.

Bug Fix

BZ#647495

Prior to this update, ypbind started too late in the boot sequence, which caused problems in some environments, where it needed to be started before netfs. This update changes the priority of the ypbind service. Now, ypbind starts as expected.

All users of ypbind are advised to upgrade to these updated packages, which fix this bug.

7.292. YPSERV

7.292.1. RHBA-2013:0330 — ypserv bug fix update

Updated ypserv packages that fix four bugs are now available for Red Hat Enterprise Linux 6.

The ypserv packages provide the Network Information Service (NIS) server. NIS is a system that provides network information such as login names, passwords, home directories, and group information to all the machines on a network.

Bug Fixes

BZ#790812

Prior to this update, the NIS server was returning "0" (YP_FALSE) instead of "-1" (YP_NOMAP) after a request for a database not present in the server's domain. This behavior caused the autofs mount attempts to fail on Solaris clients. With this update, the return value has been fixed and the autofs mounts no longer fail on Solaris clients.

BZ#816981

Previously, when the crypt() function returned NULL, the yppasswd utility did not properly recognize the return value. This bug has been fixed, and the NULL return values of crypt() are now recognized and reported correctly by yppaswd.

BZ#845283

Previously, the ypserv utility allocated large amounts of virtual memory when parsing XDR requests, but failed to free that memory in case the request was not parsed successfully. Consequently, memory leaks occurred. With this update, a patch has been provided to free the already allocated memory when parsing of a request fails. As a result, the memory leaks no longer occur.

BZ#863952

Previously, the yppush(8) man page did not describe how to change settings of the yppush utility. The manual page has been amended to specify that the settings can be changed in the /var/yp/Makefile file.

All users of ypserv are advised to upgrade to these updated packages, which fix these bugs.

7.293. YUM-RHN-PLUGIN

7.293.1. RHBA-2013:0389 — yum-rhn-plugin bug fix update

Updated yum-rhn-plugin packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The yum-rhn-plugin packages make it possible to receive content from Red Hat Network in yum.

Bug Fixes

BZ#789092

Previously, yum-rhn-plugin ignored the timeout value set for yum. In some scenarios with slow networking, this could cause yum to timeout when communicating with Red Hat Network. Now, yum-rhnplugin abides by the timeout set for all yum repositories.

BZ#802636

Previously, the check-update utility could in certain cases incorrectly return a 0 error code if an error occurred. With this update, "1" is returned if an error occurs.

BZ#824193

Prior to this update, applying automatic updates with the yum-rhn-plugin utility on Red Hat Enterprise Linux 6 system could fail with an "empty transaction" error message. This was because the cached version of yum-rhn-plugin metadata was not up-to-date. With this update, yum-rhn-plugin downloads new metadata if available, ensuring that all packages are available for download.

BZ#830219

Previously, the messaging in yum-rhn-plugin was specific only to Red Hat Network Classic scenarios. This update clarifies what source yum-rhn-plugin is receiving updates from to reduce confusion.

BZ#831234

Prior to this update, yum-rhn-plugin did not correctly try the alternate server URLs provided if the first option failed. This update ensures that fail-over situations are handled correctly.

All users of yum-rhn-plugin are advised to upgrade to these updated packages which fix these bugs.

7.294. YUM

7.294.1. RHBA-2013:0406 — yum bug fix and enhancement update

Updated yum packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

Yum is a command-line utility that allows the user to check for updates and automatically download and install updated RPM packages. **Yum** automatically obtains and downloads dependencies, prompting the user for permission as necessary.

Bug Fixes

BZ#674756

When running the **`yum localinstall`** command, various *requires*, *obsoletes*, and *conflicts* situations were not handled properly and resulted in inconsistent package installations using different **Yum** commands. The underlying source code has been modified and **Yum** resolves all the aforementioned situations properly.

BZ#727553

When trying to execute the **`yum update --skip-broken`** command on the command line, the package dependency resolution never ended. This bug is now fixed and dependencies are resolved successfully after executing the **`yum update --skip-broken`** command.

BZ#802462

After creating a new yum history file, the **`yum history stats`** command failed with a traceback instead of reporting an actual error. This bug is now fixed and when the **`yum history stats`** command fails after creating a new yum history file, it displays an error message.

BZ#815568

Previously, when running the **`yum makecache`** command, followed by the **`yum -C updateinfo`** command, the second command failed to execute because although the updateinfo file had been downloaded by **`yum makecache`** it was uncompressed and treated as unavailable by **`yum -C updateinfo`**. This bug is now fixed and **`yum -C updateinfo`** works as expected in this scenario.

BZ#834159

Previously, when trying to install an obsoleted package from a repository, **Yum** reported *Nothing to do* instead of providing an "obsolete" error message. This bug is now fixed and **Yum** now correctly warns users about obsolete packages.

BZ#840543

Previously, when the **`yum upgrade`** command failed to execute, **Yum** displayed a misleading *Protected multilib versions* error message instead of the accurate one. This bug is now fixed and if **Yum** fails, it displays the correct error message.

BZ#872518

When **Yum** was executed by a regular user, **Yum** downloaded metadata even if the "root" metadata were up-to-date. This bug is now fixed and **Yum** does not download unnecessary data if the "root" metadata are up-to-date.

BZ#809117

A typo in the yum(8) man page has been fixed.

BZ#878335

After a rebase update of the **createrepo** utility, execution of the **`createrepo --update`** command took significantly longer. This update reduces the time for executing the **`createrepo --update`** command.

BZ#737173

Previously, when the **`yum updateinfo`** command, provided by the **yum-security** plug-in, was used, **Yum** did not merge the version information from multiple repositories. This could prevent the latest version of a package that was present in multiple repositories to not be installed. Now, when installing packages from multiple repositories, **Yum** installs only the latest packages available.

BZ#819522

Previously, when trying to reinstall an unavailable package and the execution failed, the exit code had the value of 0. This bug is now fixed and when reinstallation of an unavailable package fails, it returns an exit code with the value of 1.

BZ#820674

Previously, when the **`yum-debug-restore`** command was used to restore multiple installonly packages, **Yum** tried to keep a limit of packages that were installed simultaneously and removed packages that were present in the system. Also, **Yum** restored multiple packages but assumed that just one would be installed. **Yum**'s **`installonly_limit`** configuration now determines what to install and remove correctly when multiple items are installed at once. This is most noticeable when using commands like **`yum shell`** and **`yum-debug-restore`**.

BZ#858844

When using the **`yum.yumBase().update()`** function to specify a package name, version, and/or release of a certain package, the function terminated and failed to update the aforementioned variables. This bug is now fixed and the **`yum.yumBase().update()`** function can be used successfully to specify a package name, version, and release.

BZ#868840

Previously, when trying to resolve dependencies while updating packages that had dependencies, **Yum** entered a loop and no packages were installed after execution of the **`yum update`** command. After this update, the **`yum update`** command now handles packages with obsoleting dependencies as expected.

BZ#880968

Due to an incorrect prioritization of actions performed by **Yum** after entering a command with a syntactically incorrect subcommand, **Yum** performed a series of unnecessary actions before acknowledging the typo. This bug has been fixed and **Yum** performs an immediate syntax check in the described scenario.

BZ#887935

When updateinfo.xml was generated via the update_md.UpdateNotice() method, the yum API only accounted for the "issued date" element and ignored the *updated date* element. Now, the yum API accounts for the "updated date" element and the "updated date" element is displayed in the XML file.

BZ#885159

Previously, users were not notified that different certificate files with the same basename were treated as identical, which could lead to various problems. With this update, **Yum** checks certificate files for such duplicates and displays an error message appropriately.

Enhancements

BZ#684859

Yum plug-ins are now able to set exit codes on any **Yum** operations.

BZ#744335

With this update, **`yum-cron`** is now documented in the yum-cron(8) man page.

BZ#748054

Support for the **`installonlypkgs`** functionality in rhev-hypervisor packages has been added.

Users of yum are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

7.295. ZLIB

7.295.1. RHBA-2013:0398 — zlib bug fix and enhancement update

Updated zlib packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The zlib packages provide a general-purpose lossless data compression library that is used by many different programs.

Bug Fix

BZ#754694

Due to missing information about the zlib version, some applications using zlib could not work properly. The zlib.map version script, which provides version information, has been added to the underlying source code and zlib now works as expected.

Enhancement

BZ#823007

This enhancement optimizes the zlib compression library for IBM System z.

All users of zlib are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

7.296. GNOME-POWER-MANAGER

7.296.1. RHBA-2013:0597 — gnome-power-manager bug fix update

Updated gnome-power-manager packages that fix one bug are now available for Red Hat Enterprise Linux 6.

GNOME Power Manager is a session daemon for the GNOME desktop environment which allows users to manage power settings on their laptop or desktop system.

Bug Fix

BZ#912270

When the power saving features (reduce backlight brightness and dim display when idle) were enabled for the "on battery power" mode and the brightness was adjusted manually, then leaving the laptop idle caused it to forget custom brightness settings. Currently, the "dim display when idle" functionality is disabled by default and laptops remember custom brightness settings.

Users of gnome-power-manager are advised to upgrade to these updated packages, which fix this bug.

7.297. GHOSTSCRIPT

7.297.1. RHBA-2013:0651 — ghostscript bug fix update

Updated ghostscript packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The Ghostscript suite contains utilities for rendering PostScript and PDF documents. Ghostscript translates PostScript code to common, bitmap formats so that the code can be displayed or printed.

Bug Fix

BZ#920251

Due to a bug in a function that copies CIDFontType 2 fonts, document conversion attempts sometimes caused the ps2pdf utility to terminate unexpectedly with a segmentation fault. A patch has been provided to address this bug so that the function now copies fonts properly and ps2pdf no longer crashes in the described scenario.

Users of ghostscript are advised to upgrade to these updated packages, which fix this bug.

7.298. BOOST

7.298.1. RHBA-2013:0692 — boost bug fix update

Updated boost packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The boost packages provide free peer-reviewed portable C++ source libraries with emphasis on libraries which work well with the C++ Standard Library.

Bug Fix

BZ#921441

Users experienced problems when trying to build MongoDB, because the version of boost (1.41), which was installed by default on Red Hat Enterprise Linux 6.4 had codes that violated the compilation rules which the version of GCC (4.4.7) verified. The previous version of GCC did not check for the error in the boost code, and this caused builds to fail for any projects that included the boost/thread.h header file from boost version 1.41. This update fixes this bug by explicitly spelling out the full destructor definition of the boost::exception_ptr class, and the previous version is now fully compatible with version 4.4.7.

Users of boost are advised to upgrade to these updated packages, which fix this bug.

7.299. COREUTILS

7.299.1. RHBA-2013:0703 — coreutils bug fix update

Updated coreutils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The coreutils package contains the core GNU utilities. It is a combination of the old GNU fileutils, sh-utils, and textutils packages.

Bug Fix

BZ#924711

The "tail -f" command uses inotify for tracking changes in files. For remote file systems [-/,] inotify is not available. In the case of unknown file systems, for example panasas, "tail -f" failed instead of falling back to polling. Now, the list of known file systems is updated and "tail -f" is modified to fall back into polling for unknown file systems. As result, "tail -f" now works correctly, even on unknown file systems, with only a warning about the unknown file system and a fall back to polling.

Users of coreutils are advised to upgrade to these updated packages, which fix this bug.

7.299.2. RHBA-2013:0858 — coreutils bug fix update

Updated coreutils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The coreutils package contains the core GNU utilities. It is a combination of the old GNU fileutils, sh-utils, and textutils packages.

Bug Fix

BZ#963327

When parsing the file content and the end of a field was specified using the obsolete key formats (+POS -POS), the sort utility determined the end of the field incorrectly, and therefore produced incorrect output. This update fixes the parsing logic to match the usage of the "-k" option when using these obsolete key formats. The sort utility now returns expected results in this situation.

Users of coreutils are advised to upgrade to these updated packages, which fix this bug.

7.300. ESC

7.300.1. RHBA-2013:0735 — esc bug fix update

Updated esc packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The esc packages contain the Smart Card Manager GUI, which allows user to manage security smart cards. The primary function of the tool is to enroll smart cards, so that they can be used for common cryptographic operations, such as secure e-mail and website access.

Bug Fix

BZ#922646

The ESC utility did not start when the latest 17 series release of the XULRunner runtime environment was installed on the system. This update includes necessary changes to ensure that ESC works as expected with the latest version of XULRunner.

Users of esc are advised to upgrade to these updated packages, which fix this bug.

7.301. GZIP

7.301.1. RHBA-2013:0862 — gzip bug fix update

Updated gzip packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The gzip packages provide the GNU gzip data compression program.

Bug Fix

BZ#963195

The O_NONBLOCK flag was recently added to the open() system call. As a consequence gzip did not prevent opening of parity (PAR) and Ots File List (OFL) files that are managed by the SGI Data Migration Facility (DMF). Processing of such files resulted in gzip aborts or corrupted output files. With this update, if an attempt to read a file with the O_NONBLOCK flag fails with the EAGAIN error code, the file is re-read without O_NONBLOCK. The gzip utility no longer aborts or produce corrupted output files in this situation.

Users of gzip are advised to upgrade to these updated packages, which fix this bug.

7.302. CLUSTER

7.302.1. RHBA-2013:1189 — cluster and gfs2-utils bug fix update

Updated cluster and gfs2-utils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The Red Hat Cluster Manager is a collection of technologies working together to provide data integrity and the ability to maintain application availability in the event of a failure. Using redundant hardware, shared disk storage, power management, and robust cluster communication and application failover mechanisms, a cluster can meet the needs of the enterprise market.

Bug Fix

BZ#1001504

Prior to this update, if one of the gfs2_tool, gfs2_quota, gfs2_grow, or gfs2_jadd commands was killed unexpectedly, a temporary GFS2 metadata mount point used by those tools could be left mounted. The mount point was also not registered in the /etc/mtab file, and so the "umount -a -t gfs2" command would not unmount it. This mount point could prevent systems from rebooting properly, and cause the kernel to panic in cases where it was manually unmounted after the normal GFS2 mount point. This update corrects the problem by creating an mtab entry for the temporary mount point, which unmounts it before exiting when signals are received.

Users of the Red Hat Cluster Manager and GFS2 are advised to upgrade to these updated packages, which fix this bug.

7.302.2. RHBA-2013:1055 — cluster and gfs2-utils bug fix update

Updated cluster and gfs2-utils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The Red Hat Cluster Manager is a collection of technologies working together to provide data integrity and the ability to maintain application availability in the event of a failure. Using redundant hardware, shared disk storage, power management, and robust cluster communication and application failover mechanisms, a cluster can meet the needs of the enterprise market.

Bug Fix

BZ#982700

Previously, the cman init script did not handle its lock file correctly. During a node reboot, this could have caused the node itself to be evicted from the cluster by other members. With this update, the cman init script now handles the lock file correctly, and no fencing action is taken by other nodes of the cluster.

Users of cluster and gfs2-utils are advised to upgrade to these updated packages, which fix this bug.

7.303. CRASH-GCORE-COMMAND

7.303.1. RHBA-2013:1102 — crash-gcore-command bug fix update

Updated crash-gcore-command packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The crash-gcore-command packages contain an extension module for the crash utility that adds a "gcore" command which can create a core dump file of a user-space task that was running in a kernel dumpfile.

Bug Fix

BZ#968897

VDSO and vsyscall pages are not contained in the generated process core dump, due to a backported madvise/MADV_DONTDUMP change in the Red Hat Enterprise Linux 6 kernel. With this update, the VDSO and vsyscall pages are contained in the generated core dump.

Users of crash-gcore-command are advised to upgrade to these updated packages, which fix this bug.

7.304. CUPS

7.304.1. RHBA-2013:1163 — cups bug fix update

Updated cups packages that fix a bug are now available for Red Hat Enterprise Linux 6.

The Common UNIX Printing System (CUPS) provides a portable printing layer for Linux, UNIX, and similar operating systems.

Bug Fix

BZ#994480

For queues using the "ipp" back-end, print jobs containing more than one file were previously treated as though all files were in the same format as the first file in the job when transferring the job to the remote IPP system. This has been corrected by declaring each file as having an unknown document format ("application/octet-stream") for multiple file jobs, and leaving format detection to the remote IPP system.

All users of cups are advised to upgrade to these updated packages, which fix this bug.

7.305. BUSYBOX

7.305.1. RHBA-2013:1165 — busybox bug fix update

Updated busybox packages that fix one bug are now available for Red Hat Enterprise Linux 6.

BusyBox is a binary that combines a large number of common system utilities into a single executable. BusyBox provides replacements for most GNU file utilities, shell utilities, and other command-line tools.

Bug Fix

BZ#981178

Prior to this update, the "mknod" command was unable to create device nodes with a major or minor number larger than 255. Consequently, the kdump utility failed to handle such a device. The underlying source code has been modified, and it is now possible to use the "mknod" command to create device nodes with a major or minor number larger than 255.

Users of busybox are advised to upgrade to these updated packages, which fix this bug.

7.306. AUTHD

7.306.1. RHBA-2013:1168 — authd bug fix update

Updated authd packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The authd package contains a small and fast RFC 1413 Ident Protocol daemon with both xinetd server and interactive modes that supports IPv6 and IPv4 as well as the more popular features of pidentd.

Bug Fix

BZ#994118

If authd encountered a negative UID when reading a /proc/net/tcp entry then it stopped reading at that point, and failed to identify the connection it was looking for. Consequently, authd returned a "non-existent user" error response. With this update, the handling of negative UID values in authd is modified, and authd correctly reports a valid user.

Users of authd are advised to upgrade to these updated packages, which fix this bug.

7.307. DB4

7.307.1. RHBA-2013:1258 — db4 bug fix update

Updated db4 packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The Berkeley Database (Berkeley DB) is a programmatic toolkit that provides embedded database support for both traditional and client/server applications. The Berkeley DB includes B+tree, Extended Linear Hashing, Fixed and Variable-length record access methods, transactions, locking, logging, shared memory caching, and database recovery. The Berkeley DB supports C, C++, Java, and Perl APIs. It is used by many applications, including Python and Perl, so this should be installed on all systems.

Bug Fix

BZ#1005826

Due to an incorrect order of the mutex initialization calls, the rpm utility became unresponsive under certain circumstances, until it was terminated. With this update, the order of mutex initialization calls has been revised. As a result, the rpm utility no longer becomes unresponsive.

Users of db4 are advised to upgrade to these updated packages, which fix this bug.

7.308. CHKCONFIG

7.308.1. RHBA-2013:1276 — chkconfig bug fix update

Updated chkconfig packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The basic system utility chkconfig updates and queries runlevel information for system services.

Bug Fix

BZ#1007372

Previously, the readServices() function returned a wrong value when the /etc/init.d directory was not readable. As a consequence, a segmentation fault occurred. With this update, when the /etc/init.d directory is not readable, the readServices() function properly detects the situation and exits with a failure message. As a result, a segmentation fault no longer occurs.

Users of chkconfig are advised to upgrade to these updated packages, which fix this bug.

7.309. ABRT

7.309.1. RHBA-2013:1289 — abrt bug fix update

Updated abrt packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

ABRT (Automatic Bug Reporting Tool) is a tool to help users detect defects in applications create bug reports with all the information needed by a maintainer to fix it. It uses a plug-in system to extend its functionality. libreport provides an API for reporting different problems in applications to different bug targets, such as Bugzilla, FTP, and Trac.

Bug Fixes

BZ#968345

Previously, attempts to create a Python virtualenv environment using the "--system-site-packages" option resulted in an exception when the site.py() function attempted to load the abrt_exception_handler package. This was caused because Python tried to load the abrt.pth file, in which the abrt_exception_handler module was imported. Since the abrt_exception_handler module was installed under the /usr/lib64 directory and the abrt.pth file was installed under the /usr/lib directory, the site.py() function did not find the required module. This update moves the abrt.pth file to the architecture specific folder, so on 32-bit systems to the /usr/lib/python2.7/site-packages/ directory and on 64-bit systems to the /usr/lib64/python2.7/site-packages/ directory, which corrects this issue.

BZ#1002856

Prior to this update, attempts to use ABRT to report bugs in a Bugzilla server returned the following Remote Procedure Call (RPC) error message: "fatal: RPC failed at server. The requested method 'bugzilla.getBug' was not found." Consequently, Bugzilla tickets were not created, and bugs were not reported. This update changes the code to use the new XMLRPC calls, and with the latest version of ABRT, Bugzilla tickets are created without any problems.

Users of abrt are advised to upgrade to these updated packages, which fix these bugs.

7.310. PCS

7.310.1. RHEA-2013:0655 — pcs bug fix update

Updated pcs packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The pcs packages provide a command-line tool to configure and manage Pacemaker and Corosync tools.

Bug Fix

BZ#915585

The "pcs config" command did not show resources configured as master and slave resources when the configuration of the Pacemaker cluster was reviewed. Consequently, users had to directly analyze the CIB to view the configured master and slave resources and their options. This update provides a patch to address this bug, so the "pcs config" command now shows all resources, including master and slave resources.

Users of pcs are advised to upgrade to these updated packages, which fix this bug.

7.310.2. RHBA-2013:1492 — pcs bug fix and enhancement update

Updated pcs package that fix several bugs and add various enhancements is now available for Red Hat Enterprise Linux 6.

The pcs packages provide a command-line tool to configure and manage the Pacemaker and Corosync tools.

NOTE

The pcs package has been upgraded to upstream version 0.9.90, which provides a number of bug fixes and enhancements over the previous version. (BZ#1003482)

Users of pcs are advised to upgrade to this updated package, which fix these bugs and add these enhancements.

7.311. EXPECT

7.311.1. RHBA-2013:1497 — expect bug fix update

Updated expect packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The "expect" packages contains a tool for automating and testing interactive command line programs and Tk applications. Tcl is a portable and widely used scripting language, while Tk is a graphical toolkit that eases development of text-based and GUI applications.

Bug Fix

BZ#1025202

Prior to this update, the "expect" utility leaked memory when used with the "-re" option, and its memory usage kept increasing indefinitely. A patch has been provided to fix this bug, and "expect" memory usage is now stable and without any leaks.

Users of expect are advised to upgrade to these updated packages, which fix this bug.

7.312. DBUS-GLIB

7.312.1. RHSA-2013:0568 — Important: dbus-glib security update

Updated dbus-glib packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

dbus-glib is an add-on library to integrate the standard D-Bus library with the GLib main loop and threading model.

Security Fix

CVE-2013-0292

A flaw was found in the way dbus-glib filtered the message sender (message source subject) when the "NameOwnerChanged" signal was received. This could trick a system service using dbus-glib (such as fprintd) into believing a signal was sent from a privileged process, when it was not. A local attacker could use this flaw to escalate their privileges.

All dbus-glib users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications linked against dbus-glib, such as fprintd and NetworkManager, must be restarted for this update to take effect.

7.313. JAVA-1.7.0-OPENJDK

7.313.1. RHSA-2013:0602 — Critical: java-1.7.0-openjdk security update

Updated java-1.7.0-openjdk packages that fix two security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

These packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Software Development Kit.

Security Fixes

CVE-2013-0809

An integer overflow flaw was found in the way the 2D component handled certain sample model instances. A specially-crafted sample model instance could cause Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with virtual machine privileges.

CVE-2013-1493

It was discovered that the 2D component did not properly reject certain malformed images. Specially-crafted raster parameters could cause Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with virtual machine privileges.

Note: If the web browser plug-in provided by the icedtea-web package was installed, the issues exposed via Java applets could have been exploited without user interaction if a user visited a malicious website.

This erratum also upgrades the OpenJDK package to IcedTea7 2.3.8. Refer to the NEWS file for further information.

All users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

7.313.2. RHSA-2013:1451 — Critical: java-1.7.0-openjdk security update

Updated java-1.7.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The java-1.7.0-openjdk packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Java Software Development Kit.

Security Fixes

CVE-2013-5782

Multiple input checking flaws were found in the 2D component native image parsing code. A specially crafted image file could trigger a Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with the privileges of the user running the Java Virtual Machine.

CVE-2013-5830

The class loader did not properly check the package access for non-public proxy classes. A remote attacker could possibly use this flaw to execute arbitrary code with the privileges of the user running the Java Virtual Machine.

CVE-2013-5829, CVE-2013-5814, CVE-2013-5817, CVE-2013-5842, CVE-2013-5850, CVE-2013-5838

Multiple improper permission check issues were discovered in the 2D, CORBA, JNDI, and Libraries components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-5809

Multiple input checking flaws were discovered in the JPEG image reading and writing code in the 2D component. An untrusted Java application or applet could use these flaws to corrupt the Java Virtual Machine memory and bypass Java sandbox restrictions.

CVE-2013-5802

The FEATURE_SECURE_PROCESSING setting was not properly honored by the javax.xml.transform package transformers. A remote attacker could use this flaw to supply a crafted XML that would be processed without the intended security restrictions.

CVE-2013-5825, CVE-2013-4002, CVE-2013-5823

Multiple errors were discovered in the way the JAXP and Security components processes XML inputs. A remote attacker could create a crafted XML that would cause a Java application to use an excessive amount of CPU and memory when processed.

CVE-2013-3829, CVE-2013-5840, CVE-2013-5774, CVE-2013-5783, CVE-2013-5820, CVE-2013-5851, CVE-2013-5800, CVE-2013-5849, CVE-2013-5790, CVE-2013-5784

Multiple improper permission check issues were discovered in the Libraries, Swing, JAX-WS, JAXP, JGSS, AWT, Beans, and Scripting components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass certain Java sandbox restrictions.

CVE-2013-5778

It was discovered that the 2D component image library did not properly check bounds when performing image conversions. An untrusted Java application or applet could use this flaw to disclose portions of the Java Virtual Machine memory.

CVE-2013-5804, CVE-2013-5797

Multiple input sanitization flaws were discovered in javadoc. When javadoc documentation was generated from an untrusted Java source code and hosted on a domain not controlled by the code author, these issues could make it easier to perform cross-site scripting attacks.

CVE-2013-5780

Various OpenJDK classes that represent cryptographic keys could leak private key information by including sensitive data in strings returned by toString() methods. These flaws could possibly lead to an unexpected exposure of sensitive key data.

CVE-2013-5772

The Java Heap Analysis Tool (jhat) failed to properly escape all data added into the HTML pages it generated. Crafted content in the memory of a Java program analyzed using jhat could possibly be used to conduct cross-site scripting attacks.

CVE-2013-5803

The Kerberos implementation in OpenJDK did not properly parse KDC responses. A malformed packet could cause a Java application using JGSS to exit.

Note: If the web browser plug-in provided by the icedtea-web package was installed, the issues exposed via Java applets could have been exploited without user interaction if a user visited a malicious website.

All users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

7.313.3. RHSA-2013:0957 — Critical: java-1.7.0-openjdk security update

Updated java-1.7.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

These packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Software Development Kit.

Security Fixes

CVE-2013-2470, CVE-2013-2471, CVE-2013-2472, CVE-2013-2473, CVE-2013-2463, CVE-2013-2465, CVE-2013-2469

Multiple flaws were discovered in the ImagingLib and the image attribute, channel, layout and raster processing in the 2D component. An untrusted Java application or applet could possibly use these flaws to trigger Java Virtual Machine memory corruption.

CVE-2013-2459

Integer overflow flaws were found in the way AWT processed certain input. An attacker could use these flaws to execute arbitrary code with the privileges of the user running an untrusted Java applet or application.

CVE-2013-2448, CVE-2013-2454, CVE-2013-2458, CVE-2013-2457, CVE-2013-2453, CVE-2013-2460

Multiple improper permission check issues were discovered in the Sound, JDBC, Libraries, JMX, and Serviceability components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-2456, CVE-2013-2447, CVE-2013-2455, CVE-2013-2452, CVE-2013-2443, CVE-2013-2446

Multiple flaws in the Serialization, Networking, Libraries and CORBA components can be exploited by an untrusted Java application or applet to gain access to potentially sensitive information.

CVE-2013-2445

It was discovered that the Hotspot component did not properly handle out-of-memory errors. An untrusted Java application or applet could possibly use these flaws to terminate the Java Virtual Machine.

CVE-2013-2444, CVE-2013-2450

It was discovered that the AWT component did not properly manage certain resources and that the ObjectStreamClass of the Serialization component did not properly handle circular references. An untrusted Java application or applet could possibly use these flaws to cause a denial of service.

CVE-2013-2407, CVE-2013-2461

It was discovered that the Libraries component contained certain errors related to XML security and the class loader. A remote attacker could possibly exploit these flaws to bypass intended security mechanisms or disclose potentially sensitive information and cause a denial of service.

CVE-2013-2412

It was discovered that JConsole did not properly inform the user when establishing an SSL connection failed. An attacker could exploit this flaw to gain access to potentially sensitive information.

CVE-2013-2449

It was discovered that GnomeFileTypeDetector did not check for read permissions when accessing files. An untrusted Java application or applet could possibly use this flaw to disclose potentially sensitive information.

CVE-2013-1571

It was found that documentation generated by Javadoc was vulnerable to a frame injection attack. If such documentation was accessible over a network, and a remote attacker could trick a user into visiting a specially-crafted URL, it would lead to arbitrary web content being displayed next to the documentation. This could be used to perform a phishing attack by providing frame content that spoofed a login form on the site hosting the vulnerable documentation.

CVE-2013-1500

It was discovered that the 2D component created shared memory segments with insecure permissions. A local attacker could use this flaw to read or write to the shared memory segment.

Red Hat would like to thank Tim Brown for reporting CVE-2013-1500, and US-CERT for reporting CVE-2013-1571. US-CERT acknowledges Oracle as the original reporter of CVE-2013-1571.

Note: If the web browser plug-in provided by the icedtea-web package was installed, the issues exposed via Java applets could have been exploited without user interaction if a user visited a malicious website.

After installing this update, users of icedtea-web must install RHBA-2013:0959 for icedtea-web to continue functioning.

This erratum also upgrades the OpenJDK package to IcedTea7 2.3.10. Refer to the NEWS file for further information.

7.313.4. RHSA-2013:0751 — Critical: java-1.7.0-openjdk security update

Updated java-1.7.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

These packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Software Development Kit.

Security Fixes

CVE-2013-1569, CVE-2013-2383, CVE-2013-2384

Multiple flaws were discovered in the font layout engine in the 2D component. An untrusted Java application or applet could possibly use these flaws to trigger Java Virtual Machine memory corruption.

CVE-2013-1558, CVE-2013-2422, CVE-2013-2436, CVE-2013-1518, CVE-2013-1557

Multiple improper permission check issues were discovered in the Beans, Libraries, JAXP, and RMI components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-1537

The previous default value of the java.rmi.server.useCodebaseOnly property permitted the RMI implementation to automatically load classes from remotely specified locations. An attacker able to connect to an application using RMI could use this flaw to make the application execute arbitrary code.

CVE-2013-2420

Note: The fix for CVE-2013-1537 changes the default value of the property to true, restricting class loading to the local CLASSPATH and locations specified in the java.rmi.server.codebase property. Refer to Red Hat Bugzilla bug 952387 for additional details.

The 2D component did not properly process certain images. An untrusted Java application or applet could possibly use this flaw to trigger Java Virtual Machine memory corruption.

CVE-2013-2431, CVE-2013-2421, CVE-2013-2423

It was discovered that the Hotspot component did not properly handle certain intrinsic frames, and did not correctly perform access checks and MethodHandle lookups. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-2429, CVE-2013-2430

It was discovered that JPEGImageReader and JPEGImageWriter in the ImageIO component did not protect against modification of their state while performing certain native code operations. An untrusted Java application or applet could possibly use these flaws to trigger Java Virtual Machine memory corruption.

CVE-2013-1488, CVE-2013-2426

The JDBC driver manager could incorrectly call the toString() method in JDBC drivers, and the ConcurrentHashMap class could incorrectly call the defaultReadObject() method. An untrusted Java application or applet could possibly use these flaws to bypass Java sandbox restrictions.

CVE-2013-0401

The sun.awt.datatransfer.ClassLoaderObjectInputStream class may incorrectly invoke the system class loader. An untrusted Java application or applet could possibly use this flaw to bypass certain Java sandbox restrictions.

CVE-2013-2417, CVE-2013-2419

Flaws were discovered in the Network component's InetAddress serialization, and the 2D component's font handling. An untrusted Java application or applet could possibly use these flaws to crash the Java Virtual Machine.

CVE-2013-2424

The MBeanInstantiator class implementation in the OpenJDK JMX component did not properly check class access before creating new instances. An untrusted Java application or applet could use this flaw to create instances of non-public classes.

CVE-2013-2415

It was discovered that JAX-WS could possibly create temporary files with insecure permissions. A local attacker could use this flaw to access temporary files created by an application using JAX-WS.

Note: If the web browser plug-in provided by the icedtea-web package was installed, the issues exposed via Java applets could have been exploited without user interaction if a user visited a malicious website.

This erratum also upgrades the OpenJDK package to IcedTea7 2.3.9. Refer to the NEWS file for further information.

All users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

7.314. JAVA-1.6.0-OPENJDK

7.314.1. RHSA-2013:0770 — Important: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2013-1569, CVE-2013-2383, CVE-2013-2384

Multiple flaws were discovered in the font layout engine in the 2D component. An untrusted Java application or applet could possibly use these flaws to trigger Java Virtual Machine memory corruption.

CVE-2013-1558, CVE-2013-2422, CVE-2013-1518, CVE-2013-1557

Multiple improper permission check issues were discovered in the Beans, Libraries, JAXP, and RMI components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-1537

The previous default value of the java.rmi.server.useCodebaseOnly property permitted the RMI implementation to automatically load classes from remotely specified locations. An attacker able to connect to an application using RMI could use this flaw to make the application execute arbitrary code.

CVE-2013-2420

Note: The fix for CVE-2013-1537 changes the default value of the property to true, restricting class loading to the local CLASSPATH and locations specified in the java.rmi.server.codebase property. Refer to Red Hat Bugzilla bug 952387 for additional details.

The 2D component did not properly process certain images. An untrusted Java application or applet could possibly use this flaw to trigger Java Virtual Machine memory corruption.

CVE-2013-2431, CVE-2013-2421

It was discovered that the Hotspot component did not properly handle certain intrinsic frames, and did not correctly perform MethodHandle lookups. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-2429, CVE-2013-2430

It was discovered that JPEGImageReader and JPEGImageWriter in the ImageIO component did not protect against modification of their state while performing certain native code operations. An untrusted Java application or applet could possibly use these flaws to trigger Java Virtual Machine memory corruption.

CVE-2013-1488, CVE-2013-2426

The JDBC driver manager could incorrectly call the toString() method in JDBC drivers, and the ConcurrentHashMap class could incorrectly call the defaultReadObject() method. An untrusted Java application or applet could possibly use these flaws to bypass Java sandbox restrictions.

CVE-2013-0401

The sun.awt.datatransfer.ClassLoaderObjectInputStream class may incorrectly invoke the system class loader. An untrusted Java application or applet could possibly use this flaw to bypass certain Java sandbox restrictions.

CVE-2013-2417, CVE-2013-2419

Flaws were discovered in the Network component's InetAddress serialization, and the 2D component's font handling. An untrusted Java application or applet could possibly use these flaws to crash the Java Virtual Machine.

CVE-2013-2424

The MBeanInstantiator class implementation in the OpenJDK JMX component did not properly check class access before creating new instances. An untrusted Java application or applet could use this flaw to create instances of non-public classes.

CVE-2013-2415

It was discovered that JAX-WS could possibly create temporary files with insecure permissions. A local attacker could use this flaw to access temporary files created by an application using JAX-WS.

This erratum also upgrades the OpenJDK package to IcedTea6 1.11.10. Refer to the NEWS file for further information.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

7.314.2. RHSA-2013:1014 — Important: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2013-2470, CVE-2013-2471, CVE-2013-2472, CVE-2013-2473, CVE-2013-2463, CVE-2013-2465, CVE-2013-2469

Multiple flaws were discovered in the ImagingLib and the image attribute, channel, layout and raster processing in the 2D component. An untrusted Java application or applet could possibly use these flaws to trigger Java Virtual Machine memory corruption.

CVE-2013-2459

Integer overflow flaws were found in the way AWT processed certain input. An attacker could use these flaws to execute arbitrary code with the privileges of the user running an untrusted Java applet or application.

CVE-2013-2448, CVE-2013-2457, CVE-2013-2453

Multiple improper permission check issues were discovered in the Sound and JMX components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-2456, CVE-2013-2447, CVE-2013-2455, CVE-2013-2452, CVE-2013-2443, CVE-2013-2446

Multiple flaws in the Serialization, Networking, Libraries and CORBA components can be exploited by an untrusted Java application or applet to gain access to potentially sensitive information.

CVE-2013-2445

It was discovered that the Hotspot component did not properly handle out-of-memory errors. An untrusted Java application or applet could possibly use these flaws to terminate the Java Virtual Machine.

CVE-2013-2444, CVE-2013-2450

It was discovered that the AWT component did not properly manage certain resources and that the ObjectStreamClass of the Serialization component did not properly handle circular references. An untrusted Java application or applet could possibly use these flaws to cause a denial of service.

CVE-2013-2407, CVE-2013-2461

It was discovered that the Libraries component contained certain errors related to XML security and the class loader. A remote attacker could possibly exploit these flaws to bypass intended security mechanisms or disclose potentially sensitive information and cause a denial of service.

CVE-2013-2412

It was discovered that JConsole did not properly inform the user when establishing an SSL connection failed. An attacker could exploit this flaw to gain access to potentially sensitive information.

CVE-2013-1571

It was found that documentation generated by Javadoc was vulnerable to a frame injection attack. If such documentation was accessible over a network, and a remote attacker could trick a user into visiting a specially-crafted URL, it would lead to arbitrary web content being displayed next to the documentation. This could be used to perform a phishing attack by providing frame content that spoofed a login form on the site hosting the vulnerable documentation.

CVE-2013-1500

It was discovered that the 2D component created shared memory segments with insecure permissions. A local attacker could use this flaw to read or write to the shared memory segment.

Red Hat would like to thank US-CERT for reporting CVE-2013-1571, and Tim Brown for reporting CVE-2013-1500. US-CERT acknowledges Oracle as the original reporter of CVE-2013-1571.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

7.314.3. RHSA-2013:0605 — Critical: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix two security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability associated with each description below.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2013-0809

An integer overflow flaw was found in the way the 2D component handled certain sample model instances. A specially-crafted sample model instance could cause Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with virtual machine privileges.

CVE-2013-1493

It was discovered that the 2D component did not properly reject certain malformed images. Specially-crafted raster parameters could cause Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with virtual machine privileges.

Note: If your system has not yet been upgraded to Red Hat Enterprise Linux 6.4 and the web browser plug-in provided by the icedtea-web package was installed, the issues exposed via Java applets could have been exploited without user interaction if a user visited a malicious website. Thus, this update has been rated as having critical security impact as a one time exception. The icedtea-web package as provided with Red Hat Enterprise Linux 6.4 uses OpenJDK 7 instead.

This erratum also upgrades the OpenJDK package to IcedTea6 1.11.9. Refer to the NEWS file for further information.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

7.314.4. RHSA-2013:1505 — Important: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The java-1.6.0-openjdk packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Java Software Development Kit.

Security Fixes

CVE-2013-5782

Multiple input checking flaws were found in the 2D component native image parsing code. A specially crafted image file could trigger a Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with the privileges of the user running the Java Virtual Machine.

CVE-2013-5830

The class loader did not properly check the package access for non-public proxy classes. A remote attacker could possibly use this flaw to execute arbitrary code with the privileges of the user running the Java Virtual Machine.

CVE-2013-5829, CVE-2013-5814, CVE-2013-5817, CVE-2013-5842, CVE-2013-5850

Multiple improper permission check issues were discovered in the 2D, CORBA, JNDI, and Libraries components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-5809

Multiple input checking flaws were discovered in the JPEG image reading and writing code in the 2D component. An untrusted Java application or applet could use these flaws to corrupt the Java Virtual Machine memory and bypass Java sandbox restrictions.

CVE-2013-5802

The FEATURE_SECURE_PROCESSING setting was not properly honored by the javax.xml.transform package transformers. A remote attacker could use this flaw to supply a crafted XML that would be processed without the intended security restrictions.

CVE-2013-5825, CVE-2013-4002, CVE-2013-5823

Multiple errors were discovered in the way the JAXP and Security components processes XML inputs. A remote attacker could create a crafted XML that would cause a Java application to use an excessive amount of CPU and memory when processed.

CVE-2013-3829, CVE-2013-5840, CVE-2013-5774, CVE-2013-5783, CVE-2013-5820, CVE-2013-5849, CVE-2013-5790, CVE-2013-5784

Multiple improper permission check issues were discovered in the Libraries, Swing, JAX-WS, JGSS, AWT, Beans, and Scripting components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass certain Java sandbox restrictions.

CVE-2013-5778

It was discovered that the 2D component image library did not properly check bounds when performing image conversions. An untrusted Java application or applet could use this flaw to disclose portions of the Java Virtual Machine memory.

CVE-2013-5804, CVE-2013-5797

Multiple input sanitization flaws were discovered in javadoc. When javadoc documentation was generated from an untrusted Java source code and hosted on a domain not controlled by the code author, these issues could make it easier to perform cross-site scripting attacks.

CVE-2013-5780

Various OpenJDK classes that represent cryptographic keys could leak private key information by including sensitive data in strings returned by toString() methods. These flaws could possibly lead to an unexpected exposure of sensitive key data.

CVE-2013-5772

The Java Heap Analysis Tool (jhat) failed to properly escape all data added into the HTML pages it generated. Crafted content in the memory of a Java program analyzed using jhat could possibly be used to conduct cross-site scripting attacks.

CVE-2013-5803

The Kerberos implementation in OpenJDK did not properly parse KDC responses. A malformed packet could cause a Java application using JGSS to exit.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

7.315. XULRUNNER

7.315.1. RHSA-2013:0614 — Critical: xulrunner security update

Updated xulrunner packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

XULRunner provides the XUL Runtime environment for applications using the Gecko layout engine.

Security Fix

CVE-2013-0787

A flaw was found in the way XULRunner handled malformed web content. A web page containing malicious content could cause an application linked against XULRunner (such as Mozilla Firefox) to crash or execute arbitrary code with the privileges of the user running the application.

Red Hat would like to thank the Mozilla project for reporting this issue. Upstream acknowledges VUPEN Security via the TippingPoint Zero Day Initiative project as the original reporter.

For technical details regarding this flaw, refer to the Mozilla security advisories.

All XULRunner users should upgrade to these updated packages, which correct this issue. After installing the update, applications using XULRunner must be restarted for the changes to take effect.

7.316. THUNDERBIRD

7.316.1. RHSA-2013:1480 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-5590, CVE-2013-5597, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602

Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-5595

It was found that the Thunderbird JavaScript engine incorrectly allocated memory for certain functions. An attacker could combine this flaw with other vulnerabilities to execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-5604

A flaw was found in the way Thunderbird handled certain Extensible Stylesheet Language Transformations (XSLT) files. An attacker could combine this flaw with other vulnerabilities to execute arbitrary code with the privileges of the user running Thunderbird.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Jesse Ruderman, Christoph Diehl, Dan Gohman, Byoungyoung Lee, Nils, and Abhishek Arya as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

For technical details regarding these flaws, refer to the Mozilla security advisories for Thunderbird 17.0.10 ESR.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 17.0.10 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

7.316.2. RHSA-2013:0697 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated for each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-0788

Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-0795

A flaw was found in the way Same Origin Wrappers were implemented in Thunderbird. Malicious content could use this flaw to bypass the same-origin policy and execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-0796

A flaw was found in the embedded WebGL library in Thunderbird. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird. Note: This issue only affected systems using the Intel Mesa graphics drivers.

CVE-2013-0800

An out-of-bounds write flaw was found in the embedded Cairo library in Thunderbird. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-0793

> A flaw was found in the way Thunderbird handled the JavaScript history functions. Malicious content could cause a page to be displayed that has a baseURI pointing to a different site, allowing cross-site scripting (XSS) and phishing attacks.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Olli Pettay, Jesse Ruderman, Boris Zbarsky, Christian Holler, Milan Sreckovic, Joe Drew, Cody Crews, miaubiz, Abhishek Arya, and Mariusz Mlynski as the original reporters of these issues.

Note: All issues except CVE-2013-0800 cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 17.0.5 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

7.316.3. RHSA-2013:1269 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-1718, CVE-2013-1722, CVE-2013-1725, CVE-2013-1730, CVE-2013-1732, CVE-2013-1735, CVE-2013-1736

> Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-1737

> A flaw was found in the way Thunderbird handled certain DOM JavaScript objects. An attacker could use this flaw to make JavaScript client or add-on code make incorrect, security sensitive decisions.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges André Bargull, Scoobidiver, Bobby Holley, Reuben Morais, Abhishek Arya, Ms2ger, Sachin Shinde, Aki Helin, Nils, and Boris Zbarsky as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 17.0.9 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

7.316.4. RHSA-2013:1142 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-1701

Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-1710

A flaw was found in the way Thunderbird generated Certificate Request Message Format (CRMF) requests. An attacker could use this flaw to perform cross-site scripting (XSS) attacks or execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-1709

A flaw was found in the way Thunderbird handled the interaction between frames and browser history. An attacker could use this flaw to trick Thunderbird into treating malicious content as if it came from the browser history, allowing for XSS attacks.

CVE-2013-1713

It was found that the same-origin policy could be bypassed due to the way Uniform Resource Identifiers (URI) were checked in JavaScript. An attacker could use this flaw to perform XSS attacks, or install malicious add-ons from third-party pages.

CVE-2013-1714

It was found that web workers could bypass the same-origin policy. An attacker could use this flaw to perform XSS attacks.

CVE-2013-1717

It was found that, in certain circumstances, Thunderbird incorrectly handled Java applets. If a user launched an untrusted Java applet via Thunderbird, the applet could use this flaw to obtain read-only access to files on the user's local system.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Jeff Gilbert, Henrik Skupin, moz_bug_r_a4, Cody Crews, Federico Lanusse, and Georgi Guninski as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 17.0.8 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

7.316.5. RHSA-2013:0982 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-1682, CVE-2013-1684, CVE-2013-1685, CVE-2013-1686, CVE-2013-1687, CVE-2013-1690

Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-1692

It was found that Thunderbird allowed data to be sent in the body of XMLHttpRequest (XHR) HEAD requests. In some cases this could allow attackers to conduct Cross-Site Request Forgery (CSRF) attacks.

CVE-2013-1693

Timing differences in the way Thunderbird processed SVG image files could allow an attacker to read data across domains, potentially leading to information disclosure.

CVE-2013-1694, CVE-2013-1697

Two flaws were found in the way Thunderbird implemented some of its internal structures (called wrappers). An attacker could use these flaws to bypass some restrictions placed on them. This could lead to unexpected behavior or a potentially exploitable crash.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Gary Kwong, Jesse Ruderman, Andrew McCreight, Abhishek Arya, Mariusz Mlynski, Nils, Johnathan Kuskos, Paul Stone, Boris Zbarsky, and moz_bug_r_a4 as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 17.0.7 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

7.316.6. RHSA-2013:0627 — Important: thunderbird security update

An updated thunderbird package that fixes one security issue is now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fix

CVE-2013-0787

> A flaw was found in the processing of malformed content. Malicious content could cause Thunderbird to crash or execute arbitrary code with the privileges of the user running Thunderbird.

Red Hat would like to thank the Mozilla project for reporting this issue. Upstream acknowledges VUPEN Security via the TippingPoint Zero Day Initiative project as the original reporter.

Note: This issue cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. It could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which corrects this issue. After installing the update, Thunderbird must be restarted for the changes to take effect.

7.316.7. RHSA-2013:0821 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-0801, CVE-2013-1674, CVE-2013-1675, CVE-2013-1676, CVE-2013-1677, CVE-2013-1678, CVE-2013-1679, CVE-2013-1680, CVE-2013-1681

> Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-1670

> A flaw was found in the way Thunderbird handled Content Level Constructors. Malicious content could use this flaw to perform cross-site scripting (XSS) attacks.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Christoph Diehl, Christian Holler, Jesse Ruderman, Timothy Nikkel, Jeff Walden, Nils, Ms2ger, Abhishek Arya, and Cody Crews as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 17.0.6 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

7.317. FIREFOX

7.317.1. RHSA-2013:1476 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2013-5590, CVE-2013-5597, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to terminate unexpectedly or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-5595

It was found that the Firefox JavaScript engine incorrectly allocated memory for certain functions. An attacker could combine this flaw with other vulnerabilities to execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-5604

A flaw was found in the way Firefox handled certain Extensible Stylesheet Language Transformations (XSLT) files. An attacker could combine this flaw with other vulnerabilities to execute arbitrary code with the privileges of the user running Firefox.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Jesse Ruderman, Christoph Diehl, Dan Gohman, Byoungyoung Lee, Nils, and Abhishek Arya as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories> for Firefox 17.0.10 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 17.0.10 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

7.317.2. RHSA-2013:1140 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2013-1701

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-1710

A flaw was found in the way Firefox generated Certificate Request Message Format (CRMF) requests. An attacker could use this flaw to perform cross-site scripting (XSS) attacks or execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-1709

A flaw was found in the way Firefox handled the interaction between frames and browser history. An attacker could use this flaw to trick Firefox into treating malicious content as if it came from the browser history, allowing for XSS attacks.

CVE-2013-1713

It was found that the same-origin policy could be bypassed due to the way Uniform Resource Identifiers (URI) were checked in JavaScript. An attacker could use this flaw to perform XSS attacks, or install malicious add-ons from third-party pages.

CVE-2013-1714

It was found that web workers could bypass the same-origin policy. An attacker could use this flaw to perform XSS attacks.

CVE-2013-1717

It was found that, in certain circumstances, Firefox incorrectly handled Java applets. If a user launched an untrusted Java applet via Firefox, the applet could use this flaw to obtain read-only access to files on the user's local system.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Jeff Gilbert, Henrik Skupin, moz_bug_r_a4, Cody Crews, Federico Lanusse, and Georgi Guninski as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 17.0.8 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 17.0.8 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

7.317.3. RHSA-2013:0981 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2013-1682, CVE-2013-1684, CVE-2013-1685, CVE-2013-1686, CVE-2013-1687, CVE-2013-1690

> Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-1692

> It was found that Firefox allowed data to be sent in the body of XMLHttpRequest (XHR) HEAD requests. In some cases this could allow attackers to conduct Cross-Site Request Forgery (CSRF) attacks.

CVE-2013-1693

> Timing differences in the way Firefox processed SVG image files could allow an attacker to read data across domains, potentially leading to information disclosure.

CVE-2013-1694, CVE-2013-1697

> Two flaws were found in the way Firefox implemented some of its internal structures (called wrappers). An attacker could use these flaws to bypass some restrictions placed on them. This could lead to unexpected behavior or a potentially exploitable crash.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Gary Kwong, Jesse Ruderman, Andrew McCreight, Abhishek Arya, Mariusz Mlynski, Nils, Johnathan Kuskos, Paul Stone, Boris Zbarsky, and moz_bug_r_a4 as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 17.0.7 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 17.0.7 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

7.317.4. RHSA-2013:0696 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with the description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2013-0788

> Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-0795

A flaw was found in the way Same Origin Wrappers were implemented in Firefox. A malicious site could use this flaw to bypass the same-origin policy and execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-0796

A flaw was found in the embedded WebGL library in Firefox. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox. Note: This issue only affected systems using the Intel Mesa graphics drivers.

CVE-2013-0800

An out-of-bounds write flaw was found in the embedded Cairo library in Firefox. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-0793

A flaw was found in the way Firefox handled the JavaScript history functions. A malicious site could cause a web page to be displayed that has a baseURI pointing to a different site, allowing cross-site scripting (XSS) and phishing attacks.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Olli Pettay, Jesse Ruderman, Boris Zbarsky, Christian Holler, Milan Sreckovic, Joe Drew, Cody Crews, miaubiz, Abhishek Arya, and Mariusz Mlynski as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 17.0.5 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 17.0.5 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

7.317.5. RHSA-2013:1268 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2013-1718, CVE-2013-1722, CVE-2013-1725, CVE-2013-1730, CVE-2013-1732, CVE-2013-1735, CVE-2013-1736

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-1737

A flaw was found in the way Firefox handled certain DOM JavaScript objects. An attacker could use this flaw to make JavaScript client or add-on code make incorrect, security sensitive decisions.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges André Bargull, Scoobidiver, Bobby Holley, Reuben Morais, Abhishek Arya, Ms2ger, Sachin Shinde, Aki Helin, Nils, and Boris Zbarsky as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 17.0.9 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 17.0.9 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

7.317.6. RHSA-2013:0820 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2013-0801, CVE-2013-1674, CVE-2013-1675, CVE-2013-1676, CVE-2013-1677, CVE-2013-1678, CVE-2013-1679, CVE-2013-1680, CVE-2013-1681

> Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-1670

> A flaw was found in the way Firefox handled Content Level Constructors. A malicious site could use this flaw to perform cross-site scripting (XSS) attacks.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Christoph Diehl, Christian Holler, Jesse Ruderman, Timothy Nikkel, Jeff Walden, Nils, Ms2ger, Abhishek Arya, and Cody Crews as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 17.0.6 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 17.0.6 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

7.318. MYSQL

7.318.1. RHSA-2013:0772 — Important: mysql security update

Updated mysql packages that fix several security issues are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) and many client programs and libraries.

Security Fix

CVE-2012-5614, CVE-2013-1506, CVE-2013-1521, CVE-2013-1531, CVE-2013-1532, CVE-2013-1544, CVE-2013-1548, CVE-2013-1552, CVE-2013-1555, CVE-2013-2375, CVE-2013-2378, CVE-2013-2389, CVE-2013-2391, CVE-2013-2392

> This update fixes several vulnerabilities in the MySQL database server. Information about these flaws can be found on the Oracle Critical Patch Update Advisory page.

These updated packages upgrade MySQL to version 5.1.69. For more information, refer to the MYSQL release notes located here:

http://dev.mysql.com/doc/relnotes/mysql/5.1/en/news-5-1-68.html

http://dev.mysql.com/doc/relnotes/mysql/5.1/en/news-5-1-69.html

All MySQL users should upgrade to these updated packages, which correct these issues. After installing this update, the MySQL server daemon (mysqld) will be restarted automatically.

7.319. OPENSWAN

7.319.1. RHSA-2013:0827 — Important: openswan security update

Updated openswan packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

Openswan is a free implementation of Internet Protocol Security (IPsec) and Internet Key Exchange (IKE). IPsec uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. When using Opportunistic Encryption, Openswan's pluto IKE daemon requests DNS TXT records to obtain public RSA keys of itself and its peers.

Security Fix

CVE-2013-2053

> A buffer overflow flaw was found in Openswan. If Opportunistic Encryption were enabled ("oe=yes" in "/etc/ipsec.conf") and an RSA key configured, an attacker able to cause a system to perform a DNS lookup for an attacker-controlled domain containing malicious records (such as by sending an email that triggers a DKIM or SPF DNS record lookup) could cause Openswan's pluto IKE daemon to crash or, potentially, execute arbitrary code with root privileges. With "oe=yes" but no RSA key configured, the issue can only be triggered by attackers on the local network who can control the reverse DNS entry of the target system. Opportunistic Encryption is disabled by default.

This issue was discovered by Florian Weimer of the Red Hat Product Security Team.

All users of openswan are advised to upgrade to these updated packages, which contain backported patches to correct this issue. After installing this update, the ipsec service will be restarted automatically.

7.320. HAPROXY

7.320.1. RHSA-2013:1120 — Moderate: haproxy security update

An updated haproxy package that fixes one security issue is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

HAProxy provides high availability, load balancing, and proxying for TCP and HTTP-based applications.

Security Fix

CVE-2013-2175

> A flaw was found in the way HAProxy handled requests when the proxy's configuration ("/etc/haproxy/haproxy.cfg") had certain rules that use the hdr_ip criterion. A remote attacker could use this flaw to crash HAProxy instances that use the affected configuration.

Red Hat would like to thank HAProxy upstream for reporting this issue. Upstream acknowledges David Torgerson as the original reporter.

HAProxy is released as a Technology Preview in Red Hat Enterprise Linux 6. More information about Red Hat Technology Previews is available at https://access.redhat.com/support/offerings/techpreview/.

All users of haproxy are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

7.320.2. RHSA-2013:0868 — Moderate: haproxy security update

An updated haproxy package that fixes one security issue is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

HAProxy provides high availability, load balancing, and proxying for TCP and HTTP-based applications.

Security Fix

CVE-2013-1912

> A buffer overflow flaw was found in the way HAProxy handled pipelined HTTP requests. A remote attacker could send pipelined HTTP requests that would cause HAProxy to crash or, potentially, execute arbitrary code with the privileges of the user running HAProxy. This issue only affected systems using all of the following combined configuration options: HTTP keep alive enabled, HTTP keywords in TCP inspection rules, and request appending rules.

Red Hat would like to thank Willy Tarreau of HAProxy upstream for reporting this issue. Upstream acknowledges Yves Lafon from the W3C as the original reporter.

HAProxy is released as a Technology Preview in Red Hat Enterprise Linux 6. More information about Red Hat Technology Previews is available at https://access.redhat.com/support/offerings/techpreview/

All users of haproxy are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

7.321. POLKIT

7.321.1. RHSA-2013:1270 — Important: polkit security update

Updated polkit packages that fix one security issue are now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

PolicyKit is a toolkit for defining and handling authorizations.

Security Fix

CVE-2013-4288

> A race condition was found in the way the PolicyKit pkcheck utility checked process authorization when the process was specified by its process ID via the --process option. A local user could use this flaw to bypass intended PolicyKit authorizations and escalate their privileges.

Note: Applications that invoke pkcheck with the --process option need to be modified to use the pid,pid-start-time,uid argument for that option, to allow pkcheck to check process authorization correctly.

Red Hat would like to thank Sebastian Krahmer of the SUSE Security Team for reporting this issue.

All polkit users should upgrade to these updated packages, which contain a backported patch to correct this issue. The system must be rebooted for this update to take effect.

7.322. RTKIT

7.322.1. RHSA-2013:1282 — Important: rtkit security update

An updated rtkit package that fixes one security issue is now available for Red Hat Enterprise Linux 6.

The Red Hat Security Response Team has rated this update as having important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

RealtimeKit is a D-Bus system service that changes the scheduling policy of user processes/threads to SCHED_RR (that is, realtime scheduling mode) on request. It is intended to be used as a secure mechanism to allow real-time scheduling to be used by normal user processes.

Security Fix

CVE-2013-4326

> It was found that RealtimeKit communicated with PolicyKit for authorization using a D-Bus API that is vulnerable to a race condition. This could have led to intended PolicyKit authorizations being bypassed. This update modifies RealtimeKit to communicate with PolicyKit via a different API that is not vulnerable to the race condition.

All rtkit users are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

APPENDIX A. REVISION HISTORY

Revision 1-1.37	**Thu Jan 21 2016**	**Lenka Špačková**

Added information about the removed systemtap-grapher package to the Deprecated Functionality Chapter.

Revision 1-1.36	**Wed Jun 04 2014**	**Miroslav Svoboda**

Republished to include the latest description changes in the RHSA-2014:0634 kernel advisory.

Revision 1-1.33	**Wed Mar 12 2014**	**Miroslav Svoboda**

Republished to include the latest description changes in the RHSA-2014:0284 kernel advisory.

Revision 1-1.32	**Fri Jan 24 2014**	**Milan Navrátil**

Republished to include Section 7.103.14, “RHBA-2013:0093 — kernel bug fix update” .

Revision 1-1.30	**Tue Dec 02 2013**	**Miroslav Svoboda**

Republished to include the latest description changes in the RHBA-2013-1770 kernel advisory.

Revision 1-1.29	**Fri Nov 29 2013**	**Miroslav Svoboda**

Republished to include Section 7.103.4, “ RHBA-2013:1770 — kernel bug fix and enhancement update ” and several other z-stream errata.

Revision 1-1.26	**Wed Oct 16 2013**	**Miroslav Svoboda**

Republished to include Section 7.103.5, “ RHSA-2013:1436 — Moderate: kernel security and bug fix update ” .

Revision 1-1.25	**Wed Aug 28 2013**	**Miroslav Svoboda**

Republished to include Section 7.103.6, “ RHSA-2013:1173 — Important: kernel security and bug fix update ” .

Revision 1-1.22	**Tue Jul 23 2013**	**Miroslav Svoboda**

Republished to include Section 7.103.7, “ RHSA-2013:1051 — Moderate: kernel security and bug fix update ” .

Revision 1-1.21	**Tue Jun 25 2013**	**Eliška Slobodová**

Republished to include a samba4 known issue.

Revision 1-1.20	**Tue Jun 11 2013**	**Miroslav Svoboda**

Republished to include Section 7.103.8, “ RHSA-2013:0911 — Important: kernel security, bug fix and enhancement update ” .

Revision 1-1.17	**Fri May 24 2013**	**Eliška Slobodová**

Removed the numad package from Technology Previews as it is now fully supported.

Revision 1-1.15	**Fri Apr 26 2013**	**Eliška Slobodová**

Republished the book to include a known issue.

Revision 1-1.13	**Fri Mar 22 2013**	**Miroslav Svoboda**

Republished to include Section 7.103.9, “ RHSA-2013:0744 — Important: kernel security and bug fix update ” .

Revision 1-1.11	**Fri Mar 22 2013**	**Martin Prpič**

Republished to include Section 7.128.1, “ RHBA-2013:0664 — libvirt bug fix and enhancement update ” .

Revision 1-1.10	**Tue Mar 12 2013**	**Eliška Slobodová**

Republished the book to include the RHSA-2013:0630 kernel advisory and a new known issue, BZ# 918647.

Revision 1-1.2	**Mon Feb 25 2013**	**Martin Prpič**

Fixed incorrect `lpfc` driver version: BZ#915284.

Revision 1-1.1	**Thu Feb 21 2013**	**Eliška Slobodová**

Release of the Red Hat Enterprise Linux 6.4 Technical Notes.