Red Hat Enterprise Linux 6

6.6 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 6.6

Edition 6

Last Updated: 2017-10-20

Red Hat Enterprise Linux 6 6.6 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 6.6
Edition 6

Red Hat Customer Content Services

Legal Notice

Abstract

The Red Hat Enterprise Linux 6.6 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 6.5 and minor release Red Hat Enterprise Linux 6.6.

Table of Contents

PREFACE

The *Red Hat Enterprise Linux 6.6 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 6.5 and minor release Red Hat Enterprise Linux 6.6.

For system administrators and others planning Red Hat Enterprise Linux 6.6 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 6.6 Technical Notes* provide a single, organized source for change tracking and compliance testing.

For every user, the *Red Hat Enterprise Linux 6.6 Technical Notes* provide details of what has changed in this new release.

CHAPTER 1. RED HAT ENTERPRISE LINUX 6.6 INTERNATIONAL LANGUAGES

Red Hat Enterprise Linux 6.6 supports installation of multiple languages and changing of languages based on your requirements.

The following languages are supported in Red Hat Enterprise Linux 6.6:

- East Asian Languages - Japanese, Korean, Simplified Chinese, and Traditional Chinese
- European Languages - English, German, Spanish, French, Portuguese Brazilian, and Russian,
- Indic Languages - Assamese, Bengali, Gujarati, Hindi, Kannada, Malayalam, Marathi, Oriya, Punjabi, Tamil, and Telugu

The table below summarizes the currently supported languages, their locales, default fonts installed and packages required for some of the supported languages

Table 1.1. Red Hat Enterprise Linux 6 International Languages

Territory	Language	Locale	Fonts	Package Names
China	Simplified Chinese	zh_CN.UTF-8	AR PL (ShanHeiSun and Zenkai) Uni	fonts-chinese, scim-pinyin, scim-tables
Japan	Japanese	ja_JP.UTF-8	Sazanami (Gothic and Mincho)	fonts-japanese, scim-anthy
Korea	Hangul	ko_KR.UTF-8	Baekmuk (Batang, Dotum, Gulim, Headline)	fonts-korean, scim-hangul
Taiwan	Traditional Chinese	zh_TW.UTF-8	AR PL (ShanHeiSun and Zenkai) Uni	fonts-chinese, scim-chewing, scim-tables
Brazil	Portuguese	pt_BR.UTF-8	standard latin fonts	
France	French	ft_FR.UTF-8	standard latin fonts	
Germany	German	de_DE.UTF-8	standard latin fonts	
Italy	Italy	it_IT.UTF-8	standard latin fonts	
Russia	Russian	ru_RU.UTF-8	KOI8-R, fonts-KOI8-R-100dpi, fonts-KOI8-R-75dpi and xorg-x11-fonts-cyrillic	fonts-KO18-R, fonts-KO18-R-100 dpi,fonts-KO18-R-75dpi, xorg-x11-fonts-cyrillic

Territory	Language	Locale	Fonts	Package Names
Spain	Spanish	es_ES.UTF-8	standard latin fonts	
India	Assamese	as_IN.UTF-8	Lohit Bengali	fonts-bengali, scim-m17n, m17n-db-assamese
	Bengali	bn_IN.UTF-8	Lohit Bengali	fonts-bengali, scim-m17n, m17n-db-bengali
	Gujarati	gu_IN.UTF-8	Lohit Gujarati	fonts-gujarati, scim-m17n, m17n-db-gujarati
	Hindi	hi_IN.UTF-8	Lohit Hindi	fonts-hindi, scim-m17n, m17n-db-hindi
	Kannada	kn_IN.UTF-8	Lohit Kannada	fonts-kannada, scim-m17n, m17n-db-kannada
	Malayalam	ml_IN.UTF-8	Lohit Malayalam	fonts-malayalam, scim-m17n, m17n-db-malayalam
	Marathi	mr_IN.UTF-8	Lohit Hindi	fonts-hindi, scim-m17n, m17n-db-marathi
	Oriya	or_IN.UTF-8	Lohit Oriya	fonts-oriya, scim-m17n, m17n-db-oriya
	Punjabi	pa_IN.UTF-8	Lohit Punjabi	fonts-punjabi, scim-m17n, m17n-db-punjabi
	Tamil	ta_IN.UTF-8	Lohit Tamil	fonts-tamil, scim-m17n, m17n-db-tamil
	Telugu	te_IN.UTF-8	Lohit Telugu	fonts-telugu, scim-m17n, m17n-db-telugu

CHAPTER 2. 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 6.6. These changes include added or updated **procfs** entries, **sysfs** default values, boot parameters, kernel configuration options, or any noticeable behavior changes.

MemAvailable

Using this parameter provides an estimate of how much memory is available for starting new applications without swapping. However, unlike the data provided by the Cache or Free fields, MemAvailable takes into account page cache and also that not all reclaimable slab will be reclaimable due to items being in use.

overcommit_kbytes

This parameter allows the user to determine the specific number of kilobytes of physicial RAM that a committed address space is not permitted to exceed when the overcommit_memory parameter is set to "2". Therefore, overcommit_bytes works as the counterpart to the overcommit_ratio, and setting one automatically disables the other.

meminfo_legacy_layout

Setting this parameter to a non-zero value will disable the reporting of new entries introduced to /proc/meminfo and the kernel will keep the legacy (2.6.32) layout when reporting data through that interface. Note that the default value is "1". This parameter is available to Red Hat Enterprise Linux 6 only, for reasons of retroactive compatibility.

disable_cpu_apicid

This parameter allows the kdump kernel to disable BSP during boot and then to successfully boot up with multiple processors. This resolves the problem of lack of available interrupt vectors for systems with a high number of devices and ensures that kdump can now successfully capture a core dump on these systems.

earlyprintk

Previously usable only for VGA hardware, this parameter now supports the "efi" value, which allows users to debug early booting issues on EFI hardware.

edac_report

By setting the value of this parameter to "on" or "off", the user can enable or disable the Error Detection and Correction (EDAC) module to report hardware events. It is also possible to make EDAC impossible to be overridden by a higher-priority module by using the "force" value. The default value of this parameter is "on".

intel_iommu

This parameter enables the user to turn off the support of large pages, using the "sp_off" value. By default, however, large pages are supported as long as the Intel input/output management unit (IOMMU) meets the requirements.

nfs.recover_lost_locks

Previously, NFSv4 clients could resume expired or lost file locks. Nevertheless, this sometimes resulted in file corruption if the file was modified in the meantime. Therefore, recovering these locks

has been disabled, but can be enabled by changing the value of the above parameter from "0" to "1". Note, however, that doing so still carries a risk of data corruption.

CHAPTER 3. DEVICE DRIVERS

This chapter provides a comprehensive listing of all device drivers which were updated in Red Hat Enterprise Linux 6.6.

Storage Drivers

- The **bnx2i** driver has been upgraded to version 2.7.10.1.
- The **hpsa** driver has been upgraded to version 3.4.4-1-RH1.
- The **bfa** driver has been upgraded to version 3.2.23.0.
- The **mvsas** driver has been upgraded to the latest upstream version.
- The **qla4xxx** driver has been upgraded to version 5.03.00.00.06.06-k0.
- The **mpt2sas** driver has been upgraded to version 16.100.00.00.
- The **qla2xxx** driver has been upgraded to version 8.07.00.08.06.6-k.
- The **bnx2fc** driver has been upgraded to version 2.4.2.
- The **lpfc** driver has been upgraded to version 10.2.8020.1.
- Device driver ID changes have been implemented for the **pm80xx** driver to support series 8 controllers.
- Configuration parameters have been updated for the **be2iscsi** driver to support Dual Chute mode.
- The version string has been changed for the **hpsa** driver.
- The **megaraid_sas** driver has been upgraded to the latest upstream version. In addition, its changelog has been updated.

Network Drivers

- The Brocade **BNA** driver has been updated to version 3.2.23.0.
- The **qlcnic** driver has been updated to version 5.3.59.
- The Emulex **be2net** driver has been updated to version 10.2.
- The **bnx2x** driver has been updated to utilize the version 7.8.19 firmware.
- The **qlge** driver has been updated to version 1.00.00.34.
- A fix has been implemented for the **igbvf** driver to properly handle 32-bit DMA masks.
- A fix has been implemented for the **igb** driver to properly handle 32-bit DMA masks.
- The **bnx2** driver has been updated to version 2.2.4.
- All Mellanox **mlx** drivers have been updated to their latest upstream versions.

- The **i40evf** driver has been updated to its latest upstream version.
- The **i40e** driver has been updated to its latest upstream version.
- The **netxen** driver has been updated to version 4.0.82.
- The **enic** driver has been updated to support the Cisco low latency network interface controller.
- The **ixbevf** driver has been updated to the latest upstream version.
- The **ixbe** driver has been updated to the latest upstream version.
- The **tg3** driver has been updated to version 3.137.
- Product naming has been updated for the **sfc** driver.
- The General Public License header and Copyright information have been updated for the **e1000e** driver.

Miscellaneous Drivers

- A cache device mapper target has been added to the **dm** driver.
- The **cnic** driver has been updated to version 2.5.20. In addition, its copyright year has been updated.
- The **sb_edac** has been updated to support the Haswell microarchitecture-based systems.
- The InfiniBand **iser** driver has been updated to version 1.3.
- The InfiniBand **srp** driver has been updated to the latest upstream version. In addition, its release date information has been updated.
- The InfiniBand **qib** driver has been updated to support Direct Connect Architecture.
- The **intel_pstate** driver has been updated to support Haswell CPU models.
- The **rtsx** driver has been updated to support the Realtek RTL8411B Ethernet controller.
- The **openvswitch** driver has been updated to support the Stream Control Transmission Protocol.
- The **Direct Rendering Manager (DRM)** module has been updated to version 3.14.2.
- The **cnic** driver has been updated to version 2.5.20. In addition, its copyright year has been updated.
- The **hid-multitouch** module has been updated to the latest upstream version, adding the support for Windows 8-certified touchescreens.
- An update notifier for changes of Open Firmware device tree properties has been implemented into the **pseries** driver.
- The **DRBG** module has been implemented, introducing a SP800-90A Deterministic Random Bit Generator.

- Accelerated computation for the PCLMULQDQ instruction has been implemented into the **crct10dif** module.
- The **ccis** driver has been updated to the latest upstream version.
- The **NVMe** driver has been updated to include device and queue numbers in interrupt names.
- MCE decoding support has been expanded for the **mce_amd** driver.

CHAPTER 4. TECHNOLOGY PREVIEWS

This chapter provides a list of all available Technology Previews in Red Hat Enterprise Linux 6.6.

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

dm-era Device Mapper

The device-mapper-persistent-data package now provides tools to help use the new **dm-era** device mapper functionality released as a Technology Preview. The **dm-era** functionality keeps track of which blocks on a device were written within user-defined periods of time called an **era**. This functionality allows backup software to track changed blocks or restore the coherency of a cache after reverting changes.

dm-cache device-mapper Target

The **dm-cache** device-mapper target, which allows fast storage devices to act as a cache for slower storage devices, has been added as a Technology Preview. See the lvmcache manual page for more information.

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-3.6.9-164

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 and later, SIGAR is considered a Technology Preview package.

Package: sigar-1.6.5-0.4.git58097d9

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-2.6.32-431

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: lvm2-2.02.100-8

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

4.2. NETWORKING

Mellanox SR-IOV Support

Single Root I/O Virtualization (SR-IOV) is now supported as a Technology Preview in the Mellanox **`libmlx4`** library and the following drivers:

- **`mlx_core`**
- **`mlx4_ib`** (InfiniBand protocol)
- **`mlx_en`** (Ethernet protocol)

Package: kernel-2.6.32-335

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

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-2.6.32-431

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-0.2-1

4.3. CLUSTERING AND HIGH AVAILABILITY

luci support for fence_sanlock

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

Package: luci-0.26.0-48

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-3.0.12.1-59

4.4. AUTHENTICATION

Apache Modules for External Authentication

A set of Apache modules has been added to Red Hat Enterprise Linux 6.6 as a Technology Preview. The `mod_authnz_pam`, `mod_intercept_form_submit`, and `mod_lookup_identity` Apache modules in the respective packages can be used by Web applications to achieve tighter interaction with external authentication and identity sources, such as Identity Management in Red Hat Enterprise Linux.

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. Red Hat Enterprise Linux 6.4 and later includes SSSD enhanced to allow the users to select the DIR: cache for users that are logging in via SSSD. This feature is introduced as a Technology Preview.

Package: sssd-1.9.2-129

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-2.6.32-431

4.7. KERNEL

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-2.6.32-431

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-3.1.5-35

4.8. VIRTUALIZATION

Red Hat Enterprise Linux 6.6 Hosted as a Generation 2 Virtual Machine

As a Technology Preview, Red Hat Enterprise Linux 6.6 can be used as a generation 2 virtual machine in the Microsoft Hyper-V Server 2012 R2 host. In addition to the functions supported in the previous generation, generation 2 provides new functions on a virtual machine; for example: boot from a SCSI virtual hard disk, and UEFI firmware support.

CHAPTER 5. DEPRECATED FUNCTIONALITY

Btrfs file system

B-tree file system (Btrfs) is considered deprecated for Red Hat Enterprise Linux 6. Btrfs was previously provided as a Technology Preview, available on AMD64 and Intel 64 architectures.

eCryptfs file system

eCryptfs file system, which was previously available as a Technology Preview, is considered deprecated for Red Hat Enterprise Linux 6.

`mingw` component, BZ#1063396

Following the deprecation of Matahari packages in Red Hat Enterprise Linux 6.3, at which time the mingw packages were noted as deprecated, and the subsequent removal of Matahari packages from Red Hat Enterprise Linux 6.4, the mingw packages are now being removed from Red Hat Enterprise Linux 6.6.

The mingw packages will no longer be shipped in future Red Hat Enterprise Linux 6 minor releases, nor will they receive security-related updates. Consequently, users are advised to uninstall any earlier releases of the mingw packages from their Red Hat Enterprise Linux 6 systems.

`virtio-win` component, BZ#1001981

The VirtIO SCSI driver has been removed from the virtio-win package and is no longer supported on Microsoft Windows Server 2003 platform.

`qemu-kvm` component

The qemu-guest-agent-win32 package is no longer shipped as part of the qemu-kvm package. The Windows guest agent is now delivered in the Supplementary channel together with other Windows components, for example, virtio-win drivers.

`fence-agents` component

Prior to Red Hat Enterprise Linux 6.5 release, the Red Hat Enterprise Linux High Availability Add-On was considered fully supported on certain VMware ESXi/vCenter versions in combination with the fence_scsi fence agent. Due to limitations in these VMware platforms in the area of SCSI-3 persistent reservations, the **`fence_scsi`** fencing agent is no longer supported on any version of the Red Hat Enterprise Linux High Availability Add-On in VMware virtual machines, except when using iSCSI-based storage. See the Virtualization Support Matrix for High Availability for full details on supported combinations:

https://access.redhat.com/site/articles/29440

Users using **`fence_scsi`** on an affected combination can contact Red Hat Global Support Services for assistance in evaluating alternative configurations or for additional information.

`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.

- 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 6. KNOWN ISSUES

6.1. INSTALLATION

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

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.

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.

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.

6.2. ENTITLEMENT

`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.

6.3. 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.

6.4. 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.

qemu-kvm component, BZ#1027582

Microsoft Windows 8.1 and Microsoft Windows Server 2012 R2 require some CPU features, for example Compare Exchange 8Byte and Compare Exchange 16Byte, which are not present in all qemu-kvm CPU models. As a consequence, Microsoft Windows 8.1 and Microsoft Windows Server 2012 R2 guests do not boot if they use the following CPU model definitions: Opteron_G1, Conroe, and kvm64. To work around this problem, use CPU models that include the features required by Microsoft Windows 8.1 and Microsoft Windows Server 2012 R2, for example Penryn, Nehalem, Westmere, SandyBridge, Haswell, Opteron_G2, Opteron_G3, Opteron_G4, or Opteron_G5.

kernel component, BZ#1025868

KVM (Kernel-based Virtual Machine) cannot handle the values written in the MSR_IA32_MC4_CTL preprocessor macro by Linux guests when using some CPU or family model values. As a consequence, kernel panic occurs when booting on Red Hat Enterprise Linux 4 guests. Red Hat Enterprise Linux 5 and later incorrectly ignore certain exceptions so they are not affected. To work around this problem, use the **nomce** kernel command-line option on the guest, which disables MCE support. Alternatively, use a different CPU model name on the virtual machine configuration. As a result, guests boot as expected and kernel panic no longer occurs.

kernel component, BZ#1035571

After alternately hot plugging and unplugging SCSI disks more then three times, the guest displays information about the incorrect SCSI disk that has been removed. The work around this problem, the guest can need to wait for up to three minutes before it can rescan the bus to obtain correct information of the changed device.

virtio-win component

When upgrading the **NetKVM** driver through the Windows Device Manager, the old registry values are not removed. As a consequence, for example, non-existent parameters may be available.

qemu-kvm component

When working with very large images (larger than 2TB) created with very small cluster sizes (for example, 512bytes), block I/O errors can occur due to timeouts in qemu. To prevent this problem from occurring, use the default cluster size of 64KiB or larger.

kernel component

On Microsoft Windows Server 2012 containing large dynamic VHDX (Hyper-V virtual hard disk) files and using the ext3 file system, a call trace can appear, and, consequently, it is not possible to shut down the guest. To work around this problem, use the ext4 file system or set a logical block size of 1MB when creating a VHDX file. Note that this can only be done by using Microsoft PowerShell as the Hyper-V manager does not expose the –BlockSizeBytes option which has the default value of 32MB. To create a dynamix VHDX file with an approximate size of 2.5TB and 1MB block size run:

```
New-VHD –Path .\MyDisk.vhdx –SizeBytes 5120MB –BlockSizeBytes 1MB -
Dynamic
```

libvirt component

The storage drivers do not support the **virsh vol-resize** command options **--allocate** and **--shrink**. Use of the **--shrink** option will result in the following error message:

```
error: invalid argument: storageVolumeResize: unsupported flags (0x4)
```

Use of the **--allocate** option will result in the following error message:

```
error: invalid argument: storageVolumeResize: unsupported flags (0x1)
```

Shrinking a volume's capacity is possible as long as the value provided on the command line is greater than the volume allocation value as seen with the **virsh vol-info** command. You can shrink an existing volume by name through the followind sequence of steps:

1. Dump the XML of the larger volume into a file using the **vol-dumpxml** .
2. Edit the file to change the name, path, and capacity values, where the capacity must be greater than or equal to the allocation.
3. Create a temporary smaller volume using the **vol-create** with the edited XML file.
4. Back up and restore the larger volumes data using the **vol-download** and **vol-upload** commands to the smaller volume.
5. Use the **vol-delete** command to remove the larger volume.
6. Use the **vol-clone** command to restore the name from the larger volume.
7. Use the **vol-delete** command to remove the temporary volume.

In order to allocate more space on the volume, follow a similar sequence, but adjust the allocation to a larger value than the existing volume.

virtio-win component

It is not possible to downgrade a driver using the **Search for the best driver in these locations** option because the newer and installed driver will be selected as the "best" driver. If you want to force installation of a particular driver version, use the **Don't search** option and the **Have Disk** button to select the folder of the older driver. This method will allow you to install an older driver on a system that already has a driver installed.

virtio-win component BZ#1052845

Performing Automatic System Recovery (ASR) on Windows 2003 guest system with virtio-blk attached system disk fails. To work around this issue, the following files need to be copied from virtio-win floppy image to ASR floppy image :

- **txtsetup.oem**,
- **disk1**,
- **\i386(amd64)\Win2003***

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.

`grubby` component, BZ#893390

When a Red Hat Enterprise Linux 6.4 guest updates the kernel and then the guest is turned off 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 certain version of Microsoft Hyper-V Manager. 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 boot or 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. This is a host problem. Guest **kdump** works as expected on Microsoft Hyper-V 2012 R2 host.

`qemu-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 allow 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.

`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 can lead to the system being unresponsive and, consequently, to a crash during the final steps of the installation process. 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.

`libguestfs` component

The libguestfs packages do not support remote access to disks over the network in Red Hat Enterprise Linux 6. Consequently, the **virt-sysprep** tool as well as other tools do not work with remote disks. Users who need to access disks remotely with tools such as **virt-sysprep** are advised to upgrade to Red Hat Enterprise Linux 7.

6.5. STORAGE AND FILE SYSTEMS

`device-mapper-persistent-date` component, BZ#960284

Tools provided by the device-mapper-persistent-data package fail to operate on 4K hard-sectored metadata devices.

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.

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 workaroud 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
```

kernel component

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

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>
```

6.6. NETWORKING

389-ds-base component, BZ#1008013

Under certain conditions, when the server is processing multiple outgoing replication or windows sync agreements using the TLS or SSL protocol, and processing incoming client requests that use TLS or SSL, and incoming BIND requests where the password used is hashed using SSHA512, the server

becomes unresponsive to new incoming client requests. A restart of the **dirsrv** service is required. As the server is unresponsive, restarting can require terminating the **ns-slapd** process by running the **kill -9** command.

kernel component

In cluster environment, the multicast traffic from the guest to a host can be unreliable. To work around this problem, enable multicast_querier for the bridge. The setting is located in the **/sys/class/net/<bridge_name>/bridge/multicast_querier** file. Note that if the setting is not available, the problem should not occur.

kernel component

A missing part of the **bcma** driver causes the **brcmsmac** driver not to load automatically when the **bcma** driver scans the for devices. This causes the kernel not to load the **brcmsmac** module automatically on boot. Symptoms can be confirmed by running the **lspci -v** command for the device and noting the driver to be **bmca**, not **brcmsmac**. To load the driver manually, run **modprobe brcmsmac** on the command line.

389-ds-base component

Under certain conditions, when the server is processing multiple outgoing replication or windows sync agreements using the TLS or SSL protocol, and processing incoming client requests that use TLS or SSL and Simple Paged Results, the server becomes unresponsive to new incoming client requests. The **dirsrv** service will stop responding to new incoming client requests. A restart of the **dirsrv** service is required to restore service.

kernel component, BZ#1003475

When some Fibre Channel over Ethernet (FCoE) switch ports connected to the bfa host bus adapter go offline and then return in the online state, the bfa port may not re-establish the connection with the switch. This is due to a failure of the bfa driver's retry logic when interacting with certain switches. To work around this problem, reset the bfa link. This can be done either by running:

```
]# echo 1 > /sys/class/fc_host/host/issue_lip
```

or by running:

```
]# modprobe -r bfa && modprobe bfa
```

anaconda component, BZ#984129

For HP systems running in HP FlexFabric mode, the designated iSCSI function can only be used for iSCSI offload related operations and will not be able to perform any other Layer 2 networking tasks, for example, DHCP. In the case of iSCSI boot from SAN, the same SAN MAC address is exposed to both the corresponding **ifconfig** record and the iSCSI Boot Firmware Table (iBFT), therefore, Anaconda will skip the network selection prompt and will attempt to acquire the IP address as specified by iBFT. If DHCP is desired, Anaconda will attempt to acquire DHCP using this iSCSI function, which will fail and Anaconda will then try to acquire DHCP indefinitely. To work around this problem, if DHCP is desired, the user must use the **asknetwork** installation parameter and provide a "dummy" static IP address to the corresponding network interface of the iSCSI function. This prevents Anaconda from entering an infinite loop and allows it to request the iSCSI offload function to perform DHCP acquisition instead.

iscsi-initiator-utils component, BZ#825185

If the corresponding network interface has not been brought up by **dracut** or the tools from the iscsi-initiator-utils package, this prevents the correct MAC address from matching the offload interface, and host bus adapter (HBA) mode will not work without manual intervention to bring the corresponding network interface up. To work around this problem, the user must select the corresponding Layer 2 network interface when **anaconda** prompts the user to choose "which network interface to install through". This will inherently bring up the offload interface for the installation.

`kernel` component

When an **`igb`** link us up, the following **ethtool** fields display incorrect values as follows:

- *Supported ports: [ ]* - for example, an empty bracket can be displayed.
- *Supported pause frame use: No* - however, pause frame is supported.
- *Supports auto-negotiation: No* - auto-negotiation is supported.
- *Advertised pause frame use: No* - advertised pause frame is turned on.
- *Advertised auto-negotiation: No* - advertised auto-negotiation is turned on.
- *Speed: Unknown!* - the speed is known and can be verified using the **dmesg** tool.

`linuxptp` component

End-to-End (E2E) slaves that communicated with an E2E master once can synchronize to Peer-to-Peer (P2P) masters and vice versa. The slaves cannot update their path delay value because E2E ports reject peer delay requests from P2P ports. However, E2E ports accept SYNC messages from P2P ports and the slaves keep updating clock frequency based on undesired offset values that are calculated by using the old path delay value. Therefore, a time gap will occur if the master port is started with an incorrect delay mechanism. The "delay request on P2P" or "pdelay_req on E2E port" message can appear. To work around these problems, use a single delay mechanism for one PTP communication path. Also, because E2E and P2P mismatch can trigger a time gap of slave clock, pay attention to the configuration when starting or restarting a node on a running domain.

`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.

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.

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
```

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**.

bind-dyndb-ldap component, BZ#1142176

The **bind-dyndb-ldap** library incorrectly compares current time and the expiration time of the Kerberos ticket used for authentication to an LDAP server. As a consequence, the Kerberos ticket is not renewed under certain circumstances, which causes the connection to the LDAP server to fail.

The connection failure often happens after a **BIND** service reload is triggered by the **logrotate** utility, and you need to run the **pkill -9 named** command to terminate BIND after a deadlock occurs. To work around this problem, set the validity period of the Kerberos ticket to be at least 10 minutes shorter than the logrotate period.

bind-dyndb-ldap component, BZ#1142152

The **BIND** service incorrectly handles errors returned by dynamic databases (from dyndb API). As a consequence, **BIND** enters a deadlock situation on shutdown under certain circumstances. No workaround is available at the moment. If the deadlock occurs, terminate **BIND** by running the **pkill -9 named** command and restart the service manually.

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

Some network interface cards (NICs) might fail to get an IPv4 address assigned after the system is booted. The default time to wait for the link to come up is 5 seconds. To work around this issue, increase this wait time by specifying the LINKDELAY directive in the interface configuration file. For example, add the following line to the **/etc/sysconfig/network-scripts/ifcfg-<*interface*>** file:

```
LINKDELAY=10
```

In addition, check STP settings on all network switches in the path of the DHCP server as the default STP forward delay is 15 seconds.

samba component

Current Samba versions shipped with Red Hat Enterprise Linux 6 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 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.

6.7. SECURITY

openssl component, BZ#1022002

The external Advanced Encryption Standard (AES) New Instructions (AES-NI) engine is no longer available in openssl; the engine is now built-in and therefore no longer needs to be manually enabled.

6.8. 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.

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.

6.9. AUTHENTICATION

ipa component, BZ#1024744

OpenLDAP and 389 Directory Server treat the grace logins differently. 389 Directory Server treats them as "number of grace logins left" while OpenLDAP treats them as "number of grace logins used". Currently the SSSD only handles the semantics used by 389 Directory server. As a result, when using OpenLDAP server, the grace password warning might be incorrect.

ipa component, BZ#1024959

The Identity Management server does not write the initial user password correctly to password history. As a consequence, when a new Identity Management user is created and a password is generated for him, the first time that user changes the password, the value of the first password is disregarded when the password policy plug-in checks the password history. This means that user can "change" the initial password to the same value as the previous one, with no regards to the configured password history. Password history is applied correctly to all subsequent password changes.

`ipa` component, BZ#1009102

When an Identity Management server installed on Red Hat Enterprise Linux 6.2 is updated to the version provided by Red Hat Enterprise Linux 6.4 or later, the new pbac permission "Write DNS Configuration" is created without any of the required object classes. Consequently, the permission may not show up on the Identity Management Web UI permission page or when the **`--sizelimit`** parameter is used for the CLI **`permission-find`** command. The permission is still accessible using the command line when the **`--sizelimit`** option is not specified. To work around this problem, run the following command on the server to trigger the DNS permission update process again and fix the list of permission object classes:

```
]# ipa-ldap-updater --ldapi /usr/share/ipa/updates/40-dns.update
```

This problem can also be avoided when a replica of Red Hat Enterprise Linux 6.4 or later is installed, or when an Identity Management server is reinstalled or upgraded.

`ipa` component, BZ#983237

ipa-adtrust-install, an Identity Management Active Directory Trust configuration tool, does not explicitly specify authentication mechanism when performing Active Directory Trust configuration changes. When the user specifies the default LDAP authentication mechanism other than the expected default (for example, by setting the SASL_MECH configuration option to GSSAPI in the LDAP configuration file for the root user, **`.ldaprc`**), **ipa-adtrust-install** will not use the expected authentication mechanism and will fail to configure some of the parts of the Active Directory Integration feature, a crash of samba daemon (smbd) can occur or the user will be unable to use the feature. To work around this problem, remove any user default settings related to LDAP authentication mechanism from the **`.ldaprc`** file. The **ipa-adtrust-install** installer will then successfully configure the Active Directory integration feature.

`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 6.5 or later 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

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, 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
```

6.10. DEVICES

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.

`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 not 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.

6.11. KERNEL

`kernel` component

When Single Root I/O Virtualization (SR-IOV) is enabled on mlx4 adapters, initialization of the **`mlx4_core`** module can take longer than 30 seconds. However, **`udev`** has a 30-second timer for hardware initialization and terminates the modprobe sequence if the time is exceeded. As a consequence, the **`mlx4_en`** and **`mlx4_ib`** modules are not loaded after the **`mlx4_core`** module has finished initializing.

Two workarounds are available:

To work around the **`udev`** time limit, run the **`rmmod mlx4_core; modprobe mlx4_core`** command on a system that does not run on mlx4 hardware. Running this command enables you to have the full configured number of virtual devices, but for example guest operating systems that are configured to start on boot may need to be started manually once all the devices are present.

Alternatively, reduce either the total number of virtual functions that are enabled on the card, or functions that are probed by the guest driver, or both, until the card initialization sequence can be reliably completed in less than 30 seconds. However, you can be limited in the number of guests you can run due to insufficient virtual functions.

`kernel` component, BZ#1126294

The **modprobe** configuration file does not use the full path name of the **`modprobe`** binary file. As a consequence, **modprobe** fails to load the **`ib_qib`** module. To work around this problem, run the **`modprobe ib_qib`** command after each boot. Alternatively, to fix the problem permanently, edit the **`/etc/modprobe.d/truescale.conf`** and change the instance of **modprobe** to be /**sbin**/**modprobe**. As a result, the **`ib_qib`** module loads as expected.

`kernel` component

Sun Fire X4500 data server enumerates the e1000 card with Peripheral Component Interconnect Extended (PCI-X) and enables 64-bit direct memory access (DMA), however, 64-bit DMA is not fully supported on this hardware. If possible, disable 64-bit DMA in BIOS.

`grubby` component

Use of multiboot images makes discerning different image types problematic during kernel updates. As a consequence, using the tboot package and multiple types of kernels at the same time does not work properly. If, for example, tboot is in use and the kernel-debug package is installed, bootloader configuration can sometimes reflect an incorrect image list. To avoid this, do not use the kernel-debug on a system utilizing tboot, or vice versa. If such a situation is unavoidable, manually verify that the bootloader configuration is reasonable after each update before rebooting.

`kexec-tools` component

When the debug kernel is installed and also used as the Red Hat Enterprise Linux kdump kernel, the reserved kdump memory must be increased to a minimum of 256 MB. To assure this setting, start the **system-config-kdump** tool, modify the kdump memory, and reboot your Linux instance. Alternatively, you can configure a particular kernel that is always used as the kdump kernel, independently of the running kernel. For more information, consult the Red Hat Enterprise Linux 6 Deployment Guide.

`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 and later 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.

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 6.3 i386 and later 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

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.

6.12. DESKTOP

python component, BZ#1114434

In a multi-thread **Python** program, if a non-main thread receives a signal while the **signal.pause()**

function is in use in the main thread, **signal.pause()** does not return or otherwise handle the received signal, and **signal.pause()** works only when the main thread is signaled. As a consequence, a **Python** program could become unresponsive. To work around this problem, avoid calling **signal.pause()** in the main thread.

mesa-private-llvm component, BZ#1121576

The mesa-private-llvm packages have a syntax error in their %postun script in versions prior to 3.4. As a consequence, when updating mesa-private-llvm to a later version, the following error message is displayed:

```
Upgrading from mesa-private-llvm-3.3-0.3.rc3.el6.x86_64 causes:
/sbin/ldconfig: relative path `1' used to build cache
warning: %postun(mesa-private-llvm-3.3-0.3.rc3.el6.x86_64) scriptlet
failed, exit status 1
```

This message is harmless and does not affect the user.

xorg-x11-drv-fbdev component, BZ#1011657

The X server in Red Hat Enterprise Linux 6.5, when presented with an **xorg.conf** file that identifies both a PCI driver and an fbdev driver, the fbdev driver is ignored and only the PCI device is initialized. In Red Hat Enterprise Linux 6.6, the server can attempt to initialize both devices present in such a configuration file. As a consequence, installations in this scenario initialize on all screens, which can cause a loss of functionality. To work around this problem, edit **xorg.conf** manually: remove the fbdev device stanza or edit it appropriately. As a result, a single X server can now drive both PCI devices using native drivers and non-PCI devices with the fbdev driver.

gnome-panel component, BZ#1017631

The **gnome-panel** utility can sometimes terminate unexpectedly on 64-bit PowerPC architecture using the XDMCP protocol.

xorg-x11-drv-intel component, BZ#889574

Red Hat Enterprise Linux 6 graphics stacs does not support NVIDIA Optimus hardware configurations. On laptops with both Intel and NVIDIA GPUs, some or all external video ports may not function correctly when using the Intel GPU. If external video ports are needed, configure the BIOS to use the NVIDIA GPU instead of the Intel GPU if possible.

xorg-x11-drv-synaptics component, BZ#873721

Two-finger scrolling is default for devices that announce two-finger capability. However, on certain machines, although the touchpad announces two-finger capability, events generated by the device only contain a single finger position at a time and two-finger scrolling therefore does not work. To work around this problem, use edge scrolling instead.

firefox component

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.

wacomcpl component, 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.

6.13. TOOLS

`mvapich2` component

The mvapich2 packages use the **`GNU Autotools`** set of tools (**`autoconf`**, **`automake`**, and **`libtool`**) to process its configuration. Features included in version 1.12 and later are required, but are not available in Red Hat Enterprise Linux 6.6 and earlier. As a consequence, rebuilding mvapich2 fails with earlier versions of **`GNU Autotools`**. To work around this problem, uninstall the autoconf, automake, and libtool packages, rebuild mvapich2, and then reinstall **`GNU Autotools`**.

`freeipmi` component, BZ#1020650

Under certain circumstances, the **`IPMI`** service is not started and the **`ipmi_devintf`** kernel module that provides the device node interface is not loaded. As a consequence, some hardware could reboot unexpectedly after installation before the first intentional reboot. To work around this problem, run the following commands as root:

```
chkconfig --level 345 ipmi on
service ipmi restart
service bmc-watchdog condrestart
```

Alternatively, log in as root, create the **`/etc/modprobe.d/watchdog-reboot-workaround.conf`** file, and include the following three aliases:

- alias acpi:IPI000*:* ipmi_si
- alias acpi:IPI000*:* ipmi_devintf
- alias acpi:IPI000*:* ipmi_msghandler

`ssh-keygen` component

The following example in the description of the -V option in the ssh-keygen(1) manual page is incorrect:

```
“-4w:+4w” (valid from four weeks ago to four weeks from now)
```

If you set a date range in this format, the certificate is valid from four weeks ago until now.

`perl-WWW-curl` component

Attempting to access the CURLINFO_PRIVATE value can cause **curl** to terminate unexpectedly with a segmentation fault.

`freerpd` component, BZ#988277

The ALSA plug-in is not supported in Red Hat Enterprise Linux 6. Instead of the ALSA plug-in, use the pulseaudio plug-in. To enable it, use the **`--plugin rpdsnd`** option with the **`xfreerdp`** command without specifying which plug-in should be used; the pulseaudio plug-in will be used automatically in this case.

`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
```

CHAPTER 7. NEW PACKAGES

7.1. RHEA-2014:1521 — NEW PACKAGE: CONVMV

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

The convmv package contains a tool for converting the character-set encoding of file names. It is particularly useful for converting file names encoded in a legacy charset encoding such as ISO-8859 to UTF-8, or EUC to UTF-8.

This enhancement update adds the convmv package to Red Hat Enterprise Linux 6. (BZ#1005068)

All users who require convmv are advised to install this new package.

7.2. RHEA-2014:1602 — NEW PACKAGES: CRYPTSETUP-REENCRYPT

New cryptsetup-reencrypt packages are now available for Red Hat Enterprise Linux 6.

The cryptsetup-reencrypt packages provide the cryptsetup-reencrypt utility that can be used for offline re-encryption of a disk that is encrypted with Linux Unified Key Setup-on-disk-format (LUKS). These packages also include a dracut module required for re-encryption of a device that contains a root file system.

This enhancement update adds the cryptsetup-reencrypt packages to Red Hat Enterprise Linux 6. The cryptsetup-reencrypt utility also facilitate the mass cloning of drives. (BZ#1107729, BZ#847172)

All users who require cryptsetup-reencrypt are advised to install these new packages.

7.3. RHBA-2014:1498 — NEW PACKAGES: GDISK

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

The gdisk packages provide a fdisk-like partitioning tool for GPT disks. GPT fdisk features a command-line interface, fairly direct manipulation of partition table structures, recovery tools fort dealing with corrupt partition tables, and the ability to convert MBR disks to GPT format.

This enhancement update adds the gdisk packages to Red Hat Enterprise Linux 6. (BZ#1015157)

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

7.4. RHBA-2014:1577 — NEW PACKAGES: GLIB-NETWORKING

New glib-networking packages are now available for Red Hat Enterprise Linux 6.

The glib-networking packages provide modules that extend the networking support in Glib. In particular, the packages contain a libproxy-based implementation of the GProxyResolver class type and a gnutls-based implementation of the GTlsConnection class type.

This enhancement update adds the glib-networking packages to Red Hat Enterprise Linux 6. (BZ#1101418, BZ#1119162)

The glib-networking packages are installed automatically as a dependency of the libsoup packages.

7.5. RHEA-2014:1433 — NEW PACKAGE: GOOGLE-CROSEXTRA-CALADEA-FONTS

A new google-crosextra-caladea-fonts package is now available for Red Hat Enterprise Linux 6.

The Caladea font family is metric-compatible with the Cambria font. Caladea is a serif typeface family based on the Lato font.

This enhancement update adds the google-crosextra-caladea-fonts package to Red Hat Enterprise Linux 6. (BZ#1025629)

All users who require google-crosextra-caladea-fonts are advised to install this new package.

7.6. RHEA-2014:1434 — NEW PACKAGE: GOOGLE-CROSEXTRA-CARLITO-FONTS

A new google-crosextra-carlito-fonts package is now available for Red Hat Enterprise Linux 6.

The google-crosextra-carlito-fonts package provides the Carlito font family. Carlito is metric-compatible with Calibri font. Carlito comes in regular, bold, italic, and bold italic faces. The family covers Latin-Greek-Cyrillic (not a complete set, though) with about 2,000 glyphs. It has the same character coverage as Calibri. This font is sans-serif typeface family based on Lato.

This enhancement update adds the google-crosextra-carlito-fonts package to Red Hat Enterprise Linux 6. (BZ#1025628)

All users who require google-crosextra-carlito-fonts are advised to install this new package.

7.7. RHEA-2014:1439 — NEW PACKAGE: HYPERV-DAEMONS

New hyperv-daemons packages are now available for Red Hat Enterprise Linux 6.

The hyperv-daemons packages provide a suite of daemons that are needed when a Linux guest is running on a Windows Host with HyperV. The following daemons are included: - hypervkvpd, the guest Hyper-V Key-Value Pair (KVP) daemon. - hypervvssd, the implementation of HyperV VSS functionality for Linux guest. - hypervfcopyd, the implementation of file copy service functionality for Linux Guest running on HyperV.

This enhancement update adds the hyperv-daemons packages to Red Hat Enterprise Linux 6. (BZ#977631, BZ#1107559)

All users who require hyperv-daemons are advised to install these new packages. After installing the packages, rebooting all guest machines is recommended, otherwise the Microsoft Windows server with Hyper-V will not be able to get information from these guest machines. For more information about inclusion of, and guest installation support for, Microsoft Hyper-V drivers, refer to the Red Hat Enterprise Linux 6.6 Release Notes.

7.8. RHEA-2014:1467 — NEW PACKAGES: JAVA-1.8.0-OPENJDK

New java-1.8.0-openjdk packages are now available for Red Hat Enterprise Linux 6.

java-1.8.0-openjdk packages provide the OpenJDK runtime environment.

This enhancement update adds the java-1.8.0-openjdk packages to Red Hat Enterprise Linux 6. (BZ#1081073, BZ#1113078)

All users who require java-1.8.0-openjdk are advised to install these new packages. All running instances of OpenJDK Java must be restarted for the update to take effect.

7.9. RHEA-2014:1530 — NEW PACKAGES: JSON-C

New json-c packages are now available for Red Hat Enterprise Linux 6.

JSON-C implements a reference counting object model that allows users to easily construct JavaScript Object Notation (JSON) objects in C, output them as JSON formatted strings and parse JSON formatted strings back into the C representation of JSON objects.

This enhancement update adds the json-c packages to Red Hat Enterprise Linux 6. (BZ#966964)

All users who require json-c are advised to install these new packages.

7.10. RHEA-2014:1519 — NEW PACKAGE: KSC

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

The ksc package contains KSC, a kernel module source code checker to find usage of non-whitelist symbols.

This enhancement update adds the ksc package to Red Hat Enterprise Linux 6. (BZ#1085004)

All users who require ksc are advised to install this new package.

7.11. RHEA-2014:1596 — NEW PACKAGES: KSM_PRELOAD

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

The ksm_preload packages provide the ksm_preload library that allows applications to share memory pages. It also enables "legacy" applications to leverage Linux's memory deduplication.

This enhancement update adds the ksm_preload packages to Red Hat Enterprise Linux 6. (BZ#1034763)

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

7.12. RHEA-2014:1518 — NEW PACKAGES: LIBEE

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

The libee packages contain an event expression library inspired by the Common Event Expression (CEE), a standard proposed by the MITRE organization that is used to describe network events in a number of normalized formats. Its goal is to unify many different representations that exist in the industry. The core idea of libee is to provide a small API layer above the CEE standard.

This enhancement update adds the libee packages to Red Hat Enterprise Linux 6. (BZ#966972)

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

7.13. RHEA-2014:1501 — NEW PACKAGE: LIBESTR

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

The libestr packages contain the string handling essentials library used by the Rsyslog daemon, and is required by the rsyslog7 package.

This enhancement update adds the libestr packages to Red Hat Enterprise Linux 6. (BZ#966966)

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

7.14. RHEA-2014:1441 — NEW PACKAGES: LIBMICROHTTPD

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

GNU libmicrohttpd is a lightweight C library that can be used to easily embed an HTTP server in another application.

This enhancement update adds the libmicrohttpd packages to Red Hat Enterprise Linux 6. (BZ#1087821)

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

7.15. RHEA-2014:1516 — NEW PACKAGES: LIBNETFILTER_QUEUE

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

The libnetfilter_queue packages include a user space library providing an API to packets that have been queued by the kernel packet filter. It is part of a system that deprecates the old ip_queue or libipq mechanism.

This enhancement update adds the libnetfilter_queue packages to Red Hat Enterprise Linux 6. (BZ#738244)

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

7.16. RHEA-2014:1456 — NEW PACKAGES: MOD_AUTHNZ_PAM, MOD_INTERCEPT_FORM_SUBMIT, MOD_LOOKUP_IDENTITY

New authentication and identity modules for Apache HTTP server are now available for Red Hat Enterprise Linux 6.

The mod_authnz_pam, mod_intercept_form_submit, and mod_lookup_identity are a set of Apache HTTP server modules to support authentication and identity functions for web applications.

The mod_authnz_pam Apache module serves as a PAM authorization module, supplementing authentication done by other modules, for example mod_auth_kerb. It can also be used as a full Basic Authentication provider for testing purposes, running the login and password authentication through the PAM stack.

The mod_intercept_form_submit Apache module intercepts application's login form submission and runs the PAM authentication.

The mod_lookup_identity Apache module retrieves additional information about the authenticated user.

This enhancement update adds the mod_authnz_pam, mod_intercept_form_submit, mod_lookup_identity packages to Red Hat Enterprise Linux 6. (BZ#1075121, BZ#1075122, BZ#1080478)

All users who require the new authentication and identity modules for Apache HTTP server are advised to install these new packages.

7.17. RHEA-2014:1523 — NEW PACKAGES: NUMATOP

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

NumaTOP is an observation tool for runtime memory locality characterization and analysis of processes and threads running on a Non-Uniform Memory Access (NUMA) system. NumaTOP can help the user characterize the NUMA behavior of processes and threads and locate NUMA-related performance problems.

This enhancement update adds the numatop packages to Red Hat Enterprise Linux 6. (BZ#1066152)

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

7.18. RHEA-2014:1540 — NEW PACKAGE: RSYSLOG7

New rsyslog7 packages are now available for Red Hat Enterprise Linux 6.

The rsyslog7 packages provide an enhanced, multi-threaded syslog daemon. It supports on-demand disk buffering, reliable syslog over TCP, SSL, TLS and RELP, writing to databases (MySQL, PostgreSQL, Oracle, and many more), email alerting, fully configurable output formats (including high-precision timestamps), the ability to filter on any part of the syslog message, on-the-wire message compression, and the ability to convert text files to syslog.

This enhancement update adds the rsyslog7 packages to Red Hat Enterprise Linux 6. These packages are a replacement for previously used rsyslog packages. (BZ#869600)

All users who require rsyslog7 are advised to install these new packages. All users of rsyslog are advised to migrate to these new packages.

7.19. RHEA-2014:1471 — NEW PACKAGE: SCAP-SECURITY-GUIDE

A new scap-security-guide package is now available for Red Hat Enterprise Linux 6.

The scap-security-guide package provides a SCAP Security Guide (SSG) project's guide for configuration of the system from the final system's security point of view. The guidance is specified in the Security Content Automation Protocol (SCAP) format and constitutes a catalog of practical hardening advice, linked to government requirements where applicable. The project bridges the gap between generalized policy requirements and specific implementation guidelines.

The Red Hat Enterprise Linux 6 system administrator can use the oscap command-line tool from the openscap-utils package to verify that the system conforms to the provided guideline. For further information. see the scap-security-guide(8) manual page.

This enhancement update adds the scap-security-guide package to Red Hat Enterprise Linux 6. (BZ#1066390)

All users who require scap-security-guide are advised to install this new package.

7.20. RHEA-2014:1431 — NEW PACKAGE: TAGSOUP

New tagsoup package is now available for Red Hat Enterprise Linux 6.

TagSoup is a SAX-compliant HTML parser written in Java.

This enhancement update adds the tagsoup package to Red Hat Enterprise Linux 6. (BZ#1088492)

All users who require tagsoup are advised to install this new package.

7.21. RHEA-2014:1598 — NEW PACKAGES: TMON

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

The tmon packages provide a utility to query the thermal monitoring system of the Linux kernel.

This enhancement update adds the tmon packages to Red Hat Enterprise Linux 6. (BZ#1104389)

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

7.22. RHEA-2014:1514 — NEW PACKAGES: XMLSEC1, LASSO, MOD_AUTH_MELLON

New xmlsec1, lasso, mod_auth_mellon packages are now available for Red Hat Enterprise Linux 6.

The mod_auth_mellon packages provide the mod_auth_mellon module that is an authentication service implementing the Security Assertion Markup Language (SAML) federation protocol version 2.0. It grants access based on the attributes received in assertions generated by an IDP server.

The lasso packages provide the Lasso library that implements the Liberty Alliance Single Sign On standards, including the SAML and SAML2 specifications. It allows handling of the whole life-cycle of SAML-based federations, and provides bindings for multiple languages.

The xmlsec1 packages provide XML Security Library, a C library based on LibXML2 and OpenSSL. The library was created with a goal to support major XML security standards "XML Digital Signature" and "XML Encryption".

This enhancement update adds the xmlsec1, lasso, and mod_auth_mellon packages to Red Hat Enterprise Linux 6 in order to provide SAML Service Provider support in the Apache HTTP server. (BZ#1083605, BZ#1087555, BZ#1090812)

All users who require support for SAML-based federations in the Apache HTTP server are advised to install these new packages.

CHAPTER 8. UPDATED PACKAGES

8.1. 389-DS-BASE

8.1.1. RHBA-2014:1385 — 389-ds-base bug fix and enhancement update

Updated 389-ds-base packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

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.

Bug Fixes

BZ#1001037

When a new user was created on Active Directory (AD) and their password was set, the system administor checked the flag "User must change password on next login". Afterwards, the default password was sent to Red Hat Directory Server (RHDS), which set the password but removed the aforementioned flag. With this update, the flag for password change at next login persists, and the password sync tool for by-passing the 7-day constraint is allowed if the flag is checked.

BZ#1008021

If an ACI (access control instruction) is configured to give permissions to "self", bound user itself, the result of a granted access for an entry was cached and could erroneously be reused for all entries. Consequently, a bound client could retrieve entries or attributes it was not supposed to, or fail to retrieve those entries and attributes it was supposed to retrieve. With this update, certain accesses are granted per entry, making sure that if a granted access is cached, it is purged for the next entry.

BZ#1009122

The multi-master replication protocol keeps a cumulative counter of the relative time offsets between servers. However, prior to this update, if the system time was adjusted by more than one day, the counter became off by more than one day. Consequently, a replication consumer refused to accept changes from the master and the replication process failed. This update adds a new configuration attribute to cn=config - nsslapd-ignore-time-skew, with the default of "off". In addition, an error message is logged warning the system administrator about the time skew issue. Alternatively, if this attribute is set to "on", a replication consumer allows replication to proceed despite the excessive time skew.

BZ#1012699

Previously, when an invalid install script from host name to the server was supplied, a vague error message was returned to the user. This update provides a proper error message to be returned when a setup script encounters an error in the host name.

BZ#1044218

Previously, the size of the directory server was constantly increasing after search requests for simple paged results were processed. The memory leak causing this bug has been fixed, and the server size no longer increases in the aforementioned situation.

BZ#1049029

Prior to this update, Windows Sync Control request returned the renamed member of a group entry only, not the group containing this member. As a consequence, renaming user Distinguished Name

(DN) on Active Directory (AD) was not applied to the synced member DN in a group that the user DN belonged to. With this update, once a rename operation is received from AD, Windows Sync Control searches groups having a member value, and replaces the old DN with the renamed DN. In addition, Windows Sync Control also updates the renamed member DN in a group as intended.

BZ#1053766

Previously, when importing an LDAP Data Interchange Format (LDIF) or doing a replication initialization that contained tombstone entries, the parent entry of the tombstone entry had its numsubordinate entry count incorrectly incremented. With this update, the parent entry numsubordinate attribute is not updated when processing a tombstone entry, and numsubordinate value is now accurate in all entries.

BZ#1057805

Previously, calculating the size of an entry in the memory was underestimated: the entry cache size was larger than the specified size in the configuration. This bug has been fixed by calculating each entry size more accurately, which leads to more accurate size of the entry cache.

BZ#1060385

When trying to process an empty log file, the logconv.pl utility failed to run and reported a series of Perl errors. To fix this bug, empty log files are checked and ignored, and logconv.pl reports the empty log file by the following message:

```
Skipping empty access log, /var/log/dirsrv/slapd-ID/access.
```

BZ#1070583

While a Total Replication Update or Replica Initialization was occurring, the server could terminate unexpectedly. With this update, the replication plugin is not allowed to terminate while the total update of replica is still running, and the server thus no longer crashes.

BZ#1070720

Prior to this update, using the "-f" filter option caused the rsearch utility to return a filter syntax error. This update makes sure the filter is properly evaluated, and rsearch now works correctly when using the "-f" option.

BZ#1071707

Previously, when a search request for simple paged results was sent to a server and the request was abandoned, the paged result slot in the connection table was not properly released. Consequently, as the slot was not available, the temporary initial slot number "-1" was kept to access an array, which caused its invalid access. With this update, the abandoned slot content is properly deleted for reuse. As a result, the temporary slot number is now replaced with the correct slot number, and invalid array accesses no longer occur.

BZ#1073530

Due to exceeded size limit, Access Control Instruction (ACI) group evaluation failed. However, the "sizelimit" value could be a false value retrieved from a non-search operation. With this update, detected false values are replaced with an unlimited value (-1), and ACI group evaluation no longer fails due to an unexpected sizelimit exceeded error.

BZ#1077895

Performing an LDAP operation using the proxied authentication control could previously lead to server memory leaks. With this update, the allocated memory is released after the operation

completion, and the server no longer leaks memory when processing operations using the proxied authentication control.

BZ#1080185

Prior to this update, the tombstone data resurrection did not consider the case in which its parent entry became a conflict entry. In addition, resurrected tombstone data treatment was missing in the entryrdn index. As a consequence, the parent-child relationship became confused when the tombstone data was being resurrected. With this update, the Directory Information Tree (DIT) structure is properly maintained; even if the parent of a tombstone-data entry becomes a conflict entry, the parent-child relationship is now correctly managed.

BZ#1083272

Due to improper use of the valueset_add_valueset() function, which expects only empty values to be passed to it, the server could terminate unexpectedly. This update handles the misuse of the function, which now no longer causes the server to crash.

BZ#1086454

Previously, the logging level was too verbose for the severity of the message, and the errors log could fill up with redundant messages. To fix this bug, the logging has been changed to be written only when "access control list processing" log level is being used, and thus the errors log no longer fills up with harmless warning messages.

BZ#1086903

Previously, if the do_search() function failed at the early phase, the memory storing the given baseDN was not freed. The underlying source code has been fixed, and the baseDN no longer leaks memory even if the search fails at the early phase.

BZ#1086907

Previously, in the entry cache, some delete operations failed with an error when entries were deleted while tombstone purging was in process. This update retries to obtain the parent entry until it succeeds or times out. As a result, delete operations in the entry cache now succeed as intended.

BZ#1092097

Previously, when Multi Master Replication was configured, if an entry was updated on Master 1 and deleted on Master2, the replicated update from Master 1 could target on a deleted entry (a tombstone). This led to two consequences. Firstly, the replicated update failed and could break the replication. Secondly, the tombstone entries differed on Master 1 and Master 2. This update allows updates on a tombstone if the update originates in a replication. Now, replication succeeds and tombstone entries are identical on all servers.

BZ#1097002

When deleting a node entry whose descendants were all deleted, previously, only the first position was checked. Consequently, the child entry at the first position was deleted in the database. However, it could be reused for the replaced tombstone entry, which reported the false error "has children", and thus caused the node deletion to fail. With this update, instead of checking the first position, all child entries are checked whether they are tombstones or not; in case all of them are tombstones, the node is deleted. Now, the false error "has children" is no longer reported, and a node entry whose children are all tombstones is successfully deleted.

BZ#1098653

When a replication is configured, a replication change log database is also a target of the backup.

However, backing up a change log database previously failed because there was no back end instance associated with the replication change log database. As a consequence, backing up on a server failed. With this update, if a backing up database is a change log database, the db2bak.pl utility skips checking the back end instance, and backing up thus works as intended.

BZ#1103287

When processing a large amount of access logs without using any verbose options, memory continued to grow until the system was exhausted of available memory, or logs were completely processed. The back-ported feature causing excessive memory consumption has been removed, and memory now remains stable regardless of the amount of logging being processed.

BZ#1103337

Previously, the following message was incorrectly coded as an error level:

```
changelog iteration code returned a dummy entry with csn %s, skipping
...
```

Consequently, once the server run into the state, this benign error message was logged in the error log repeatedly. To fix this bug, the log level has been changed, and the the message is no longer logged.

BZ#1106917

Prior to this update, when performing a modrdn operation on a managed entry, the managed entry plugin failed to properly update managed entry pointer. The underlying source code has been fixed, and the managed entry link now remains intact on modrdn operations.

BZ#1109333

The previous MemberOf plugin code assumed the Distinguished Name (DN) value to have the correct syntax, and did not check the normalized value of that DN. This could lead to dereferencing a NULL pointer and unexpected termination. This update checks the normalized value and logs a proper error. As a result, invalid DN no longer causes crashes and errors are properly logged.

BZ#1109335

When adding and deleting entries, the modified parent entry, numsubordinates, could be replaced in the entry cache, even if the operation failed. As a consequence, parent numsubordinate count could be incorrectly updated. This update adds code to unswitch the parent entry in the cache, and parent numsubordinate count is now guaranteed to be correct.

BZ#1109337

Previously, if nested tombstone entries were present, parents were always purged first, and thus their child entries became orphaned. With this update, when doing the tombstone purge, the candidate list is processed in the reverse order, which removes the child entries before the parent entries. As a result, orphaned tombstone entries are no longer left orphaned after purging.

BZ#1109352

Previously, a tombstone purge thread issued a callback search that started reading the id2entry file, even if the back end had already been stopped or disabled. This could cause the server to terminate unexpectedly. Now, when performing a search and returning entries, this update checks if the back end is started before reading id2entry. As a result, even if the tombstone purge occurs while the back end is stopped, the server no longer crashes.

BZ#1109356

Due to various mistakes in the source code, potential memory leaks, corrupted memory, or crashes could occur. All the aforementioned bugs have been addressed, and the server now behaves as expected without crashing or leaking memory.

BZ#1109358

Due to a failure in back end transaction, the post plugin was not properly passed to the back end. As a consequence, the ldapdelete client unexpectedly executed a tombstone deletion. A failure check code has been added with this update, and a tombstone deletion by ldapdelete now fails as expected.

BZ#1109361

Previously, the server enabled the rsa_null_sha cipher, which was not considered secure. With this update, rsa_null_sha is no longer available.

BZ#1109363

Previously, the caller of the slapi_valueset_add_attr_valuearray_ext() function freed the returned Slapi_ValueSet data type improperly upon failure. Consequently, Slapi_ValueSet leaked memory when the attribute adding operation failed. This update adds the code to free the memory, and returned Slapi_ValueSet no longer leaks memory.

BZ#1109373

Prior to this update, syntax plugins were loaded during bootstrapping. However, in that phase, attributes had already been handled. As a consequence, the sorted results of multi-attribute values in schema and Directory Server specific Entries (DSE) became invalid. This update adds a default syntax plugin, and the sorted results of DSE and schema are now in the right order.

BZ#1109377

Previously, environment variables, except from TERM and LANG, were ignored if a program was started using the "service" utility. Consequently, memory fragmentation could not be configured. To fix this bug, mallopt environment variables, "SLAPD_MXFAST", "MALLOC_TRIM_THRESHOLD_" and "MALLOC_MMAP_THRESHOLD_", have been made configurable. Now, memory fragmentation can be controlled explicitly and provide instructions to the "service" utility.

BZ#1109379

Prior to this update, when running a CLEANALLRUV task, the changelog replication incorrectly examined a Change Sequence Number (CSN) which could be deleted and returned as the minimum CSN for a replica. With this update, CSNs that are from a "cleaned" replica ID are ignored, and replication now uses the correct minimum CSN.

BZ#1109381

Previously, a group on Active Directory (AD) had a new member which was not a target of windows sync and existed only on AD. If an operation was executed on AD, the member was replaced with other members which were the targets of the windows sync. Consequently, the new member values were not synchronized. With this update, a modify operation follows including the member value, which is now proceeded by confirming the existence on AD, thus fixing the bug.

If a group on Active Directory (AD) and Directory Server (DS) had members which were local, not synchronized, and the members were removed from the group on one side, the delete operation was synchronized and all the members including the local ones were deleted. The underlying source code

has been modified to check, firstly, if an attribute is completely deleted on one side, secondly, if each value on the other side is in the sync scope. In addition, the value is now put to the mode for the delete only if the value is in the sync scope.

BZ#1109384

Previously, the manual page for the logconv.pl utility was missing some of the command line options. The manual page has been updated to show the complete usage of logconv.pl with all the available options.

BZ#1109387

Due to a bug in partial restoration, the order of the restored index became confused. With this update, the default compare function is called. Now, after running a partial restoration, indexing problems no longer occur.

BZ#1109443

In processing Class of Service (CoS) definition entry, if the cosTemplateDn entry was not yet given when the cosAttribute entry was being processed, the parent entry Distinguished Name (DN) was set to cosTemplateDn automatically. Consequently, the parent entry could be an ancestor entry of an entry to be updated. In addition, if the entry was a target of the betxn type of plugins, a deadlock occurred. With this update, the parent entry DN is added only when codTemplateDn is not provided. Now, even if cosAttribute and cosTemplateDn are listed in the order in the CoS definition entry and the betxn type plug-ins are enabled, updating an entry no longer causes deadlocks.

BZ#1109952

Previously, if Virtual List View (VLV) search failed with "timelimit" or "adminlimit" server resources, the allocated ID list was not freed. Consequently, when the failure occurred, the memory used for the ID list leaked. This update adds the free code for the error cases, and the memory leaks caused by the VLV failure no longer occur.

Enhancement

BZ#985270

Previously, only the root Distinguished Name (DN) accounts were able to specify users that could bypass the password policy settings or add hashed passwords to users. With this update, non-root DN accounts are allowed to perform these types of operations as well.

Users of 389-ds-base are advised to upgrade to these updated packages, which fix these bugs and add this enhancement. After installing this update, the 389 server service will be restarted automatically.

8.1.2. RHBA-2014:1623 — 389-ds-base bug fix update

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

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.

Bug Fix

BZ#1080185

Bug fixes for replication conflict resolution

introduced a memory leak bug, which increased the size of the Directory Server. With this update, the memory leak code has been fixed, and the size of the Directory Servers in the replication topology is now stable under the stress. (BZ#1147479)

Users of 389-ds-base are advised to upgrade to these updated packages, which fix this bug. After installing this update, the 389 server service will be restarted automatically.

8.2. NETWORKMANAGER

8.2.1. RHBA-2014:1413 — NetworkManager bug fix update

Updated NetworkManager packages that fix two bugs 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. Its capabilities include managing Ethernet, wireless, mobile broadband (WWAN), and PPPoE devices, as well as providing VPN integration with a variety of different VPN services.

Bug Fixes

BZ#1025009

When the machine suspended, the NetworkManager daemon deactivated all network devices on that machine. Consequently, the Wake-on-LAN clients did not work because this network device was powered down, and thus could not receive the Magic Packet. With this update, NetworkManager leaves devices running at suspend time if they have the Wake-on-LAN or Wake-on-Wireless-LAN variable enabled, and Wake-on-LAN works as intended if the administrator enables it.

BZ#1034860

Previously, NetworkManager used the kernel's Point-to-point protocol over Ethernet (PPPoE) driver, which did not inform userland when it received a PPPoE Active Discovery Terminate (PADT) frame. As a consequence, when connecting to certain digital subscriber line (DSL) providers, the NetworkManager daemon failed to notice whether the connection was dropped. With this update, NetworkManager uses a userland PPPoE driver rather than the kernel driver, and dropped DSL connections are now noticed for all providers.

BZ#1113996

NetworkManager automatically provides an autoconnect for interfaces. Previously, when this connection was altered and saved, NetworkManager terminated unexpectedly. The write_ip4_setting() function has been updated to fix this bug, and NetworkManager no longer crashes after saving altered configuration.

Users of NetworkManager are advised to upgrade to these updated packages, which fix these bugs.

8.3. ORBIT2

8.3.1. RHBA-2014:1563 — ORBit2 bug fix update

Updated ORBit2 packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The ORBit2 packages provide a high-performance Object Request Broker (ORB) for the Common Object Request Broker Architecture (CORBA). ORBit allows programs to send requests and receive replies from

other programs, regardless of where the programs are located. CORBA is a standard that enables communication between program objects, regardless of the programming language and platform used.

Bug Fix

BZ#784223

Due to improper synchronization between multiple threads when accessing shared data objects, the bonobo-activation-server process was in certain cases killed by the SIGSEGV signal. With this update, clean-up tasks on one thread have been deferred, so synchronization is no longer necessary. As a result, the process does not crash anymore in the described scenario.

Users of ORBit2 are advised to upgrade to these updated packages, which fix this bug.

8.4. PACKAGEKIT

8.4.1. RHBA-2014:1481 — PackageKit bug fix update

Updated PackageKit packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

PackageKit is 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 Fixes

BZ#743399

Due to a regression, some systems reported the following entry in the Automatic Bug Reporting Tool (ABRT) even though no applications were being tested at the time and the systems were idle:

"Process /usr/sbin/packagekitd was killed by signal 11 (SIGSEGV)"

A patch has been provided to fix this bug, and ABRT no longer produces such error messages.

BZ#811097

When running the "pkcon install" command, the pkcon utility failed to provide a prompt for the user requiring more information. Instead, the pkcon utility terminated unexpectedly and returned the following error:

"Fatal error: user declined simulation"

An upstream patch has been provided to fix this bug. As a result, pkcon prompts the user with "Proceed with changes? [N/y]" to get an input, and completes successfully.

BZ#874270

Due to a series of processes all aborting and nsswitch malfunctioning, starting the KVM host or guest displayed error messages on ABRT. The bug has been fixed, and KVM no longer returns error messages.

Users of PackageKit are advised to upgrade to these updated packages, which fix these bugs.

8.5. RELEASE NOTES

8.5.1. RHEA-2014:1608 — Red Hat Enterprise Linux 6.6 Release Notes

Updated packages containing the Release Notes for Red Hat Enterprise Linux 6.6 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 6.6 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 6.6 Release Notes:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/ht ml-single/6.6_Release_Notes/index.html

8.6. X11 CLIENT LIBRARIES

8.6.1. RHSA-2014:1436 — Moderate: X11 client libraries security, bug fix, and enhancement update

Updated X11 client libraries packages that fix multiple security issues, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 X11 (Xorg) libraries provide library routines that are used within all X Window applications.

Security Fixes

CVE-2013-1981, **CVE-2013-1982**, **CVE-2013-1983**, **CVE-2013-1984**, **CVE-2013-1985**, **CVE-2013-1986**, **CVE-2013-1987**, **CVE-2013-1988**, **CVE-2013-1989**, **CVE-2013-1990**, **CVE-2013-1991**, **CVE-2013-2003**, **CVE-2013-2062**, **CVE-2013-2064**

Multiple integer overflow flaws, leading to heap-based buffer overflows, were found in the way various X11 client libraries handled certain protocol data. An attacker able to submit invalid protocol data to an X11 server via a malicious X11 client could use either of these flaws to potentially escalate their privileges on the system.

CVE-2013-1997, **CVE-2013-1998**, **CVE-2013-1999**, **CVE-2013-2000**, **CVE-2013-2001**, **CVE-2013-2002**, **CVE-2013-2066**

Multiple array index errors, leading to heap-based buffer out-of-bounds write flaws, were found in the way various X11 client libraries handled data returned from an X11 server. A malicious X11 server could possibly use this flaw to execute arbitrary code with the privileges of the user running an X11 client.

CVE-2013-1995

A buffer overflow flaw was found in the way the XListInputDevices() function of X.Org X11's libXi runtime library handled signed numbers. A malicious X11 server could possibly use this flaw to execute arbitrary code with the privileges of the user running an X11 client.

CVE-2013-2005

A flaw was found in the way the X.Org X11 libXt runtime library used uninitialized pointers. A malicious X11 server could possibly use this flaw to execute arbitrary code with the privileges of the user running an X11 client.

CVE-2013-2004

Two stack-based buffer overflow flaws were found in the way libX11, the Core X11 protocol client library, processed certain user-specified files. A malicious X11 server could possibly use this flaw to crash an X11 client via a specially crafted file.

The xkeyboard-config package has been upgraded to upstream version 2.11, which provides a number of bug fixes and enhancements over the previous version. (BZ#1077471)

Bug Fixes

BZ#1054614

Previously, updating the mesa-libGL package did not update the libX11 package, although it was listed as a dependency of mesa-libGL. This bug has been fixed and updating mesa-libGL now updates all dependent packages as expected.

BZ#971626

Previously, closing a customer application could occasionally cause the X Server to terminate unexpectedly. After this update, the X Server no longer hangs when a user closes a customer application.

The xkeyboard-config package has been upgraded to upstream version 2.11, which provides a number of bug fixes and enhancements over the previous version. (BZ#1077471)

All X11 client libraries users are advised to upgrade to these updated packages, which correct these issues and add these enhancements.

8.7. ABRT

8.7.1. RHBA-2014:1572 — abrt bug fix and enhancement update

Updated abrt packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The abrt packages provide the Automatic Bug Reporting Tool.

Bug Fix

BZ#1084467

Previously, kernel oops messages were deleted by ABRT, and thus the user was not sufficiently informed about the kernel behavior. With this update, kernel oops messages are kept and also supplemented by an explanation. The previous behavior can be restored in the newly created /etc/abrt/plugins/oops.conf file (man abrt-oops.conf).

In addition, this update adds the following

Enhancement

BZ#989530

With this update, ABRT messages include machine host name.

Users of abrt are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

8.8. AIDE

8.8.1. RHBA-2014:0948 — aide bug fix update

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

Advanced Intrusion Detection Environment (AIDE) is a utility that creates a database of files on the system, and then uses that database to ensure file integrity and detect system intrusions.

Bug Fixes

BZ#806911

Previously, the AIDE utility did not handle 'prelink' files properly if the prelink package was not installed. As a consequence, initializing the database by running the 'aide --init' command caused errors, and the database could not then be read with the 'aide --check' command. With this update, after running the 'aide --init' command in the described situation, a warning massage is displayed that prompts the user to install the prelink package first.

BZ#1119759

Prior to this update, the AIDE utility did not process the 'report_attributes' parameter correctly. Consequently, running the 'aide --check' command resulted in an incomplete report and a segmentation fault. A patch has been applied to address this bug, and AIDE now works as expected when reporting forced attributes.

Users of aide are advised to upgrade to these updated packages, which fix these bugs.

8.9. AKONADI

8.9.1. RHBA-2014:0539 — akonadi bug fix update

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

Akonadi is a storage service for personal information management (PIM) data and metadata. The service provides unique desktop-wide object identification and retrieval, and functions as an extensible data storage for all PIM applications.

Bug Fix

BZ#1073939

Previously, the Akonadi service used the hard-coded ~/.local/share/akonadi socket directory. As a consequence, the Akonadi server did not start if the home directory was located on Andrew File System (AFS), which did not support the creation of UNIX sockets. With this update, the directory that holds the sockets has been changed to '/tmp/[username]-akonadi.[random]'. As a result, Akonadi starts on systems with the home directory on AFS as expected.

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

8.10. ALSA-UTILS

8.10.1. RHBA-2014:1603 — alsa-utils bug fix update

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

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

Bug Fix

BZ#1072956

The alsa-utils packages have been updated with various upstream fixes to improve stability and usage.

Users of alsa-utils are advised to upgrade to these updated packages, which fix this bug.

8.11. AMTU

8.11.1. RHBA-2014:0639 — amtu bug fix update

Updated amtu package that fixes three bugs is now available for Red Hat Enterprise Linux 6.

The Abstract Machine Test Utility (AMTU) is an administrative utility to verify that the underlying protection mechanisms of the system hardware are being enforced correctly.

Bug Fixes

BZ#689823

Previously, Abstract Machine Test Utility (AMTU) did not handle the name of the interface correctly under certain circumstances. As a consequence, AMTU failed to obtain a list of network interfaces to test. With this update, the interface hardware type and carriers are obtained from the /sys/class/net/ directory. Now, only an Ethernet and a token ring can be used, and a carrier must be present. As a result, AMTU handles the new network interface names as expected.

BZ#723049

Prior to this update, AMTU ran network tests on interfaces configured with a static IP that did not have an existing connection, causing those tests to fail. With this update, AMTU no longer runs tests on interfaces that are not up.

BZ#1098076

Previously, the name of the network interface was restricted to 4 characters on 32-bit systems and 8 characters on 64-bit system due to using the sizeof() operator instead of the strlen() function. As a consequence, AMTU did not correctly display the full network interface name in certain portions of the output. A patch has been applied to address this bug, and AMTU now always displays the full network interface name as expected.

Users of amtu are advised to upgrade to the updated package, which fixes these bugs.

8.12. ANACONDA

8.12.1. RHBA-2014:1380 — anaconda bug fix and enhancement update

Updated anaconda packages that fix numerous bugs and add one enhancement 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#734121

When users of IBM System z had the kdump package installed, the default kernel was set to **`kernel-kdump`**. However, the **`zIPL`** utility ignored the **`Kdump`** and debugged kernels when creating the **`zipl.conf`** file. Consequently, after updating the system, the newly-installed kernel was not set as the default entry in **`zipl.conf`** since the default kernel has been set to **`kernel-kdump`**. Now, if a kernel name includes “-kdump”, such a kernel is not set as default instead of the newly-installed kernel.

BZ#979163

Under certain circumstances, downloading of a kickstart file could fail due slow network initialization. To address this bug, a new **`GATEWAY_PING_TIMEOUT`** option has been added to the Network Manager. The option checks connectivity to the server before reporting a network interface as being connected. With this update, **Anaconda** has been modified to use this feature by the **`nicedelay`** boot option that can now be used in cases of very slow network initialization.

BZ#1001960

No major release version was written to the boot menu for Red Hat Enterprise Linux. As a consequence, after installing on a multi-boot system, it was not clear which Red Hat Enterprise Linux entry corresponded to which major version. The boot menu entry now contains the major version of the Red Hat Enterprise Linux release. For Red Hat Enterprise Linux 6, this means there is the **`Red Hat Enterprise Linux 6`** entry. Note that there is not the minor version number, such as**`6.6`**. This is because there is currently no infrastructure to update the boot menu entry in place, so the entry would be incorrect after an upgrade.

BZ#1038001

When a bonding device was specified in the **`%pre`** section of a kickstart file and used with the **`%include`** kickstart option, **Anaconda** could not create the bond interface correctly. This update applies a patch to fix this bug and bonding interfaces are created as expected in the described scenario.

BZ#1039051

Previously, it was not possible to specify a local domain name by the kickstart **`network`** command. As a consequence, if a short host name was configured by the kickstart network **`--hostname`** option, name resolution of short names from local domain did not work properly in the **Anaconda** installer. A new **`--domain`** option for the **`network`** command has been added to address this bug.

BZ#1044716

When upgrading using **Anaconda**, it attempted to enable all swap devices listed in the **`/etc/fstab/`** directory on the system. However, **Anaconda** did not check whether the swap

devices existed. Consequently, non-existent swap devices listed in **/etc/fstab/** caused errors to be returned during an upgrade. With this update, when **Anaconda** encounters such a device, it displays a dialog window allowing the user to either skip the device or abort the upgrade.

BZ#1046320

The ***--percent*** parameter was omitted in the output kickstart file, even if it was provided in the input kickstart file. As a consequence, the installation would be less reproducible using the output kickstart file. With this update, the kickstart code has been modified to not omit the ***--percent*** parameter from the output kickstart file.

BZ#1067857

Previously, **Anaconda** did not check the VLAN ID that was passed as a boot parameter. Therefore, Anaconda could not retrieve a kickstart file on an NFS volume over a VLAN interface, because a VLAN connection had not been established. This update modifies **Anaconda** to check the VLAN ID.

BZ#1123791

During installation, the **/tmp/** size directory was always 250M. On systems with a large number of drives, large driver update disks, or a large number of repositories, **/tmp/** space could be exhausted, causing the installation to terminate unexpectedly. With this update, 50% of memory is reserved for **/tmp/** on systems with RAM greater than 512M, thus the installation proceeds correctly in the aforementioned scenario.

Enhancements

BZ#1081596

This update allows using the symbolic console device identifier for the ***cio_ignore*** kernel parameter in the **generic.prm** file for the IBM System z. Using this identifier prevents issues which may arise if no default console device number is available at installation time, or if the console device number is different from what was previously a hard-coded value in the **generic.prm** file. As a result, console devices using a different device identifier than what was previously hard-coded into the **generic.prm** file can be removed from the blacklist and made available for use.

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

8.13. AUDIT

8.13.1. RHBA-2014:1515 — audit bug fix and enhancement update

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

The audit packages contain the userspace utilities for storing and searching the audit records which have been generated by the audit subsystem in the Linux 2.6 kernel.

This update also fixes the following bug:

NOTE

The audit packages have been upgraded to upstream version 2.3.7, which provides a number of bug fixes and enhancements over the previous version, among which the following are especially note-worthy:

* The interpretation of the "ausearch -i" command, alternatively "ausearch --interpret", has been improved. * New event types are supported by the audit packages. * Remote logging bugs have been fixed. * The ausearch matching has been improved. * The augenrules utility support has been added to the audit packages. * Management of audispd plugins has been completely reworked. * The updated ausearch and aureport utilities can now produce reports from logs not included in the configured audit log directory by specifying the directory containing the logs on the command line. * The auditctl list rules command (the -l option) now outputs rules from the kernel in a new format which matches the formatting accepted to be loaded into the kernel. (BZ#1065067)

This update also fixes the following bug:

Bug Fixes

BZ#1065067

The interpretation of the "ausearch -i" command, alternatively "ausearch --interpret", has been improved. * New event types are supported by the audit packages. * Remote logging bugs have been fixed. * The ausearch matching has been improved. * The augenrules utility support has been added to the audit packages. * Management of audispd plugins has been completely reworked. * The updated ausearch and aureport utilities can now produce reports from logs not included in the configured audit log directory by specifying the directory containing the logs on the command line. * The auditctl list rules command (the -l option) now outputs rules from the kernel in a new format which matches the formatting accepted to be loaded into the kernel.

BZ#1028635

Previously, the audisp-remote plugin did not connect to the remote server after a transient "critical" network error. The underlying source code has been patched, and audisp-remote now connects to the remote server as intended.

The audit packages have been upgraded to upstream version 2.3.7, which provides a number of bug fixes and enhancements over the previous version, among which the following are especially note-worthy:

In addition, this update adds the following

Enhancements

BZ#96723

With this update, audit rules can be built from a directory of rule files. Rule files can be stored in the /etc/audit/rules.d/ directory based on what packages are installed. When rules need to be loaded into the kernel, they are now assembled into one master file by the augenrules utility and then loaded.

BZ#967240

This update adds a new command line option, --checkpoint. When invoked, the --checkpoint option causes the ausearch utility to report only new complete events on successive executions. This option is especially useful for running periodic reports that display the updates since the last report.

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

8.14. AUGEAS

8.14.1. RHBA-2014:1517 — augeas bug fix and enhancement update

Updated augeas packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

Augeas is a utility for editing configuration. Augeas parses configuration files in their native formats and transforms them into a tree. Configuration changes are made by manipulating this tree and saving it back into native configuration files. Augeas also uses "lenses" as basic building blocks for establishing the mapping from files into the Augeas tree and back.

Bug Fixes

BZ#1001635, BZ#1059383

Previously, the Grub lens did not support "setkey", "lock", and "foreground" directives, which caused virt-v2v process to terminate unexpectedly with an error message. The bug has been fixed, and virt-v2v process no longer fails.

BZ#1093711, BZ#1016904

When sudo configuration files, sudoers, contained directives with user aliases or group names using underscore characters, the sudoers lens was unable to parse the configuration file. With this update, underscores have been permitted in group names, and the sudoers lens now parses files successfully.

BZ#1033795

Prior to this update, when shell configuration files contained "export" lines with multiple variables or case statements with two semicolons (;;) on the same line as an expression, Augeas was unable to parse these files. With this update, Augeas handles multiple variables on the same export line and case statements with two semicolons as expected, and the aforementioned files are successfully parsed.

BZ#1043636

Previously, when the sysconfig lens was used to parse a shell configuration file containing a blank comment after another comment, the parsing process failed. The lens has been fixed to parse this combination of comments, and parsing is now finished successfully.

BZ#1062091

When parsing yum configuration files with spaces around key or value separators, Augeas was unable to parse the files. The underlying source code has been fixed, and yum configuration files are now parsed successfully.

BZ#1073072

Prior to this update, no generic lens existed for parsing the INI-style files, and parsing thus failed with an error message. The IniFile module has been fixed to contain generic lenses, and INI-style files are now parsed as intended.

BZ#1075112

When automounter maps contained references to hosts with host names containing hyphens, the automounter lens failed to parse the /etc/auto.export configuration file. A patch has been provided to fix this bug, and /etc/auto.export is now parsed as expected.

BZ#1083016

Prior to this update, the default rsyslog configuration file provided in Red Hat Enterprise Linux failed to parse using Augeas. The rsyslog lens has been fixed to parse the filters and templates used, and /etc/rsyslog.conf is now parsed successfully.

BZ#1100237

When Nagios Remote Plugin Executor (NRPE) configuration files contained the "allow_bash_command_substitution" option, the NRPE lens was unable to parse the files. A patch has been provided to fix this bug, and files with "allow_bash_command_substitution" are now parsed as intended.

In addition, this update adds the following

Enhancements

BZ#1016899

With this update, lenses have been added to parse configuration files relating to Red Hat JBoss A-MQ, including ActiveMQ configurations, ActiveMQ XML files, Jetty configuration, and JMX access files.

BZ#1016900

A new lens has been added to parse the Splunk configuration files, and thus the user can now manage Splunk configuration through the Puppet module.

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

8.15. AUTHCONFIG

8.15.1. RHBA-2014:1558 — authconfig bug fix and enhancement update

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

The authconfig packages contain 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#852997

Previously, the authconfig utility did not back up the /etc/passwd files, /etc/group, /etc/shadow, and /etc/gshadow files. As a consequence, if the "authconfig --restorebackup" command was run, these files were not reverted. With this update, authconfig backs up the aforementioned files, and when the "--restorebackup" option is used, it properly reverts the state of these files.

BZ#912851

Prior to this update, the authconfig utility did not properly read the LDAP base from the nslcd.conf file if there were multiple specific the LDAP bases specified. Consequently, the value of the LDAP base read from nslcd.conf was incorrect. With this update, authconfig ignores the specific LDAP bases, and reads and overwrites only the general LDAP base value.

BZ#975203

In some cases the authconfig utility was not able to properly detect whether SSSD or Winbind should be enabled. As a consequence, these daemons were stopped when authconfig was run although they should have not been effected. With this update, authconfig no longer changes the state nor restarts the services if the services configuration is not changed. As a result, the SSSD or Winbind runs after the execution of the "authconfig --update" command and does not effect any settings related to SSSD or Winbind.

BZ#1023294

When the "authconfig --disableipav2 --update" command was used, the "ipa-client-install --uninstall" command was not run. As a consequence, the IPA client was not properly deinitialized on the machine and the machine was not removed from the previously joined domain. The updated authconfig utility now correctly calls "ipa-client-install --uninstall" in the described scenario, and the IPA client of the machine is properly deinitialized, and the machine removed from the domain.

BZ#1025065

Prior to this update, the default umask when creating home directories with the pam_mkhomedir utility was 0022, which made these directories world-readable. To fix this bug, the "umask=0077" option with pam_mkhomedir is used by default, and the home directories newly created by pam_mkhomedir are no longer world-readable.

BZ#1119797

Previously, the ipa-client-install command used for the IPAv2 domain join was interactively asking for input. When called from the authconfig-gtk GUI, the user could not interact with it, and thus the domain join operation failed. With this update, the authconfig GUI uses the "ipa-client-install --unattended" command and no longer tries to interact with the user. As a result, the IPAv2 domain join operation is now successful.

In addition, this update adds the following

Enhancement

BZ#916574

The authconfig utility is now able to set up the automount entry in the nsswitch.conf file to pull information from the LDAP server via the SSSD client.

Users of authconfig are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.16. AUTOFS

8.16.1. RHBA-2014:1587 — autofs bug fix update

Updated autofs packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

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

Bug Fixes

BZ#994217

The am-utils package, which provides automatic mounting of maps in the amd format, is no longer supported in Red Hat Enterprise Linux 6. However, amd-formatted maps are still needed for example when using keys containing the forward slash (/), using wildcard matching for keys, or performing more complex actions after the key is matched. This update adds a parser for amd-formatted maps to the autofs utility.

BZ#1036032

If an IPv6 link-local address contained the percent sign (%), the autofs utility incorrectly reported the address as invalid. The mount location validity check has been updated, and the incorrect reports no longer occur in the described case.

BZ#1038696

When checking the mount option string, the automount daemon did not take into account the length of the string, which led to incorrect comparisons. As a consequence, the mount probes did not include NFS version 3 when the "-v" option was used, and under some circumstances, the mounts were not created properly. The option matching has been modified to account for option length, thus fixing this bug.

BZ#1046164

Due to previous changes to the autofs utility, autofs was not properly handling remote procedure calls (RPC) to probe server availability. Consequently, autofs was not querying the portmapper service for NFS version 2 and NFS version 3 mounts correctly. The RPC handling in autofs has been updated, and autofs now queries host availability properly.

BZ#1059549

The negative cache timeout was not handled properly by the autofs utility. Consequently, autofs was not correctly reading included automounter maps. This update fixes the handling of the negative cache in autofs.

BZ#1068999, BZ#1081285

The autofs utility did not apply mutual exclusion when using the initialization and termination functions from the OpenLDAP library. As these functions are not thread-safe, a double free error occurred and autofs terminated unexpectedly. This bug has been fixed by adding a mutual exclusion condition for the aforementioned OpenLDAP functions.

BZ#1073197

The autofs utility did not correctly process the output from the scandir() function. Consequently, autofs could terminate unexpectedly with a segmentation fault. The autofs utility has been modified to correctly read the scandir() output.

BZ#1081479

If the standard I/O file descriptors were closed by a process that started the autofs utility, autofs, before entering daemon state, could create file descriptor corresponding to one of the standard I/O file descriptors. When autofs entered daemon mode, these file descriptors were closed and autofs

terminated unexpectedly. Now, the device control file descriptor is closed after the autofs file system version check and a new descriptor is opened after autofs enters daemon mode.

BZ#1083744

The autofs utility did not properly check for entries that corresponded to previously failed mount attempts, the so-called "negative entries". Consequently, when the "autofs mount" command was specified with the "browse" option, the autofs utility could create directories that did not correspond to map entries within the corresponding automounter map. With this update, the check for negative map entries has been fixed.

BZ#1089576

When calling the autofs parser, the scan buffer was sometimes not properly reset for the next scan. Consequently, incorrect success returns occurred for subsequent operations. The autofs utility attempted to add these returned entries, which led to a segmentation fault. This bug has been fixed by adding a function that resets the parse buffer at the start of each map entry scan.

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

8.17. AVAHI

8.17.1. RHBA-2014:1535 — avahi bug fix update

Updated avahi packages that fix several bugs 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 Fixes

BZ#768708, BZ#885849

Previously, when the ARCOUNT field in the DNS Response Header contained a non-zero value, avahi-daemon performed a check and logged errors about invalid DNS packets being received. Note that a non-zero value of ARCOUNT is an indication of additional data sections in the DNS packet, but avahi-daemon does not interpret them. As a consequence, avahi-daemon was not sufficiently interoperable with other mDNS/DNS-SD implementations, and the automatic service discovery thus did not provide the user with the expected results on some platforms. Additionally, avahi-daemon logged inaccurate information which cluttered log files. The redundant check has been removed, and the described situation no longer occurs.

BZ#1074028

Previously, various options such as maximum count of cached resource records or numerous options related to handling of connected clients to the avahi-daemon could not be configured. As a consequence, in large networks, the avahi-daemon could reach the upper bound of some internal limits. In addition, the avahi-daemon was exhibiting erroneous behavior, such as logging error messages and failing to discover some services in large networks. To fix this bug, support for configuring various internal limits has been introduced with the following newly added options: cache-entries-max, clients-max, objects-per-client-max, entries-per-entry-group-max. For details about these options, see the avahi-daemon.conf(5) manual page.

Users of avahi are advised to upgrade to these updated packages, which fix these bugs. After installing the update, avahi-daemon will be restarted automatically.

8.18. BASH

8.18.1. RHBA-2014:1503 — bash bug fix update

Updated bash packages that fix several bugs 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#948207

Under certain circumstances, a file descriptor leak occurred in nested Bash functions. This bug has been fixed and file descriptors are no longer leaked in the described case.

BZ#951171

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" call caused the Bash shell to abort with a "double free or corruption (out)" error message. The applied patch corrects the tty driver to use the "-ERESTARTSYS" error code so the system call is restarted if needed. As a result, Bash no longer crashes in this scenario.

BZ#986095

When the HISTFILESIZE variable was set to a value larger than zero, the HISTSIZE variable was set to zero as well. If the .bash_history file had time stamps enabled and was not empty, executing the "su - " command caused Bash to become unresponsive. This bug has been fixed, and Bash no longer hangs in the aforementioned scenario.

BZ#1007926

Previously, Bash did not process quote characters correctly when using here-strings with multi-line input in a function declaration. Consequently, the declaration was corrupted, which affected copying such functions, or transferring them to another shell. This bug has been fixed, and here-strings with multi-line input are now processed correctly.

BZ#1010164

When processing larger associative arrays inside Bash scripts, a memory leak occurred. This bug has been fixed, and Bash no longer leaks memory when working with associative arrays.

BZ#1012015

If a command substitution enclosed in double-quote characters contained a double-quoted string, Bash performed brace expansion on the command before performing command substitution. Consequently, the command created different output than expected. The bug has been fixed, and command substitution now precedes brace expansion in the described case.

BZ#1102803

After editing a command in vi visual mode, Bash echoed every substituted command, which produced a lengthy shell output when editing loops. This behavior has been changed and Bash now only echoes the original string in the described scenario.

Users of bash are advised to upgrade to these updated packages, which fix these bugs.

8.19. BFA-FIRMWARE

8.19.1. RHBA-2014:1486 — bfa-firmware bug fix and enhancement update

Updated bfa-firmware package that fixes several bugs and adds various enhancements is 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 package has been upgraded to upstream version 3.2.23, which provides a number of bug fixes and enhancements over the previous version. (BZ#1054467)

All users of bfa-firmware are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

8.20. BIND

8.20.1. RHBA-2014:1373 — bind bug fix and enhancement update

Updated bind packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

BIND (Berkeley Internet Name Domain) is an implementation of the Domain Name System (DNS) 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 correctly.

Bug Fixes

BZ#1044545

Previously, the **`allow-notify`** configuration option did not take into account the Transaction SIGnature (TSIG) key for authentication. Consequently, this caused a slave server not to accept a **`NOTIFY`** message from a non-master server that used the TSIG key for authentication, even though the slave server was configured to accept **`NOTIFY`** messages when the specific TSIG key was used. The **named** source code has been fixed to also check the TSIG key ID when receiving a **`NOTIFY`** message from a non-master server, and the slave server now correctly accepts **`NOTIFY`** messages in this scenario.

BZ#1036700

Prior to this update, the Response Rate Limiting (RRL) functionality in **BIND** distributed in Red Hat Enterprise Linux 6 was missing the **`referrals-per-second`** and **`nodata-per-second`** options. As a consequence, users of **BIND** that was configured to use the RRL functionality could not explicitly filter empty responses for a valid domain and referrals or delegations to the server for a given

domain. With this update, the missing functionality has been backported to **BIND**, and users can now explicitly filter empty responses for a valid domain and referrals or delegations to the server for a given domain when using the RRL functionality in **BIND**.

BZ#1008827

Previously, the **host** utility used the same send buffer for all outgoing queries. As a consequence, under high network load, a race condition occurred when the buffer was used by multiple queries, and the **host** utility terminated unexpectedly with a segmentation fault when sending of one query finished after another query had been sent. The **host** utility source code has been modified to use a separate send buffer for all outgoing queries, and the described problem no longer occurs.

BZ#993612

Prior to this update, a bug in the **BIND** resolver source code caused a race condition, which could lead to prematurely freeing a fetch memory object. As a consequence, **BIND** could terminate unexpectedly with a segmentation fault when it accessed already freed memory. The **BIND** resolver source code has been fixed to guarantee that the resolver fetch object is not freed until there is no outstanding reference to that object, and **BIND** no longer crashes in this scenario.

BZ#1023045

Previously, the manual page for the **dig** utility contained upstream-specific options for an Internationalized Domain Name (IDN) library. Consequently, these options did not function as expected and users were incapable of disabling IDN support in dig following the steps from the manual page. The dig(1) manual page has been modified to include the options of the IDN library used in Red Hat Enterprise Linux and users can now successfully disable IDN support in **dig** following the steps from the manual page.

BZ#919545

Prior to this update, due to a regression, the **dig** utility could access an already freed query when trying multiple origins during domain name resolution. Consequently, the **dig** utility sometimes terminated unexpectedly with a segmentation fault, especially when running on a host that had multiple search domains configured in the **`/etc/resolv.conf`** file. The **dig** source code has been modified to always use a query that is still valid when trying the next origin, and the **dig** utility no longer crashes in this scenario.

BZ#1066876

Prior to this update, the **named** source code was unable to correctly handle the Internet Control Message Protocol (ICMP) Destination unreachable (Protocol unreachable) responses. Consequently, an error message was logged by **named** upon receiving such an ICMP response but **BIND** did not add the address of the name server to a list of unreachable name servers. This bug has been fixed, and no errors are now logged when the ICMP Destination unreachable (Protocol unreachable) response is received.

BZ#902431

Previously, the **`/var/named/chroot/etc/localtime`** file was created during the installation of the bind-chroot package, but its SELinux context was not restored. Consequently, **`/var/named/chroot/etc/localtime`** had an incorrect SELinux context. With this update, the command to restore the SELinux context of **`/var/named/chroot/etc/localtime`** after creation has been added in the post transaction section of the SPEC file, and the correct SELinux context is preserved after installing bind-chroot.

BZ#917356

Previously, the **/var/named/named.ca** file was outdated and the IP addresses of certain root servers were not valid. Although the **named** service fetches the current IP addresses of all root servers during its startup, invalid IP addresses can reduce performance just after a restart. Now, **/var/named/named.ca** has been updated to include the current IP addresses of root servers.

BZ#997743

Prior to this update, the **named** init script checked the existence of the **rndc.key** file only during the server startup. Consequently, the init script generated **rndc.key** even if the user had a custom Remote Name Daemon Control (RNDC) configuration. This bug has been fixed, and the init script no longer generates **rndc.key** if the user has a custom RNDC configuration.

BZ#919414

Previously, when calling the **sqlite** commands, the **zone2sqlite** utility used a formatting option that did not add single quotes around the argument. As a consequence, **zone2sqlite** was unable to perform operations on tables whose name started with a digit or contained the period (**.**) or dash (**-**) characters. With this update, **zone2sqlite** has been fixed to use the correct formatting option and the described problem no longer occurs.

BZ#980632

Previously, the **named** init script did not check whether the PID written in the **named.pid** file was a PID of a running **named** server. After an unclean shutdown of the server, the PID written in **named.pid** could belong to an existing process while the **named** server was not running. Consequently, the init script could identify the server as running and therefore the user was unable to start the server. With this update, the init script has been enhanced to perform the necessary check, and if the PID written in **named.pid** is not a PID of the running **named** server, the init script deletes the **named.pid** file. The check is performed before starting, stopping, or reloading the server, and before checking its status. As a result, the user is able to start the server without problems in the described scenario.

BZ#1025008

Prior to this update, **BIND** was not configured with the **--enable-filter-aaaa** configuration option. As a consequence, the **filter-aaaa-on-v4** option could not be used in the **BIND** configuration. The **--enable-filter-aaaa** option has been added, and users can now configure the **filter-aaaa-on-v4** option in **BIND**.

BZ#851123

Prior to this update, the **named** init script command **configtest** did not check if **BIND** was already running, and mounted or unmounted the file system into a chroot environment. As a consequence, the **named** chroot file system was damaged by executing the **configtest** command while the **named** service was running in a chroot environment. This bug has been fixed, and using the init script **configtest** command no longer damages the file system if **named** is running in a chroot environment.

BZ#848033

Previously, due to a missing statement in the **named** init script, the init script could return an incorrect exit status when calling certain commands (namely, **checkconfig**, **configtest**, **check**, and **test**) if the **named** configuration included an error. Consequently, for example, when the **service named configtest** command was run, the init script returned a zero value meaning success, regardless of the errors in the configuration. With this update, the init script has been fixed to correctly return a non-zero value in case of an error in the **named** configuration.

BZ#1051283

Previously, ownership of some documentation files installed by the bind package was not correctly set. Consequently, the files were incorrectly owned by **named** instead of the **root** user. A patch has been applied, and the ownership of documentation files installed by the bind package has been corrected.

BZ#951255

Prior to this update, the **/dev/random** device, which is a source of random data, did not have a sufficient amount of entropy when booting a newly installed virtual machine (VM). Consequently, generating the **/etc/rndc.key** file took excessively long when the **named** service was started for the first time. The init script has been changed to use **/dev/urandom** instead of **/dev/random** as the source of random data, and the generation of **/etc/rndc.key** now consumes a more reasonable amount of time in this scenario.

BZ#1064045

Previously, the **nsupdate** utility was unable to correctly handle an extra argument after the **-r** option, which sets the number of User Datagram Protocol (UDP) retries. As a consequence, when an argument followed the **-r** option, **nsupdate** terminated unexpectedly with a segmentation fault. A patch has been applied, and **nsupdate** now handles the **-r** option with an argument as expected.

BZ#948743

Previously, when the **named** service was running in a chroot environment, the init script checked whether the server was already running after it had mounted the chroot file system. As a consequence, if some directories were empty in the chroot environment, they were mounted again when the **service named start** command was used. With this update, the init script has been fixed to check whether **named** is running before mounting file system into the chroot environment and no directories are mounted multiple times in this scenario.

BZ#846065

Previously, **BIND** was not configured with the **--with-dlopen=yes** option. As a consequence, external Dynamically Loadable Zones (DLZ) drivers could not be dynamically loaded. A patch has been applied, and external DLZ drivers are now dynamically loadable as expected.

Enhancements

BZ#1092035

Previously, the number of workers and client-objects was hard-coded in the Lightweight Resolver Daemon (**lwresd**) source, and it was insufficient. This update adds two new options: the **lwres-tasks** option, which can be used for modifying the number of workers created, and the **lwres-clients** option, which can be used for specifying the number of client objects created per worker. The options can be used inside the **lwres** statement in the **named/lwresd** configuration file.

BZ#956685

This update adds support for the TLSA resource record type in input zone files, as specified in RFC 6698. TLSA records together with Domain Name System Security Extensions (DNSSEC) are used for DNS-Based Authentication of Named Entities (DANE).

Users of bind are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. After installing the update, the **BIND** daemon (**named**) will be restarted automatically.

8.21. BINUTILS

8.21.1. RHBA-2014:1414 — binutils bug fix update

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

The binutils packages provide a collection of binary utilities for the manipulation of object code in various object file formats. It includes the "ar", "as", "gprof", "ld", "nm", "objcopy", "objdump", "ranlib", "readelf", "size", "strings", "strip", and "addr2line" utilities.

Bug Fixes

BZ#1128279

Previously, the ld linker could overwrite a valid SONAME with an empty string in a DT_NEEDED record. Consequently, certain programs were linked but could not be executed because symbols from some libraries were not loaded. With this update, the ld linker correctly handles empty strings in SONAMEs, and programs linked by ld now can be executed as expected.

BZ#906079

When creating a shared library for a "ppc64" target, the ld linker selected linker stubs that were not thread-safe by default. Consequently, if such a shared library was used by a multi-threaded application, calls into the library could fail in unpredictable ways. To fix this problem, the ld linker now build shared libraries for "ppc64" targets with thread-safe linker stubs.

BZ#909056

The readelf utility incorrectly assumed that a long name table would always be available if an archive used long names. Consequently, readelf could terminate unexpectedly with a segmentation fault on archive libraries that used long names but did not have a long name table. To fix this problem, readelf now verifies the existence of a long name table on archive libraries.

BZ#959422

The ld linker incorrectly handled certain TLS relocations that appears in debugging (DWARF) sections. Consequently, debugging information for some variables in TLS sections could be incorrect. With this update, the ld linker now correctly handles TLS relocations in DWARF sections, and the related TLS variables now can be properly examined.

Users of binutils are advised to upgrade to these updated packages, which fix these bugs.

8.22. BIOSDEVNAME

8.22.1. RHBA-2014:1459 — biosdevname bug fix and enhancement update

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

The biosdevname packages contain an optional convention for naming network interfaces; it assigns names to network interfaces based on their physical location. Biosdevname is disabled by default, except for a limited set of Dell PowerEdge, C Series, and Precision Workstation systems.

NOTE

The biosdevname packages have been upgraded to upstream version 0.5.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#1053492)

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

8.23. BOOST

8.23.1. RHBA-2014:1440 — boost bug fix and enhancement update

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

The boost packages contain a large number of free peer-reviewed portable C++ source libraries. These libraries are suitable for tasks such as portable file-systems and time/date abstraction, serialization, unit testing, thread creation and multi-process synchronization, parsing, graphing, regular expression manipulation, and many others.

Bug Fixes

BZ#1037680

Due to the way the Python programming language was packaged for Red Hat Enterprise Linux, the boost packages could not be provided for secondary architectures. For example, boost-devel.i686 was not available on the x86-64 architecture. The Python packaging has been updated, and it is now possible to install secondary-architecture versions of the boost packages.

BZ#1021004

A coding error in the shared_ptr pointer previously caused a memory leak when serializing and unserializing shared pointers. The shared_ptr code has been corrected and the memory leak now no longer occurs.

BZ#969183

Due to an error in threading configuration of GNU Compiler Collection (GCC) version 4.7 or later, Boost failed to detect the support for multithreading versions of GCC. This patch fixes the error and Boost now detects multithreading support in the described circumstances correctly.

BZ#1108268

Prior to this update, a number of boost libraries were not compatible with GCC provided with Red Hat Developer Toolset. A fix has been implemented to address this problem and the affected libraries now properly work with Red Hat Developer Toolset GCC.

BZ#801534

The mpi.so library was previously missing from the boost libraries. Consequently, using the Message Passing Interface (MPI) in combination with Python scripts failed. With this update, mpi.so is included in the boost packages and using MPI with Python works as expected.

In addition, this update adds the following

Enhancement

BZ#1132455

The MPICH2 library has been replaced with a later version, MPICH 3.0. Note that Boost packaging has been updated accordingly and new packages are named boost-mpich* instead of boost-mpich2*.

Users of Boost are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.24. C-ARES

8.24.1. RHBA-2014:1478 — c-ares bug fix and enhancement update

Updated c-ares packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The c-ares C library defines asynchronous DNS (Domain Name System) requests and provides name resolving API.

NOTE

The c-ares packages have been upgraded to upstream version 1.10.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#1077544)

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

8.25. CA-CERTIFICATES

8.25.1. RHEA-2014:1500 — ca-certificates enhancement update

Updated ca-certificates package that adds various enhancements is now available for Red Hat Enterprise Linux 6.

The ca-certificates package contains a set of CA certificates chosen by the Mozilla Foundation for use with the Internet Public Key Infrastructure (PKI).

The ca-certificate package has been upgraded to version 2014.1.98, released with Network Security Services (NSS) version 3.16.1, which provides a number of enhancements over the previous version. (BZ#1035355)

Users of ca-certificates are advised to upgrade to this updated package, which adds these enhancements.

8.26. CCID

8.26.1. RHBA-2014:1531 — ccid bug fix update

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

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 that follow this standard.

Bug Fix

BZ#1071366

Smart Card readers have multiple modes, some of which have limitations on the size of commands that can be sent to the Smart Card. Previously, OmniKey 3121 supported the modes of operation that allowed longer commands, but not in the standard CCID way. As a consequence, the user received an unrecoverable error message when running a long command. This update recognizes OmniKey 3121 and enables the longer modes so that longer commands are successfully executed on the Smart Card.

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

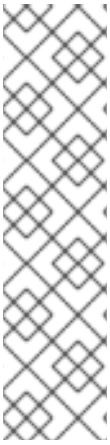
8.27. CERTMONGER

8.27.1. RHBA-2014:1512 — 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 service monitors certificates, warning of their impending expiration, and optionally attempting to re-enroll with supported Certificate Authorities (CA).

This update also fixes the following bugs:



NOTE

The certmonger packages have been upgraded to upstream version 0.75.13, which provides a number of bug fixes and enhancements over the previous version including: - support for retrieving an IPA server's root certificate and optionally storing it to specified locations - improvements in how the certmonger daemon handles disconnection from the system message bus - improvements in how the certmonger daemon runs enrollment helpers and parses results returned by them - fixed bug causing unexpected termination if an attempt to save a certificate failed - fixed incorrect use of the libdbus library that triggered the _dbus_abort() function - fixed segmentation fault with incorrectly structured entries in the /var/lib/certmonger/cas/ directory (BZ#1098208, BZ#948993, BZ#1032760, BZ#1103090, BZ#1115831)

This update also fixes the following bugs:

Bug Fix

BZ#1125342

This update fixes the implementation of the remove_known_ca dbus call in the certmonger package to prevent the certmonger daemon from terminating unexpectedly when called by remove_known_ca.

The certmonger packages have been upgraded to upstream version 0.75.13, which provides a number of bug fixes and enhancements over the previous version including: - support for retrieving an IPA

server's root certificate and optionally storing it to specified locations - improvements in how the certmonger daemon handles disconnection from the system message bus - improvements in how the certmonger daemon runs enrollment helpers and parses results returned by them - fixed bug causing unexpected termination if an attempt to save a certificate failed - fixed incorrect use of the libdbus library that triggered the _dbus_abort() function - fixed segmentation fault with incorrectly structured entries in the /var/lib/certmonger/cas/ directory (BZ#1098208, BZ#948993, BZ#1032760, BZ#1103090, BZ#1115831)

In addition, this update adds the following

Enhancement

BZ#1027265

This update adds the certmonger_selinux manual page to document the effect that SELinux has in limiting the allowed access to locations for the certmonger daemon. Also, the selinux.txt document has been added to the certmonger package to provide more details about interaction with SELinux. A reference to certmonger_selinux and selinux.txt has been added to other certmonger man pages.

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

8.28. CLUSTER

8.28.1. RHBA-2014:1420 — cluster bug fix and enhancement update

Updated cluster packages that fix several bugs and add one enhancement 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.

Bug Fixes

BZ#843160

Previously, the fencing time comparison did not work as expected when fence agent completed too fast or the corosync callback was delayed. Consequently, the Distributed Lock Manager (DLM) became unresponsive when waiting for fencing to complete. With this update, different time stamps that are not effected by the sequence of fencing or corosync callbacks are now saved and compared, and DLM no longer hangs in the aforementioned situation.

BZ#1059269

Prior to this update, the "pcs stonith confirm <node>" command failed to acknowledge the STONITH fencing technique. As a consequence, any requests from other nodes in the cluster or from clients in the same node became ignored. A patch has been provided to fix this bug, and "pcs stonith confirm" now works as expected, fencing the specified node successfully.

BZ#1029210

Due to an error in the configuration, the qdisk daemon in some situations used an incorrect "tko" parameter for its wait period when initializing. Consequently, qdisk initialization could be significantly delayed and, under some circumstances, failed entirely. With this update, the cluster configuration file has been fixed, and qdisk initialization now proceeds as expected.

BZ#980575

Previously, the ccs_read_logging() function used the create_daemon_path() function to generate daemon-specific CCS paths for the attributes. As a consequence, attributes on individual logging_daemons were not applied correctly. This bug has been fixed, and attributes on individual logging_daemons are now applied correctly.

BZ#979313

Due to a code error in corosnync, after the corosync utility terminated unexpectedly with a segmentation fault, the qdiskd daemon evicted other cluster nodes. The underlying source code has been patched, and qdiskd no longer evicts the other nodes if corosync crashes.

BZ#1074551

Prior to this update, running the "ccs_tool -verbose" command caused ccs_tool to terminate unexpectedly with a segmentation fault. This bug has been fixed, and ccs_tool now returns an error message providing more information.

BZ#1059853

Due to an overly restrictive umask, running the "gfs2_grow" command changed the /etc/mtab file permissions from default 644 to 600. A patch has been provided to fix this bug, and gfs2_grow no longer resets /etc/mtab permissions.

BZ#1062742

Previously, fsck.gfs2 did not fix corrupt quota_change system files. As a consequence, attempts to mount the file system (FS) resulted in an error, even though fsck.gfs2 reported the FS to be clean. With this patch, if fsck.gfs2 finds a corrupted quota_change file, it can rebuild it. Now, GFS2 mounts successfully as intended.

BZ#1080174

Previous attempts to mount a GFS2 file system that had already been mounted prevented further mount attempts from other nodes from completing. With this update, mount.gfs2 no longer leaves the mount group when the file system is already mounted, and attempts to mount an already mounted GFS2 file system are handled properly.

BZ#1053668

Prior to this update, a GFS2 volume failed to mount after conversion from GFS to GFS2, and the gfs2_convert utility aborted with a segmentation fault. The gfs2-utils code has been patched to fix this bug, and the aforementioned conversions now proceed successfully.

In addition, this update adds the following

Enhancement

BZ#1081517

To aid debugging and administration, fsck.gfs2 now logs a message to the system log when it starts and ends.

Users of cluster are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.29. CLUSTERMON

8.29.1. RHBA-2014:1582 — clustermon bug fix update

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

The clustermon packages are used for remote cluster management. The modclusterd service provides an abstraction of cluster status used by the Conga architecture and by the Simple Network Management (SNMP) and Common Information Model (CIM) modules of clustermon.

Bug Fix

BZ#1076716

Previously, the modcluster service mishandled requests with size in bytes divisible by 4096, which is the size of the read buffer in bytes. Consequently, modcluster incorrectly evaluated such requests as errors. This bug has been fixed, and modcluster now processes all requests as expected.

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

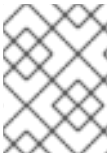
8.30. CMAKE

8.30.1. RHBA-2014:1506 — cmake bug fix and enhancement update

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

CMake is used to control the software compilation process using simple platform and compiler independent configuration files. CMake generates native makefiles and workspaces that can be used in the compiler environment of your choice. CMake is quite sophisticated: it is possible to support complex environments requiring system configuration, preprocessor generation, code generation, and template instantiation.

This update also fixes the following bugs:



NOTE

The cmake packages have been upgraded to upstream version 2.8.12, which provides a number of bug fixes and enhancements over the previous version. (BZ#606892)

This update also fixes the following bugs:

Bug Fixes

BZ#611250

Previously, the FindGTK2.cmake module was missing from the cmake packages. As a consequence, building GTK2 applications failed. This update adds FindGTK2.cmake and GTK2 applications now build as expected.

BZ#752864

Prior to this update, CMake ignored some options when working with the rpmbuild-4.8 package. As a consequence, building RPM packages on an RPM-based system failed. With this update, CMake works with rpmbuild-4.8 correctly, and the above problem no longer occurs.

BZ#896116

Due to an error in the "add_custom_target" command, CMake previously did not detect a custom target after creating it. With this update "add_custom_target" works properly, and CMake detects a created custom target as expected.

The cmake packages have been upgraded to upstream version 2.8.12, which provides a number of bug fixes and enhancements over the previous version. (BZ#606892)

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

8.31. COOLKEY

8.31.1. RHBA-2014:1611 — coolkey bug fix update

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

Coolkey is a smart card support library for the CoolKey, Common Access Card (CAC), and Personal Identity Verification (PIV) smart cards.

Bug Fix

BZ#1125987

A certain variable was previously uninitialized in the coolkey code. If that variable inherited a single "magic" value, coolkey could fail to present any certificates or keys that were stored in a smart card controlled by coolkey (a CAC, PIV, or coolkey card). Consequently, although the smart card was recognized, the certificates and keys were not visible to some applications. With this update, that variable is now initialized to a safe value and coolkey now presents its certificates and keys properly.

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

8.32. COREUTILS

8.32.1. RHBA-2014:1457 — coreutils bug fix and enhancement update

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

The coreutils packages contain the core GNU utilities. It is a combination of the old GNU fileutils, sh-utils, and textutils packages.

Bug Fixes

BZ#812449

Previously, the "df" command did not display target device information when a symbolic link was specified as a parameter. Consequently, the information about the file was shown instead of the information about the device. This update applies a patch to fix this bug and the "df" command works

as expected in the described scenario.

BZ#1016163

When no user was specified, the "id -G" and "groups" commands printed the default group ID listed in the password database. Consequently, the IDs were in certain cases ineffective or incorrect. With this update, the commands have been enhanced to print only proper IDs, thus showing correct information about the groups.

BZ#1046818

A previous update of the coreutils packages fixed the tail utility to handle symbolic links correctly. However, due to this update, tail returned unnecessary warnings about reverting to polling. This update provides a patch to fix this bug and the warning is only shown when necessary.

BZ#1057026

A recent update of the coreutils packages changed the format of the output from the "df" and "df -k" commands to one line per entry, which is required for POSIX mode. As a consequence, scripts relying on the previous two lines per entry format started to fail. To fix this bug, two-line entries have been reintroduced to the output for modes other than POSIX. As a result, scripts relying on the two-line format no longer fail.

BZ#1063887

A recent update of the coreutils packages caused a regression in the signal handling in the su utility. As a consequence, when the SIGTERM signal was received, a parent process was killed instead of the su process. With this update, handling of the SIGTERM signal has been fixed and su no longer kills the parent process upon receiving the termination signal.

BZ#1064621

The chcon(1) manual page did not describe the default behavior when dereferencing symbolic links; the "--dereference" option was not documented. This update adds the appropriate information to the manual page.

BZ#1075679

Certain file systems, for example XFS, have special features such as speculative preallocation of memory holes. These features could cause a failure of the "dd" command test in the upstream test suite. As a consequence, the coreutils package source rpm could not be rebuilt on XFS file systems. To address this bug, the test has been improved to prevent the failures in the described scenario.

BZ#1104244

The "tail --follow" command uses the inotify API to follow the changes in a file. However, inotify does not work on remote file systems and the tail utility is supposed to fall back to polling for files on such file systems. Previously, the Veritas file system was missing from the remote file system list and therefore, "tail --follow" did not display the updates to the file on this file system. The Veritas file system has been added to the remote file system list and the problem no longer occurs.

In addition, this update adds the following

Enhancement

BZ#1098078

This update enhances the "dd" command to support the count_bytes input flag. When the flag is specified, the count is treated as numbers of bytes rather than blocks. This feature is useful for example when copying virtual disk images.

Users of coreutils are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

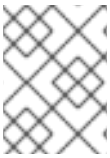
8.33. COROSYNC

8.33.1. RHBA-2014:1508 — corosync bug fix update

Updated corosync packages that fix several bugs 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.

This update also fixes the following bugs:



NOTE

The corosync packages have been upgraded to upstream version 1.4.7, which provides a number of bug fixes over the previous version. (BZ#1055584)

This update also fixes the following bugs:

Bug Fixes

BZ#1067043

If the cpg clients on active cluster nodes terminated while corosync on one of the nodes was paused, corosync did not update its internal information about cpg clients on other nodes properly after resuming. Consequently, that node considered the terminated cgp clients to be still up and running. This update modifies the cpg code to ensure that corosync properly updates information about the cpg membership in this situation.

BZ#1011307

Previously, corosync terminated unexpectedly with a segmentation fault when started on a system with the /dev/shm device full. This happened because the corosync logging system, logsys, could not be properly initialized. This update improves handling of the logsys initialization, and corosync now displays an appropriate error message and exits gracefully if logsys cannot be initialized.

BZ#1025321

Due to a list corruption bug in the Corosync Closed Process Group (CPG) API, corosync could terminate unexpectedly with a segmentation fault under some circumstances. To fix this problem, corosync has been modified to handle the CPG init and list removal functions in the same thread.

BZ#1005179

Previously, corosync could abort without logging an error properly if it was unable to store a file to the user's file system. With this update, corosync now properly verifies whether a "blackbox" can be stored on the file system. A failure of a ring ID store operation is no longer handled by assert but corosync now tries to log an error and then exits gracefully.

BZ#1001210

Previously, when using the InfiniBand Architecture (IBA) as a transport protocol for corosync, corosync could not properly handle the restart of the IBA subnet manager (SM). If the IBA SM was restarted, corosync was not able to start or became unresponsive if it was already running. A series of patches addressing this problem has been applied to corosync, and it now works properly as expected in this scenario.

The corosync packages have been upgraded to upstream version 1.4.7, which provides a number of bug fixes over the previous version. (BZ#1055584)

Users of corosync are advised to upgrade to these updated packages, which fix these bugs.

8.34. CPUPOWERUTILS

8.34.1. RHBA-2014:1422 — cpupowerutils bug fix and enhancement update

Updated cpupowerutils packages that fix several bugs and add one enhancement 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).

Bug Fix

BZ#1056310, BZ#1109187

Prior to this update, the turbostat utility did not correctly access the energy status register on certain Intel Core processors. As a consequence, turbostat displayed the following error message:

/dev/cpu/0/msr offset 0x641 read failed

With this update, turbostat has been fixed to correctly access the proper energy status registers. As a result, turbostat now returns the expected data in the described scenario.

In addition, this update adds the following

Enhancement

BZ#1093513

This update adds support for the Intel Broadwell Microarchitecture to the turbostat utility.

Users of cpupowerutils are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.35. CRASH-TRACE-COMMAND

8.35.1. RHBA-2014:1462 — crash-trace-command bug fix update

Updated crash-trace-command packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The crash-trace-command packages provide the trace extension module for the crash utility, allowing it to read ftrace data from a core dump file.

Bug Fix

BZ#895899

Previously, crash-trace-command displayed incorrect "Packager" and "Vendor" information. With this update, crash-trace-command prints "Red Hat, Inc." in these fields as expected.

Users of crash-trace-command are advised to upgrade to these updated packages, which fix this bug.

8.36. CRDA

8.36.1. RHEA-2014:1607 — crda enhancement update

Updated crda packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The crda packages contain the Central Regulatory Domain Agent that provides the kernel with the wireless regulatory rules for a given jurisdiction.

Users of crda are advised to upgrade to these updated packages, which add this enhancement.

8.37. CREATEREPO

8.37.1. RHBA-2014:0491 — createrepo bug fix and enhancement update

An updated createrepo package that fixes three bugs and adds two enhancements is now available for Red Hat Enterprise Linux 6.

The createrepo package contains a set of utilities used to generate and maintain a common metadata repository from a directory of rpm packages.

Bug Fixes

BZ#1035588

Previously, the createrepo utility did not test file locking correctly. As a consequence, createrepo terminated unexpectedly with a traceback when it was executed in a directory located on a Common Internet File System (CIFS) share provided by a NetApp storage appliance. The test for file locking has been corrected and createrepo now works as expected in the described situation.

BZ#1083185

Prior to this update, if the createrepo utility was executed with the "-i" or "--pkglist" options and the specified file name did not exist, createrepo terminated unexpectedly with a traceback. The createrepo utility has been modified to handle this error condition properly, and it now exits gracefully in this situation.

BZ#1088886

Prior to this update, the createrepo packages had descriptions which did not indicate that the maintenance utilities were present in the package. This update corrects this omission.

In addition, this update adds the following

Enhancements

BZ#952602

This update introduces support for the following new options to the modifyrepo utility: "--checksum", used to specify the checksum type; "--unique-md-filenames", used to include the file's checksum in the file name; and "--simple-md-filenames", used to not include the file's checksum in the file name. The "--unique-md-filenames" option is a default option for this utility.

BZ#1093713

Previously, certain options were not described in the modifyrepo(1) and mergerepo(1) man pages. These man pages now document the following modifyrepo utility command line options: "--mdtype", "--remove", "--compress", "--no-compress", "--compress-type", "--checksum", "--unique-md-filenames", "--simple-md-filenames", "--version", and "--help". These man pages also now document the following mergerepo utility command line options: "--no-database", "--compress-type", "--version", and "--help".

Users of createrepo are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

8.38. CRYPTSETUP-LUKS

8.38.1. RHEA-2014:1593 — cryptsetup-luks enhancement update

Updated cryptsetup-luks packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The cryptsetup-luks packages provide a utility which allows users to set up encrypted devices with the Device Mapper and the dm-crypt target.

Enhancement

BZ#1009707

FIPS products are now defined by the presence of the dracut-fips package in the system. During the initialization of a library, a cryptographic module is supposed to determine if the library is a FIPS product to reduce the amount of required integrity tests. For this purpose, a new constructor function has been added to the cryptsetup-libs library. The constructor detects if the /etc/system-fips file, which is a part of dracut-fips, exists in the system, and determines if a FIPS integrity test is needed.

Users of cryptsetup-luks are advised to upgrade to these updated packages, which add this enhancement.

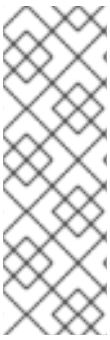
8.39. CTDB

8.39.1. RHEA-2014:1488 — ctdb bug fix and enhancement update

Updated ctdb packages that fix several bugs and add various enhancements 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.

This update also fixes the following bugs:



NOTE

The ctdb package has been upgraded to upstream version 2.5.1, which provides a number of bug fixes and enhancements over the previous version. Note that due to these changes, the new version cannot run in parallel with the previous versions on the same cluster. In addition, note that to update CTDB in an existing cluster, CTDB has to be stopped on all nodes in the cluster before the upgrade can start. Furthermore, back up your cluster nodes in case the update fails. To ensure easy recovery in case of update failure, only a single node should be updated at a time. (BZ#1061630, BZ#1085447)

This update also fixes the following bugs:

Bug Fixes

BZ#987099

Prior to this update, CTDB sometimes waited too long for file locks to establish. Consequently, clients accessing a CTDB file-server cluster could time out due to high latency. With this update, the underlying code has been fixed to address the problem, and clients can now access files on a CTDB file-server cluster without timeouts.

BZ#1075913

Previously, when CTDB was configured to use two bonded interfaces, CTDB failed to assign an IP address to the second bonded interface. As a consequence, the cluster status of the cluster node was shown as "PARTIALLYONLINE" even when the actual status was "OK". The script which handles the network interfaces has been fixed and the cluster status now shows the correct value.

BZ#1085413

Prior to this update, CTDB under some circumstances attempted to free allocated memory at an invalid address which caused CTDB to terminate unexpectedly with a segmentation fault. This update fixes the underlying code and CTDB uses the correct address for freeing allocated memory. As a result, the crash no longer occurs.

The ctdb package has been upgraded to upstream version 2.5.1, which provides a number of bug fixes and enhancements over the previous version. Note that due to these changes, the new version cannot run in parallel with the previous versions on the same cluster. In addition, note that to update CTDB in an existing cluster, CTDB has to be stopped on all nodes in the cluster before the upgrade can start. Furthermore, back up your cluster nodes in case the update fails. To ensure easy recovery in case of update failure, only a single node should be updated at a time. (BZ#1061630, BZ#1085447)

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

8.40. CUPS

8.40.1. RHSA-2014:1388 — Moderate: cups security and bug fix update

Updated cups 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 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.

CUPS provides a portable printing layer for Linux, UNIX, and similar operating systems.

Security Fixes

CVE-2014-2856

A cross-site scripting (XSS) flaw was found in the CUPS web interface. An attacker could use this flaw to perform a cross-site scripting attack against users of the CUPS web interface.

CVE-2014-3537CVE-2014-5029CVE-2014-5030CVE-2014-5031

It was discovered that CUPS allowed certain users to create symbolic links in certain directories under **`/var/cache/cups/`**. A local user with the **`lp`** group privileges could use this flaw to read the contents of arbitrary files on the system or, potentially, escalate their privileges on the system.

The CVE-2014-3537 issue was discovered by Francisco Alonso of Red Hat Product Security.

Bug Fixes

BZ#769292

When the system was suspended during polling a configured BrowsePoll server, resuming the system left the **`cups-polld`** process awaiting a response even though the connection had been dropped causing discovered printers to disappear. Now, an HTTP timeout is used so the request can be retried. As a result, printers that use BrowsePoll now remain available in the described scenario.

BZ#852846

A problem with HTTP multipart handling in the CUPS scheduler caused some browsers to not work correctly when attempting to add a printer using the web interface. This has been fixed by applying a patch from a later version, and all browsers now work as expected when adding printers.

BZ#855431

When a discovered remote queue was determined to no longer be available, the local queue was deleted. A logic error in the CUPS scheduler caused problems in this situation when there was a job queued for such a destination. This bug has been fixed so that jobs are not started for removed queues.

BZ#884851

CUPS maintains a cache of frequently used string values. Previously, when a returned string value was modified, the cache lost its consistency, which led to increased memory usage. Instances where this happened have been corrected to treat the returned values as read-only.

BZ#971079

A missing check has been added, preventing the scheduler from terminating when logging a message about not being able to determine a job's file type.

BZ#978387

A fix for incorrect handling of collection attributes in the Internet Printing Protocol (IPP) version 2.0 replies has been applied.

BZ#984883

The CUPS scheduler did not use the **fsync()** function when modifying its state files, such as **printers.conf**, which could lead to truncated CUPS configuration files in the event of power loss. A new **cupsd.conf** directive, ***SyncOnClose***, has been added to enable the use of **fsync()** on such files. The directive is enabled by default.

BZ#986495

The default environment variables for jobs were set before the CUPS configuration file was read, leading to the ***SetEnv*** directive in the **cupsd.conf** file having no effect. The variables are now set after reading the configuration, and ***SetEnv*** works correctly.

BZ#988598

Older versions of the RPM Package Manager (RPM) were unable to build the cups packages due to a newer syntax being used in the spec file. More portable syntax is now used, allowing older versions to build CUPS as expected.

BZ#1011076

A spelling typo in one of the example options for the **cupsctl** command has been fixed in the **cupsctl(8)** man page.

BZ#1012482

The **cron** script shipped with CUPS had incorrect permissions, allowing world-readability on the script. This file is now given permissions “0700”, removing group- and world-readability permissions.

BZ#1040293

The Generic Security Services (GSS) credentials were cached under certain circumstances. This behavior is incorrect because sending the cached copy could result in a denial due to an apparent “replay” attack. A patch has been applied to prevent replaying the GSS credentials.

BZ#1104483

A logic error in the code handling the web interface made it not possible to change the **Make and Model** field for a queue in the web interface. A patch has been applied to fix this bug and the field can now be changed as expected.

BZ#1110045

The CUPS scheduler did not check whether the client connection had data available to read before reading. This behavior led to a 10 second timeout in some instances. The scheduler now checks for data availability before reading, avoiding the timeout.

BZ#1120419

The Common Gateway Interface (CGI) scripts were not executed correctly by the CUPS scheduler, causing requests to such scripts to fail. Parameter handling for the CGI scripts has been fixed by applying a patch and the scripts can now be executed properly.

All cups users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the **cupsd** daemon will be restarted automatically.

8.41. CYRUS-SASL

8.41.1. RHBA-2014:1570 — cyrus-sasl bug fix and enhancement update

Updated cyrus-sasl packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The cyrus-sasl packages contain the Cyrus implementation of Simple Authentication and Security Layer (SASL). SASL is a method for adding authentication support to connection-based protocols.

Bug Fixes

BZ#838628

A memory leak in the Digest MD5 plugin was discovered. Specifically, the make_client_response() function did not correctly free the output buffer. Consequently, applications that used Digest MD5 with very large datasets could terminate unexpectedly. This update corrects make_client_response() and closes the memory leak. As a result, applications using Digest MD5 as part of authentication with large datasets now work as expected.

BZ#1081445

Previously, unnecessary quote characters were used in the cyrus-sasl.spec file when the user was created using the useradd command. Consequently, the Saslauth user was created with quotes in the comment field ("Saslauthd user"). With this update, unnecessary quotes have been removed from the comment field.

In addition, this update adds the following

Enhancement

BZ#994242

The ad_compat option has been backported to the cyrus-sasl packages from upstream. This option controls compatibility with AD or similar servers that require both integrity and confidentiality bits selected during security layer negotiation.

Users of cyrus-sasl are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.42. DEVICE-MAPPER-MULTIPATH

8.42.1. RHBA-2014:1555 — device-mapper-multipath bug fix and enhancement update

Updated device-mapper-multipath packages that fix several 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#1009061

When running a command on a specific device, the multipath utility did not accept device specification using the major:minor format. This bug has been fixed, and a multipath device can now be associated with the multipath command using a path device major:minor specification.

BZ#1027061

Previously, the readsector0 checker did not consider the blocksize when calculating the number of blocks to read, which led to readsector0 reading too much on 512 byte devices causing device errors. With this update, readsector0 considers the device blocksize when calculating the amount to read, and 512 byte devices now work with the readsector0 checker as intended.

BZ#1049637

Prior to this update, the code that handles multipathd sysfs devices could free a device structure while other data still pointed to it. As a consequence, the multipathd daemon could occasionally experience use-after-free memory corruption leading to unexpected termination. The sysfs device handling code for multipathd has been rewritten, and multipathd no longer frees sysfs device memory while it is still in use.

BZ#1078485

Some of multipathds prioritizers run scsi commands with long timeouts. These prioritizers do not run asynchronously and multipathd becomes busy waiting for one to timeout. Consequently, the multipathd daemon can become unresponsive for as long as 5 minutes when a path fails. With this update, the prioritizers use the "checker_timeout" option to configure their timeout. Now, prioritizer timeouts can be adjusted using the checker_timeout option to prevent multipathd hangs.

BZ#1080052

When a multipath device was reloaded outside the multipathd daemon and existing paths were removed from the device, mutipathd still treated them as belonging to a multipath device. Consequently, multipathd tried to access a non-existent path_group and terminated unexpectedly. With this update, multipathd correctly disassociates removed paths and no longer crashes when existing paths are removed by external programs.

BZ#1086417

If the multipathd daemon failed to add a path to the multipath device table, the path was incorrectly orphaned. As a consequence, the multipath utility treated the path as belonging to a multipath device, and multipathd could keep attempting to switch to a non-existent path_group. The underlying source code has been fixed, and multipathd now correctly orphans paths that cannot be added to the multipath device table.

In addition, this update adds the following

Enhancements

BZ#1054747

This update adds the force_sync multipath.conf option. Setting force_sync to "yes" keeps the multipathd daemon from calling the path checkers in asynchronous mode, which forces multipathd to run only one checker at a time. In addition, with this option set, multipathd no longer takes up a significant amount of CPU when a large number of paths is present.

BZ#1088013

Previously, the default path ordering often led to the Round Robin path selector picking multiple paths to the same controller, reducing the performance benefit from multiple paths. With this update,

multipath reorders device paths in order to alternate between device controllers, leading to a performance improvement.

BZ#1099932

This update adds iscsi support for the "fast_io_fail_tmo" option to allow the user to modify the speed of multipath responding to failed iscsi devices.

BZ#1101101

With this update, "-w" and "-W" options have been added to multipath; the "-w" option removes the named WWID from the wwids file, the "-W" option removes all WWIDs from the wwids file except for the WWIDs of the current multipath devices.

8.43. DEVICE-MAPPER-PERSISTENT-DATA

8.43.1. RHBA-2014:1409 — device-mapper-persistent-data bug fix and enhancement update

Updated device-mapper-persistent-data packages that fix one bug and add two enhancements are now available.

The device-mapper-persistent-data packages provide device-mapper thin provisioning (thinp) tools.

This update adds thin provisioning tools to support the dm-cache, as well as the dm-era functionality for change tracking to the device-mapper-persistent-data packages in Red Hat Enterprise Linux 6 as a Technology Preview. (BZ#1038236, BZ#1084081)

More information about Red Hat Technology Previews is available here:
https://access.redhat.com/support/offerings/techpreview/

In addition, this update fixes the following bug:

Bug Fix

BZ#1035990

The thin_dump utility as well as other persistent-data tools supported only 512 B block sizes on accessed devices. Consequently, persistent-data tools could perform I/O to misaligned buffers. The underlying source code has been updated to support 4 KB block size, thus fixing this bug.

This update adds thin provisioning tools to support the dm-cache, as well as the dm-era functionality for change tracking to the device-mapper-persistent-data packages in Red Hat Enterprise Linux 6 as a Technology Preview. (BZ#1038236, BZ#1084081)

More information about Red Hat Technology Previews is available here:
https://access.redhat.com/support/offerings/techpreview/

Users of device-mapper-persistent-data are advised to upgrade to these updated packages, which fix this bug and add these enhancements.

8.44. DHCP

8.44.1. RHBA-2014:1406 — dhcp bug fix update

Updated dhcp packages that fix several bugs 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 Fixes

BZ#1015997

When a packet with checksum having the value of 0xffff was received by the dhcpd daemon, the packet was discarded. With this update, checksum with value 0xffff is perceived as correct, and the packet is now processed as intended.

BZ#1053155

Previously, the user could not run IPv6 version of the dhcrelay service, because there was no such initiation script. To fix this bug, the initiation script of dhcrelay has been added, and the user can now run service for IPv6 version of dhcrelay.

BZ#1053431

When IPv6 version of the dhcpd daemon served too many requests, the /var/lib/dhcpd/dhcpd.leases file grew uncontrollably in size. As a consequence, dhcpd refused to restart with the following error message:

file is too long to buffer

An upstream patch has been backported to fix this bug, and dhcpd for IPv6 now rotates /var/lib/dhcpd/dhcpd.leases to prevent it from growing.

BZ#1064416

When using ISC DHCP server and clients on Infiniband cards (IPoIB), the hardware address, called GUID, did not appear in logs. This update adds GUIDs to the logs for IPoIB.

BZ#1067142

Every time the dhcpd daemon started, the ownership of the /var/lib/dhcpd/dhcpd.leases file was changed from dhcpd:dhcpd to root:root. A Fedora patch has been backported to fix this bug, and the ownership of /var/lib/dhcpd/dhcpd.leases no longer changes.

BZ#1099698

When having failover configuration of the dhcpd daemon and using very long lease times for clients, the following error was returned when starting dhcpd:

unable to write lease

A patch has been applied to fix this bug, and error messages no longer appear in logs.

BZ#1102662

Previously, when starting the dhcpd daemon or the dhcrelay agent, the user specified the name of the network interface. If longer than 15 characters, dhcpd or dhcrelay terminated unexpectedly with the following error message:

*** buffer overflow detected ***

A patch has been backported to fix this bug, and dhcpd or dhcrelay now exit gracefully with a new error message informing the user that the interface name is too long.

Users of dhcp are advised to upgrade to these updated packages, which fix these bugs.

8.45. DING-LIBS

8.45.1. RHBA-2014:1496 — ding-libs bug fix and enhancement update

Updated ding-libs packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The ding-libs packages contain a set of libraries used by the System Security Services Daemon (SSSD) and other projects and provide functions to manipulate filesystem pathnames (libpath_utils), a hash table to manage storage and access time properties (libdhash), a data type to collect data in a hierarchical structure (libcollection), a dynamically growing, reference-counted array (libref_array), and a library to process configuration files in initialization format (INI) into a library collection data structure (libini_config).

NOTE

The ding-libs packages have been upgraded to upstream version 0.3.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#1069287)

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

8.46. DNSMASQ

8.46.1. RHBA-2014:0757 — dnsmasq bug fix update

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

The dnsmasq packages contain Dnsmasq, a lightweight domain name system (DNS) forwarder and dynamic host configuration protocol (DHCP) server.

Bug Fix

BZ#991473

Previously, the Dnsmasq service status verification in the init script was not sufficiently robust and only determined the presence of all the instances of Dnsmasq running on the system. As a consequence, the init script identified Dnsmasq as running even when no Dnsmasq system instance had been initiated. The init script has been fixed to explicitly verify the process with the process ID written in the PID file of the system instance. As a result, the status of the Dnsmasq system instance is now identified correctly even if there are running instances not started by the init script.

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

8.47. DRACUT

8.47.1. RHBA-2014:1492 — dracut bug fix and enhancement update

Updated dracut packages that fix several bugs and add one enhancement 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#1022766

The Anaconda "fcoe=edd:<dcb_setting>" option was introduced to allow systems in multi-path configuration to boot from the Storage Area Network (SAN). Previously, the option worked correctly only with the systems that used Enhanced Disk Drive Services (EDD) BIOS. Consequently, systems that did not use EDD, such as UEFI-based systems, could fail to boot from SAN. With this update, the option has been enhanced to work correctly with all systems.

BZ#1026302

In FIPS mode, the self checking of binaries is only done if the /etc/system-fips file is present. The dracut utility did not copy /etc/system-fips and certain checksum files in the initial ram file system (initramfs). As a consequence, the self check of the binaries, which was needed to decrypt a partition, was not done so that the partition could not been unlocked. Now, dracut copies all the needed files in the initramfs, and systems with encrypted disks can now boot successfully in FIPS mode.

BZ#1033784

The dracut(8) manual page did not describe certain new features. With this update, the missing information has been added to the manual page.

BZ#1041484

The nvme driver was missing from the initrd images. Consequently, when Red Hat Enterprise Linux was installed on a non-volatile memory express (NVMe) storage, the post-installation reboot failed. This update adds the missing driver and Red Hat Enterprise Linux can be installed on NVMe storages as expected.

BZ#1051448

Only the plymouth module was responsible for creating the initramfs /emergency/ directory. When the module was omitted during the installation, /emergency/ was not created. This behavior caused errors to be returned because other modules required /emergency/ too. With this update, /emergency/ is created regardless of loaded modules.

BZ#1070676

The /dev/btrfs-control device node is only created, after the btrfs kernel module is loaded. Previously, utilities that attempted to access the node prior to the module was loaded terminated unexpectedly. Now, the dracut initramfs environment statically creates the device node. As a result, when a utility tries to access the node, the kernel loads btrfs automatically so that the utility no longer fails in the described scenario.

BZ#1099603

The iscsistart utility, which is used for adding iSCSI disks, could be executed only when network interfaces had been brought up successfully. When the interfaces had not been correctly specified on the kernel command line, it was not possible to run the utility and boot the system from iSCSI disks. Now, when iSCSI disks are requested on the kernel command line, the dracut initramfs environment runs iscsistart even if no network interface is properly specified, thus allowing the system to boot from iSCSI disks.

BZ#1126346

With the iSCSI server not being available, the iscsistart utility took a very long time to connect to it, which slowed the boot process. With this update, iscsistart is now launched in the background, thus connecting to the iSCSI server as soon as it is available. As a result, booting no longer takes enormous amount of time.

In addition, this update adds the following

Enhancement

BZ#737687

This update enables the server to boot from a secondary device in case the primary device fails. The new "rootfallback=<secondary_device>" parameter has been added to the dracut parameters. This parameter is used when the primary device specified with the "root=<primary_device>" parameter cannot be found.

Users of dracut are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.48. E2FSPROGS

8.48.1. RHBA-2014:1566 — e2fsprogs bug fix and enhancement 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#1036122

The resize2fs utility sometimes caused file system corruption during an offline resize of an ext4 file system. This happened because resize2fs did not reserve all existing metadata blocks prior to executing the resize operation. This update fixes resize2fs to reserve all existing metadata blocks as expected in this situation.

BZ#1040122

The tune2fs man page states that the "-f" option can be used to remove a file system journal even if the journal requires replay. However, earlier versions of tune2fs did not behave as documented. This update allows tune2fs to remove a dirty journal by supplying two "-f" options on the command line.

BZ#1093446

With previous versions of mke2fs, it was possible to specify an unsupported and unmountable file system revision on the command line by using the "-r" option. The mke2fs utility now refuses to create a file system with a revision higher than is currently supported.

BZ#1097061

Previously, the e2image program could run against a mounted block device, resulting in an inconsistent metadata image. With this update, the e2image program now displays a warning message if the block device is mounted, and requires the "-f" option to proceed in this case.

BZ#1112242

With previous versions of e2fsck, "zeroed-out" directory blocks were not reported or repaired. The e2fsck utility now detects and repairs this type of corruption.

In addition, this update adds the following

Enhancement

BZ#1052409

The enable_periodic_fsck option has been added to /etc/mke2fs.conf to enable or disable periodic e2fsck operations when creating new file systems with the mke2fs utility. A periodic file system check is enabled by default.

Users of e2fsprogs are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.49. EDAC-UTILS

8.49.1. RHBA-2014:0768 — edac-utils bug fix update

An updated edac-utils package that fixes one bug is now available for Red Hat Enterprise Linux 6.

Error Detection And Correction (EDAC) is the current set of drivers in the Linux kernel that handles detection of ECC errors from memory controllers for most chipsets on the 32-bit x86, AMD64, and Intel 64 architectures. The user-space component consists of an init script which ensures that EDAC drivers and DIMM labels are loaded at system startup, as well as a library and utility for reporting current error counts from the EDAC sysfs files.

Bug Fix

BZ#679812

Previously, the exit status of the edac-utils package init script was not set correctly. As a consequence, running the 'service edac status' command returned exit status 0, which was not expected behavior because no programs were running after executing the 'service edac start' command. With this update, the returned exit status has been changed to 3 in the described situation.

Users of edac-utils are advised to upgrade to this updated package, which fixes this bug.

8.50. EFIBOOTMGR

8.50.1. RHBA-2014:1616 — efibootmgr bug fix update

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

The efibootmgr utility is responsible for the boot loader installation on Unified Extensible Firmware Interface (UEFI) systems.

Bug Fix

BZ#1121782

Previously, during their boot process, some newer machines created variables larger than 1024 bytes, which the kernel API for Unified Extensible Firmware Interface (UEFI) does not support. Consequently, the efibootmgr utility received an error trying to read such variables, and skipped them, which caused anaconda to fail to create boot variables. This update changes efibootmgr to show the variables but not to display their contents. As a result, anaconda is able to read the large variables, and creates boot variables successfully.

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

8.51. ELFUTILS

8.51.1. RHEA-2014:1472 — elfutils bug fix and enhancement update

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

The elfutils packages contain a number of utility programs and libraries related to the creation and maintenance of executable code.

This update also fixes the following bugs:

NOTE

The elfutils packages have been upgraded to upstream version 0.158, which provides a number of bug fixes and enhancements over the previous version. The most notable additions include:

* This update introduces an eu-stack tool that retrieves the backtrace of a process or a core file. * The elfutils libdwfl() functions have been extended to provide support for associating a process state to a Dwfl object. A state can be attached to a process or a core file using the new dwfl_core_file_attach() and dwfl_linux_proc_attach() functions. When a state is attached to a Dwfl object, a new function, dwfl_getthreads(), can be used to iterate over the running threads. It is possible for each thread to unwind and inspect the frames on the call stack using the new dwfl_getthread_frames() function. * The libraries and utilities provide various improvements to recognize DWARF version 4, DWARF GNU tool chain extensions (typed DWARF stack, call_site, entry_value, DW_AT_high_pc, DW_OP_GNU_parameter_ref, and experimental support for DWZ multifiles), and new functions to handle DWARF location expressions. * The eu-readelf utility now supports the "/SYM64/" special entry to read 64-bit ar archive files used on IBM System z architecture. (BZ#755728, BZ#1059897)

This update also fixes the following bugs:

Bug Fixes

BZ#755728, BZ#1059897

This update introduces an eu-stack tool that retrieves the backtrace of a process or a core file. * The elfutils libdwfl() functions have been extended to provide support for associating a process state to a Dwfl object. A state can be attached to a process or a core file using the new dwfl_core_file_attach() and dwfl_linux_proc_attach() functions. When a state is attached to a Dwfl object, a new function, dwfl_getthreads(), can be used to iterate over the running threads. It is possible for each thread to unwind and inspect the frames on the call stack using the new dwfl_getthread_frames() function. * The libraries and utilities provide various improvements to recognize DWARF version 4, DWARF GNU tool chain extensions (typed DWARF stack, call_site, entry_value, DW_AT_high_pc, DW_OP_GNU_parameter_ref, and experimental support for DWZ multifiles), and new functions to handle DWARF location expressions. * The eu-readelf utility now supports the "/SYM64/" special entry to read 64-bit ar archive files used on IBM System z architecture.

BZ#1101440

Prior to this update, the eu-readelf utility was unable to read a corrupted ELF file with a missing string table. As a consequence, eu-readelf terminated unexpectedly with a segmentation fault. With this update, eu-readelf has been fixed to skip the data sections with a non-existent string table and read only valid data. As a result, eu-readelf no longer crashes in this scenario.

BZ#806474

Previously, due to bugs in certain tool chain utilities, the main ELF file and the separate debuginfo file had different header types or flags. As a consequence, the eu-unstrip utility was unable to combine the ELF file and the separate debuginfo file. The same problem occurred when the main ELF file was prelinked after the debug information was separated into a debuginfo file. With this update, eu-unstrip displays a warning message similar to "ELF header identification (e_ident) different" and shows which header field does not match if the stripped and unstripped files cannot be combined. Also, the "--force" option has been added so that the user can ignore the warning and combine such files anyway. Additionally, eu-unstrip prints a warning message if the DWARF data need adjusting for prelinking bias. As a result, eu-unstrip now prints appropriate warning messages and the mismatching main ELF and separate debuginfo files can be recombined into one using the "--force" option.

The elfutils packages have been upgraded to upstream version 0.158, which provides a number of bug fixes and enhancements over the previous version. The most notable additions include:

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

8.52. ETHTOOL

8.52.1. RHBA-2014:1421 — ethtool bug fix and enhancement update

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

Ethtool is a utility that enables querying and changing settings such as speed, port autonegotiation, PCI locations, and checksum offload on many network devices, especially on ethernet devices.

Bug Fixes

BZ#1003891

Previously, the ethtool utility did not support the Backplane link type. As a consequence, ethtool did not return "supported link modes" and "advertised link modes" on be2net-based devices. With this update, the support for Backplane has been added, and ethtool now returns "supported link modes" and "advertised link modes" as expected.

BZ#1010843

Previously, the ethtool utility did not correctly communicate with the network device driver when attempting to set Large Receive Offload (LRO) options. Consequently, it was not possible to set the LRO options on devices supporting LRO. With this update, ethtool has been fixed to communicate correctly with the network device driver, and the LRO options can now be set on network devices.

BZ#1018367

Due to a change to the ixgbe driver, the "ethtool -d" command in non-raw mode stopped providing output. As a consequence, "ethtool -d" could not be used to examine the state of ixgbe devices. To fix this bug, ethool has been changed to work with the new ixgbe device driver, and the "ethtool -d" command in non-raw mode can now be used again on the ixgbe devices.

In addition, this update provides the following

Enhancement

BZ#1105589

With this update, the ethtool utility supports the Medium Dependent Interface Crossover (MDI-X) mode setting on the e1000, e1000e, and igb drivers.

Users of ethtool are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.53. EVOLUTION

8.53.1. RHBA-2014:1416 — evolution bug fix update

Updated evolution packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Evolution is a GNOME application that provides integrated email, calendar, contact management and communications functionality. The components which make up Evolution are tightly integrated with one another and act as a seamless personal information-management (PIM) tool.

Bug Fixes

BZ#1052955

Previously, the option to choose the time format in the Evolution application was not offered for certain languages. As a consequence, the calendar component editor always showed time in the 24-hour format. With this update, the correct time format is displayed based on the selection the user makes in the Edit menu: Preferences, Calendar and Tasks.

BZ#1054772

Prior to this update, newly created local address books were not set correctly. Consequently, address books in the Evolution application could not be deleted, and incorrect data was displayed. With this update, address books can be removed, contacts in separated address books remain visible only in

the appropriate address books, and the add, edit, and remove operations no longer cause any inconsistency.

BZ#1054865

Previously, the Evolution application did not always handle adding new attachments correctly. As a consequence, attaching a large file caused the Evolution application to terminate unexpectedly under certain circumstances. A patch has been applied to address this bug, and adding new attachments no longer causes Evolution to crash.

BZ#1070846

Previously, the Evolution application displayed only a general prompt for the Smart Card PIN. As a consequence, the user could be uncertain what PIN to enter. This update improves the prompt, and the user now knows what certificate the requested PIN belongs to.

BZ#1080467

Prior to this update, the Evolution application did not correctly handle calling the "Mark All As Read" function. Consequently, Evolution could become unresponsive until the operation was completely finished. A patch has been provided to fix this problem, and Evolution no longer hangs in the described situation.

BZ#1139166

Previously, an error could occur when displaying a new email notification. As a consequence, the Evolution application did not work correctly under certain circumstances. With this update, the bug has been fixed and email notifications are correctly displayed.

Users of evolution are advised to upgrade to these updated packages, which fix these bugs. All running instances of Evolution must be restarted for this update to take effect.

8.54. EVOLUTION-DATA-SERVER

8.54.1. RHBA-2014:1418 — evolution-data-server bug fix and enhancement update

Updated evolution-data-server packages that fix one bug and add one enhancement 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#1040178

Due to incorrect locking of table access, Evolution previously became unresponsive on startup. This update fixes locking of table access, and Evolution now starts up as intended.

In addition, this update adds the following

Enhancement

BZ#1042996

With this update, support for TLS version 1.2 for mail accounts has been added to Evolution.

Users of evolution-data-server are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

8.55. FENCE-AGENTS

8.55.1. RHBA-2014:1562 — fence-agents bug fix update

Updated fence-agents packages that fix several 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#641632, BZ#642232, BZ#841556, BZ#1114528

Previously, timeout options could not be entered to the fence_brocade agent. In addition, issued commands were not persistent, which could lead to problems if fencing hardware was rebooted. Also, when invalid password was entered, the fence agent was terminated as a stale process without any error message being reported to the user. This update provides a new implementation of fence agents that solves the aforementioned bugs.

BZ#990537

Previously, users of the fence_ilo agent were not able to enter password that contained the quotation mark character ("). This update allows users to enter any character in the password as expected.

BZ#1018263

If the user name to log in to the fence_vmware_soap device does not have the correct privileges set, a python exception is thrown. Prior to this update, the fence_vmware_soap agent terminated the exception when the user did not have privileges for required operations. With this update, the user is informed by an error message that these privileges are not sufficient.

BZ#1048842

Previously, fence agents could use key-based authentication over SSH even if the user wanted to use password authentication. As a consequence, the user was unable to log in. This update ensures that proper authentication is used, and the user can now log in using password authentication.

BZ#1050022

Previously, using the fence_scsi_check.pl watchdog script failed to induce soft or clean reboot. But when Global File System 2 (GFS2) or other file systems were used, unmounting file systems could be blocked. This update provides a new fence_scsi_check_reboot.pl script, which ensures hard reboot, and problems with unmounting no longer occur.

BZ#1051159

Prior to this update, the fence_vmware_soap fencing agent did not support the "--delay" option, which is indispensable for avoiding fence races. This update adds the "--delay" option, which delays start of fence agents for a given amount of seconds, and thus prevents fence races from occurring.

BZ#1069618

Previously, the fence_apc utility was hard-coded with SSH1 connectivity. As a consequence, fence_apc was unable to connect to power distribution units that required SSH2 connectivity. This update introduces the "--ssh-options" option, which makes it possible to specify SSH connectivity options in fence_apc. Thus, all fencing agents that support SSH can now be adjusted to meet the SSH requirements of the fencing device.

BZ#1110428

Previously, the fence_rsb agent was unable to work with certain versions of firmware. As a consequence, fence_rsb failed after an outlet powered off. However, fence_rsb kept on issuing the command to power the outlet back on. With this update, new firmware versions are supported, and fence_rsb succeeds in turning off and on the outlet.

BZ#1075683

Prior to this update, fence agents that connected using the SSH protocol failed on login if an identity file was used as the method of authentication. The bug has been fixed, and these fence agents now successfully authenticate through an identity file.

Users of fence-agents are advised to upgrade to these updated packages, which fix these bugs.

8.56. FENCE-VIRT

8.56.1. RHBA-2014:1589 — 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#1014238

Previously, the manual page for the fence_virt.conf file did not describe the relationship between socket path for fence_virtd and virtual machine serial socket path. This could cause confusions or misunderstandings. With this update, the description of "path" in the manual page has been extended to explain the aforementioned difference.

BZ#1104740

Prior to this update, the fence-virt agent could not fence inactive virtual machines. As a consequence, the cluster became unresponsive because the fence_virtd daemon was unable to find the running domain. The underlying source code has been patched, and fence-virt now fences both active and inactive virtual machines.

In addition, this update adds the following

Enhancements

BZ#914144

With this update, the libvirt backend of the fence_virt daemon has been extended to support multiple KVM hypervisors.

BZ#1054225

With this update, fence-virt fencing using KVM serial ports instead of network multicast is supported for production use.

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

8.57. FILE

8.57.1. RHSA-2014:1606 — Moderate: file security and bug fix update

Updated file packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 "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.

Security Fixes

CVE-2014-0237, CVE-2014-0238, CVE-2014-3479, CVE-2014-3480, CVE-2012-1571

Multiple denial of service flaws were found in the way file parsed certain Composite Document Format (CDF) files. A remote attacker could use either of these flaws to crash file, or an application using file, via a specially crafted CDF file.

CVE-2014-1943, CVE-2014-2270

Two denial of service flaws were found in the way file handled indirect and search rules. A remote attacker could use either of these flaws to cause file, or an application using file, to crash or consume an excessive amount of CPU.

Bug Fixes

BZ#664513

Previously, the output of the "file" command contained redundant white spaces. With this update, the new STRING_TRIM flag has been introduced to remove the unnecessary white spaces.

BZ#849621

Due to a bug, the "file" command could incorrectly identify an XML document as a LaTex document. The underlying source code has been modified to fix this bug and the command now works as expected.

BZ#873997

Previously, the "file" command could not recognize .JPG files and incorrectly labeled them as "Minix filesystem". This bug has been fixed and the command now properly detects .JPG files.

BZ#884396

Under certain circumstances, the "file" command incorrectly detected NETpbm files as "x86 boot sector". This update applies a patch to fix this bug and the command now detects NETpbm files as expected.

BZ#980941

Previously, the "file" command incorrectly identified ASCII text files as a .PIC image file. With this update, a patch has been provided to address this bug and the command now correctly recognizes ASCII text files.

BZ#1037279

On 32-bit PowerPC systems, the "from" field was missing from the output of the "file" command. The underlying source code has been modified to fix this bug and "file" output now contains the "from" field as expected.

BZ#1064463

The "file" command incorrectly detected text files as "RRDTool DB version ool - Round Robin Database Tool". This update applies a patch to fix this bug and the command now correctly detects text files.

BZ#1067771

Previously, the "file" command supported only version 1 and 2 of the QCOW format. As a consequence, file was unable to detect a "qcow2 compat=1.1" file created on Red Hat Enterprise Linux 7. With this update, support for QCOW version 3 has been added so that the command now detects such files as expected.

All file users are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

8.58. FILE-ROLLER

8.58.1. RHBA-2014:0642 — file-roller bug fix update

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

File Roller is an application for creating and viewing archives files, such as tar or zip files.

Bug Fix

BZ#718338

Previously, the file-roller application did not correctly handle file names with spaces. As a consequence, an error could occur when adding files to an archive because names with spaces were not properly recognized by file-roller, for example when using the 'Compress' menu item in the Nautilus file manager. With this update, file-roller uses the correct API to handle file names. As a result, archives are created as expected and errors no longer occur in the described situation.

Users of file-roller are advised to upgrade to these updated packages, which fix this bug.

8.59. FINGER

8.59.1. RHBA-2014:0587 — finger bug fix update

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

The finger utility allows users to display information about users on the system, including their login names, full names, and the time they logged in to the system.

Bug Fix

BZ#816328

When the "compat" method is specified in the nsswitch.conf file, special entries containing the "+" or "-" characters are allowed to be used in the /etc/passwd file. Previously, when the finger utility was run with a "username" argument on a host that had the special entries in /etc/passwd, finger terminated with a segmentation fault. With this update, the code that handles the "username" argument has been fixed to perform the necessary checks and the finger utility no longer crashes in the described scenario.

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

8.60. FLEX

8.60.1. RHBA-2014:1402 — flex bug fix update

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

The flex packages provide a utility for generating scanners. The scanners are programs that can recognize lexical patterns in text.

Bug Fix

BZ#570661

Previously, the flex static libraries for 32-bit and 64-bit architectures were included in the same package. Consequently, an attempt to compile an i386 code on an x86_64 system failed unless the 64-bit version of the flex utility had been removed. With this update, the libraries have been moved to separate packages, and flex works as expected in the described scenario.

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

8.61. FONTCONFIG

8.61.1. RHBA-2014:0554 — fontconfig bug fix update

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

The fontconfig packages contain the font configuration and customization library, which is designed to locate fonts within the system and select them according to the requirements specified by the applications.

Bug Fixes

BZ#1035416

Previously, when the font cache file was stored on a Network File System (NFS), the fontconfig library sometimes did not handle mmap() calls correctly. As a consequence, applications using fontconfig, for example the GNOME terminal, could terminate unexpectedly with a bus error. With this update, the FONTCONFIG_USE_MMAP environment variable has been added to handle the mmap() calls regardless of the file system, and these calls are no longer used if the cache file is stored on an NFS. As a result, the bus errors no longer occur in the described situation.

BZ#1099546

Previously, the 25-no-bitmap-fedora.conf file name contained the word 'fedora', although file names in Red Hat Enterprise Linux are not supposed to include the word 'Fedora'. With this update, 25-no-bitmap-fedora.conf has been renamed to 25-no-bitmap-dist.conf, and the spec file has been updated.

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

8.62. FREERADIUS

8.62.1. RHEA-2014:1609 — freeradius enhancement update

Updated freeradius packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

FreeRADIUS is a high-performance and highly configurable free Remote Authentication Dial In User Service (RADIUS) server, designed to allow centralized authentication and authorization for a network.

Enhancement

BZ#1107843

Under certain conditions, the proxy server needs the ability to time out to the home server in less than a second. With this update, three new features addressing this requirement have been added:

The home server's "response_window" configuration option now accepts fractional values with down to microsecond precision and the minimum of one millisecond.

The "response_window" configuration option with the same precision is now also supported in client sections to enable lowering of the home server's response window for specific clients.

The "response_timeouts" configuration option is now supported in home server sections, allowing to specify the number of times when a request is permitted to miss the response window before the home server enters the defunct state.

Users of freeradius are advised to upgrade to these updated packages, which add this enhancement.

8.63. GCC

8.63.1. RHBA-2014:1377 — gcc bug fix and enhancement update

Updated gcc packages that fix numerous bugs and add one enhancement 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#858351

Previously, the GNU Compiler Collection (GCC) did not handle compiling partial specialization invalid C++ code correctly. As a consequence, GCC could terminate unexpectedly with a segmentation fault. The bug has been fixed and GCC now provides a translation-time error instead of crashing.

BZ#875472

Previously, the GNU Compiler Collection (GCC) did not handle loop vectorization correctly. Consequently, GCC could terminate with a segmentation fault. With this update, GCC correctly ignores the debug statements when the vectorizer is looking for a loop-exit PHI node, and GCC now compiles the code as expected.

BZ#1008798

Previously, after compiling the source code of a program using the "-fprofile-arcs" and "-ftest-coverage" command-line options, the program was run and the gcov utility was started, but after that, a new source code file was created and gcov was started again. As a consequence, gcov damaged the existing .gcda files. After this update, functions are properly restored if a failure occurs, and gcov no longer damages other files.

BZ#1027003

Previously, if an invalid code in gnu++11 mode used an initializer list with an invalid value in its constructor, the g++ compiler terminated with a segmentation fault. With this update, the constructor is better tested for incorrect values, and g++ no longer crashes in the described scenario.

BZ#1061435

Previously, the Clang compiler did not handle certain headers correctly. As a consequence, a program using the typeinfo and exception headers failed to compile, and an "incomplete type" error message was displayed. With this update, the exception header in the libstdc++ library has been adjusted, and programs now compile as expected with the Clang compiler.

BZ#1085442

Previously, the standard uncaught_exception() function returned the "True" value even when the initialization of the exception object was not complete. As a consequence, the GNU Compiler Collection (GCC) could generate wrong code. With this update, uncaught_exception() returns the "True" value only after the exception object is created, and GCC always generates correct code as expected.

BZ#1087806

Prior to this update, the g++ compiler rejected code that tried to pass a type with a non-trivial copy constructor through variable arguments. As a consequence, programs compiled with the GNU Compiler Collection (GCC) terminated unexpectedly with an "Illegal instruction" error message. With this update g++ now accepts the code because it treats passing variadic arguments of non-trivial types as a pass-by-invisible reference.

BZ#1113793

Previously, the gfortran compiler did not correctly handle compiling code that involved invalid old-style initialization for derived type components. As a consequence, gfortran could terminate unexpectedly with a segmentation fault. A patch has been applied to address this bug, and the code is now properly rejected when needed, and an appropriate error message is displayed.

BZ#1113878

Larger aggregate contains the same fields as the smaller one with just some fields added at the end. Prior to this update, optimizing code that contained conversion from a larger aggregate to a smaller aggregate could cause the GNU Compiler Collection (GCC) to generate incorrect code. Consequently, using GCC with turned on optimizations failed and a segmentation fault occurred. With this update, conversions between aggregates with different sizes are never considered useless, and GCC no longer generates incorrect code in the described situation.

Enhancements

BZ#1099549

OpenMP 4.0 support has been added to the GNU OpenMP library, which allows applications built with DTS 3.0 and using OpenMP to link on Red Hat Enterprise Linux 6.

Users of gcc are advised to upgrade to these updated packages, which which fix these bugs and add this enhancement.

8.64. GCC-LIBRARIES

8.64.1. RHBA-2014:1438 — gcc-libraries bug fix and enhancement update

Updated gcc-libraries packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The gcc-libraries packages contain various GNU Compiler Collection (GCC) runtime libraries, such as libatomic and libitm.

NOTE

The gcc-libraries packages have been upgraded to upstream version 4.9.0, which provides a number of bug fixes and enhancements over the previous version to match the features in Red Hat Developer Toolset 3.0. Among others, this update adds the libcilkrts library to gcc-libraries. (BZ#1062230, BZ#1097800)

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

8.65. GDB

8.65.1. RHBA-2014:1534 — gdb bug fix and enhancement update

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

The gdb packages provide the GNU Debugger (GDB) to debug 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#1104587

Previously, when the users tried to debug certain core dump files generated from multi-threaded applications, GDB was unable to handle correctly specific situations, for example, when a referenced DWARF Compilation Unit was aged out. As a consequence, performing the "thread apply all bt" command to display a backtrace of all threads could cause GDB to terminate unexpectedly. A patch has been provided to fix this bug, and GDB no longer crashes in this scenario.

BZ#913146

Previously, when executing the signal handling code, GDB was calling certain non-reentrant functions, such as the calloc() function. This could sometimes result in a deadlock situation. To avoid deadlocks in this scenario, the relevant GDB code has been modified to handle non-reentrant functions correctly.

BZ#1007614

Previously, due to a bug in a specific function in the support for Python, if a Python script read a memory region from the program that was being debugged, and the reference to the memory region became out of scope, GDB did not deallocate the memory. As a consequence, this led to a memory leak, which was particularly significant in memory-intensive scenarios. A patch has been applied, and GDB now frees the acquired memory correctly.

BZ#903734

Prior to this update, GDB did not add the necessary offsets when dealing with bit fields inside nested instances of the struct data type. Consequently, when the user tried to set the value of a bit field that was declared inside such a data structure, GDB was unable to calculate it correctly. With this update, GDB calculates the values of bit fields inside nested data structures correctly.

BZ#1080656

Previously, GDB was unable to correctly access Thread Local Storage (TLS) data on statically linked binaries. Consequently, the user could not inspect TLS data on the program being debugged if the program was linked statically. This bug has been fixed, and users can now inspect TLS data on statically linked binaries as expected.

BZ#981154

Prior to this update, GDB incorrectly handled symbolic links related to build-id files. As a consequence, when the user tried to debug core dump files generated from programs that were not installed on the system, GDB printed misleading error messages instructing the user to run incorrect commands to install the binary files. Subsequently, the suggested commands did not fully work and the program package was not correctly installed. This bug has been fixed, and GDB now issues a message containing correct commands to install the necessary binary files.

In addition, this update adds the following

Enhancement

BZ#971849

This update adds the "$_exitsignal" internal variable to GDB. Now, when debugging a core dump file of a program that was killed by a signal, "$_exitsignal" provides the signal number to the user.

Users of gdb are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.66. GDM

8.66.1. RHBA-2014:1591 — gdm bug fix update

Updated gdm packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The GNOME Display Manager (GDM) provides the graphical login screen, shown shortly after boot up, log out, and when user-switching.

Bug Fixes

BZ#827257

Due to the bugs in the XDMCP remote desktop protocol chooser and indirect query code, deadlocks and incorrect size arguments occurred on GDM. As a consequence, the host chooser failed to properly delegate to other hosts. To fix this bug, correct-size information is now used, and the recursive deadlock has been removed. As a result, the indirect chooser now works more reliably.

BZ#992907

Previously, the logic for determining when to force the X server to run on virtual console 1 was inadequate, which caused the login screen and subsequent user sessions to switch to virtual console 7 after the initial logout. This update introduces a change in the logic to make virtual console 1 use the statically hardwired display. Now, only auxiliary displays needed for user switching run on virtual console 7 and above, and the main login screen with subsequent user sessions always runs on virtual console 1.

BZ#1004484

Prior to this update, the "Switch User" menu item depended on the GDM display manager for starting a login screen. Consequently, the "Switch User" menu item terminated unexpectedly if the user initially logged in with KDM. With this update, the broken "Switch User" menu item is hidden if the user has not logged in with GDM.

BZ#1004909

Due to a missing NULL check in the code, a benign error was logged in the slave log file when logging in via a remote XDMCP connection. The missing NULL check has been added to fix this bug, and error messages are no longer returned.

BZ#1013351

Previously, GDM failed to create xauth entries usable by remote X clients. Consequently, remote clients could not gain access to the host X server without resorting to ssh tunnels. With this update, GDM writes out xauth entries suitable for remote clients when the DisallowTCP option is set to "false" in the configuration. As a result, xauth entries usable by remote clients are now successfully generated.

BZ#1030163

When debugging was enabled and DNS misconfigured, errors in debug logging code made GDM enter an infinite loop. As a consequence, the XDMCP remote desktop protocol did not work or worked sporadically when debug mode was enabled; debug code printed NULL instead of remote server host in failure scenarios. To fix this bug, the debug code has been changed not to call itself and not to nullify or leak the host name. As a result, GDM no longer locks up and returns more comprehensible error messages.

BZ#1048769

Due to incorrect handling of the machine state in user switching code, user switching applet could terminate unexpectedly shortly after login. With this update, the machine state is handled differently, and user switching applet crashes no longer occur.

BZ#1073546

If the window manager attempted to focus a window before user interaction, benign warning messages were logged in the /var/log/gdm/:0-greeter.log file. With this update, window focusing in the early start up is avoided, and the window manager no longer returns warning messages.

Users of gdm are advised to upgrade to these updated packages, which fix these bugs. GDM must be restarted for this update to take effect. Rebooting achieves this, but changing the runlevel from 5 to 3 and back to 5 also restarts GDM.

8.67. GETTEXT

8.67.1. RHBA-2014:0586 — gettext bug fix update

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

The GNU gettext packages provide a set of tools and documentation for producing multi-lingual messages in programs.

Bug Fix

BZ#1024681

Previously, when the xgettext utility encountered an invalid file and generated a warning message it would exit with a fatal error if any additional files were supplied to be processed. Consequently, no output was generated. This update fixes the error-processing code and xgettext now works as expected in the described situation.

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

8.68. GHOSTSCRIPT-FONTS

8.68.1. RHBA-2014:0260 — ghostscript-fonts bug fix update

An updated ghostscript-fonts package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The ghostscript-fonts package contains a set of fonts that Ghostscript, a PostScript interpreter, uses to render text. These fonts are in addition to the fonts shared by Ghostscript and the X Window System.

Bug Fix

BZ#1067294

Previously, the ghostscript-fonts package contained fonts with a restrictive license. With this update, the fonts with restricted rights causing a licensing problem are removed from the package.

Users of ghostscript-fonts are advised to upgrade to this updated package, which fixes this bug.

8.69. GLIB2

8.69.1. RHBA-2014:1538 — glib2 bug fix and enhancement update

Updated glib2 packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

GLib is a low-level core library that forms the basis for projects such as GTK+ and GNOME. It provides data structure handling for C, portability wrappers, and interfaces for such runtime functionality as an event loop, threads, dynamic loading, and an object system.

NOTE

The glib2 packages have been upgraded to upstream version 2.28.8, which provides a number of bug fixes and enhancements over the previous version. (BZ#1101398)

Users of glib2 are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

8.70. GLIBC

8.70.1. RHSA-2014:1391 — Moderate: glibc security, bug fix, and enhancement update

Updated glibc packages that fix two security issues, several bugs, and add two 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 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.

Security Fixes

CVE-2013-4237

An out-of-bounds write flaw was found in the way the glibc's readdir_r() function handled file system entries longer than the NAME_MAX character constant. A remote attacker could provide a specially crafted NTFS or CIFS file system that, when processed by an application using readdir_r(), would cause that application to crash or, potentially, allow the attacker to execute arbitrary code with the privileges of the user running the application.

CVE-2013-4458

It was found that getaddrinfo() did not limit the amount of stack memory used during name resolution. An attacker able to make an application resolve an attacker-controlled hostname or IP address could possibly cause the application to exhaust all stack memory and crash.

Bug Fixes

BZ#845218

When performing an address lookup to a defective Domain Name System (DNS) server using the getaddrinfo utility with the ai_family option set to AF_UNSPEC, the server could respond with a valid response for the A record and a referral response for the AAAA record, which resulted in a lookup failure. With this update, getaddrinfo has been fixed to return the valid response in such a case.

BZ#905941

Under certain rare circumstances, the pthreads utility terminated unexpectedly during stack unwinding on thread cancellation on the PowerPC architecture. The bug has been fixed and pthreads no longer crashes in the described case.

BZ#981942

Name lookup of internationalized domain names using the getaddrinfo utility occasionally caused the calling program to abort unexpectedly. This update fixes the getaddrinfo code to prevent the abort.

BZ#995972

Due to a bug in the thread local storage (TLS) initialization, the dlopen() function occasionally terminated unexpectedly with a segmentation fault. This bug has been fixed, and dlopen() no longer crashes.

BZ#1019916

The order of relocations was incorrect during symbol dependency testing in the dynamic linker. Consequently, IFUNC resolvers terminated unexpectedly if the dependent symbols have not yet been relocated. This occurred when one of the environment variables LD_WARN or LD_TRACE_PRELINKING was set. This update ensures that relocations done during symbol dependency testing are performed in correct order, thus avoiding the crash.

BZ#1027101

This update modifies certain code paths used by the C library's memory allocator "fastbins" feature to be thread-safe, which prevents segmentation faults previously caused by a corruption in the memory allocator.

BZ#1032628

This update fixes the symbol lookup in the elf/dl-lookup.c function to return correct values.

BZ#1039988

Previously, querying for a non-existent netgroup when the nscd daemon was running returned a spurious empty result and no error message. For example, executing 'getent netgroup foo' retured a spurious empty netgroup and exited successfully with status 0 even if no netgroup named 'foo' existed. This bug has been fixed, and the above command now exits with non-zero exit status, as expected.

BZ#1043557

Due to problems with the buffer extension and reallocation, the nscd daemon terminated unexpectedly with a segmentation fault when processing long netgroup entries. With this update, the handling of long netgroup entries has been fixed, and nscd no longer crashes in the described scenario.

BZ#1044628

The getaddrinfo() function returned an incorrect permanent error EAI_NONAME when the Domain Name System (DNS) server was unreachable or the DNS query timed out. Now, getaddrinfo() returns EAI_AGAIN to indicate a temporary failure in name resolution.

BZ#1054846

This update fixes a bug in the nscd daemon that caused the sudo utility to deny access for valid users in permitted netgroups.

BZ#1074342

This update prevents a memory corruption and a subsequent unexpected crash due to a segmentation fault in the nscd daemon when querying certain netgroups with nested members.

BZ#1085273

When querying an empty netgroup, the nscd daemon occasionally became unresponsive. This has been fixed so that an appropriate error code is returned in the described case.

BZ#1099025

This update fixes a bug in the gettimeofday() function's implementation of the Virtual Dynamic Shared Object (VDSO) that caused the gettimeofday() function to return an incorrect non-changing value.

Enhancements

BZ#1027261

This update adds information about the malloc() function requests satisfied by the mmap system call to the output created by the malloc_info() function.

BZ#1028285

This update adds Virtual Dynamic Shared Object (VDSO) indirect function support for the gettimeofday() system call on 64-bit PowerPC system to improve the performance of gettimeofday().

All glibc users are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements.

8.71. GLUSTERFS

8.71.1. RHBA-2014:1576 — glusterfs bug fix and enhancement update

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

Red Hat Storage is software-only, scale-out storage that provides flexible and affordable unstructured data storage for an enterprise. GlusterFS, a key building block of Red Hat Storage, is based on a stackable user-space design and can deliver exceptional performance for diverse workloads. GlusterFS aggregates various storage servers over network interconnections into one large, parallel network file system.

This update also fixes the following bugs:

NOTE

The glusterfs packages have been upgraded to upstream version 3.6.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#1095604)

This update also fixes the following bugs:

Bug Fixes

BZ#1044797

When trying to mount a remote gluster share using the "backupvolfile-server" option, the process failed and returned an "Invalid argument" error message. A new mount point option, backup-volfile-servers, has been added to provide backward compatibility and allows remote gluster shares to be mounted successfully.

BZ#1119205

Previously, when updating the gluster utility from Red Hat Enterprise Linux 6.5 to version 6.6, glusterfs-libs POSTIN scriptlet terminated unexpectedly. The underlying source code has been patched, and POSTIN no longer fails.

The glusterfs packages have been upgraded to upstream version 3.6.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#1095604)

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

8.72. GNOME-PACKAGEKIT

8.72.1. RHBA-2014:1479 — gnome-packagekit bug fix and update

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

The gnome-packagekit packages provide session applications for the PackageKit API.

Bug Fixes

BZ#720922

Previously, if a search query was issued in the gnome-packagekit GUI before the list of packages in the left pane was populated, gnome-packagekit became unresponsive. With this update, gnome-packagekit has been modified so that it does not permit search queries before loading the package list. As a result, gnome-packagekit no longer hangs in the described case.

BZ#732796

Prior to this update, the "Install Updates" button in the gpk-update-viewer GUI was incorrectly re-enabled when the authentication dialog started. This bug has been fixed, and the button remains disabled when the authentication dialog appears.

Users of gnome-packagekit are advised to upgrade to these updated packages, which fix these bugs.

8.73. GNOME-SESSION

8.73.1. RHBA-2014:1585 — gnome-session bug fix and enhancement update

Updated gnome-session packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The gnome-session packages manage the GNOME desktop session. It starts up the other core components of GNOME and handles logout and saving of the session.

Bug Fixes

BZ#684767

Due to insufficient checking, the "Switch User" button appeared in the logout dialog window even when user switching was disabled by the lock down configuration. A patch has been provided to fix this bug, and the "Switch User" button is now removed when the user logs out.

BZ#785828, BZ#1069503

Due to incorrect clean up of resources at shutdown, the "Startup Applications" GUI did not submit changes immediately. If the user closed the dialog window earlier than 2 seconds after making a change, the change failed to be committed. To fix this bug, the dialog window on shutdown has been deleted, so that its dispose handler commits pending changes immediately. As a result, the user can enable or disable additional startup programs and quickly close the dialog window without the risk of losing changes.

BZ#982423

Prior to this update, there were inadequate checks in the gnome-session utility for a preexisting gnome-session instance. Consequently, running gnome-session within a GNOME session started a nested broken session. With this update, a check for the SESSION_MANAGER environment variable has been added. As a result, if the user runs gnome-session within a preexisting session by mistake, an error message is returned.

In addition, this update adds the following

Enhancement

BZ#786573

Previously, if the user accidentally clicked "Remember Running Applications" and was using the custom session selector, they could not proceed without saving. This update provides the close button for the session selector to enable the user to refrain from saving.

Users of gnome-session are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.74. GNUPG2

8.74.1. RHBA-2014:0806 — gnupg2 bug fix update

Updated gnupg2 packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The GNU Privacy Guard (GnuPG or GPG) is a tool for encrypting data and creating digital signatures, compliant with the proposed OpenPGP Internet standard and the S/MIME standard.

Bug Fixes

BZ#638635

Previously, the secret key management daemon for GnuPG, gpg-agent, failed to encode a new iteration count value when it created a new protected key or changed an existing key. As a consequence, the key could not be unprotected and gpg-agent thus did not properly interact with a number of programs that use key decryption, such as KMail or Kleopatra. With this update, the new iteration count is encoded properly and the decryption of keys created or modified by gpg-agent no longer fails.

BZ#966493

Prior to this update, the GnuPG encryption and signing tool, gpg2, by default used CAST5, an encryption algorithm not approved by FIPS standards. Consequently, when gpg2 was run in FIPS mode, data encryption and decryption failed and caused gpg2 to terminate unexpectedly. With this update, GnuPG uses AES, a FIPS-approved encryption algorithm, and gpg2 data encryption and decryption in FIPS mode work as intended.

BZ#1006879

Previously, the GnuPG signature checking tool, gpgv2, did not correctly interact with the Libgcrypt library. As a consequence, when the gpgv command was used on a file, gpgv2 terminated unexpectedly. This update fixes the error and the gpgv command now functions correctly.

BZ#1078957

Prior to this update, GnuPG did not check for availability of the RIPEMD-160 hash function digest. Because the RIPEMD-160 algorithm is not approved by FIPS standards, GnuPG therefore terminated unexpectedly when the "gpg --verify" command was used in FIPS mode to verify a signature that contained a RIPEMD-160 hash. With this update, GnuPG properly checks for RIPEMD-160 support and the crash no longer occurs.

Users of gnupg2 are advised to upgrade to these updated packages, which fix these bugs.

8.75. GPXE

8.75.1. RHBA-2014:1574 — gpxe bug fix update

An updated gpxe package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The gpxe package provides gPXE, an open source Pre-boot Execution Environment (PXE) implementation and boot loader.

Bug Fixes

BZ#1057249

The PXE booting did not respect the specified boot order when multiple NICs of the same type were configured for a virtual machine. Instead, the gPXE image attempted to boot from all NICs supported by the loaded image in the PCI bus scan order. This resulted in boot delays, attempting to perform a PXE boot on unintended devices, as well as in booting from unintended devices in case of success. This update provides the gPXE boot image with the PCI address of the intended boot device, ensuring that the image only attempts to boot on the intended device.

BZ#1105189

HTTP requests generated by gPXE set wrong TCP flag (SYN & PSH) in the first packet of a session. Consequently, when using a firewall, the TCP packet flow would be blocked and the HTTP module integrated with gPXE would not work. With this update, gPXE no longer set the PSH flag in the first packet of a session and the system now boots as expected.

Users of gpxe are advised to upgrade to this updated package, which fixes these bugs.

8.76. GREP

8.76.1. RHBA-2014:0622 — grep bug fix update

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

The grep utility searches through textual input for lines which contain a match to a specified pattern and then prints the matching lines. GNU grep utilities include grep, egrep and fgrep.

Bug Fix

BZ#683753

Previously, the grep utility did not request processing of UTF-8 from the Perl-compatible regular expressions (PCRE) library if a UTF-8 locale was in effect. As a consequence, Unicode symbols were not correctly matched if a Perl regular expression (the "-P" option) was used with a UTF-8 locale. This update adds a request for UTF-8 processing to the PCRE library, and grep now correctly handles Unicode symbols in the described situation.

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

8.77. GRUB

8.77.1. RHBA-2014:1476 — grub bug fix update

Updated grub packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The grub packages provide GRUB (Grand Unified Boot Loader), a boot loader capable of booting a wide variety of operating systems.

Bug Fixes

BZ#1002809

On some systems that are not case sensitive, the "bootx64" command incorrectly launched the GRUB shell instead of booting the GRUB installer. With this update, "bootx64" also checks for the existence of the GRUB booting file (BOOTX64), which allows for using "bootx64" to boot GRUB on systems which are not case sensitive.

BZ#1121321

A regular expression in the grub-install program could not match multipath devices when the "user_friendly_name" option was set to "no". As a consequence, the user was not able to install the GRUB utility on a specified device. To fix this bug, the regular expression has been updated to match the requested device names. As a result, GRUB now installs successfully.

BZ#1129466

Prior to this update, exiting the GRUB shell menu and rebooting the ISO file on an extensible firmware interface (EFI) system changed the boot device path, which in turn caused an assert error. As a consequence, GRUB sometimes failed to boot. This update prevents the boot device path from being changed, and as a result, exiting the GRUB shell and rebooting the ISO file now proceeds as expected.

BZ#1130209

Previously, the biodisk function incorrectly returned "0" instead of the correct values of the read and write calls. Due to this bug, the kernel under some circumstances detected disk errors when booting, which caused the boot to fail. This update fixes the behavior of biodisk, and the boot failure no longer occurs.

BZ#1128137

Previously, booting GRUB with trusted boot (tboot) enabled under some circumstances caused the tboot screen to be blue, making the text output impossible to read. This update adds a number of conditions for graphic initialization to GRUB, which ensure that the tboot screen displays in normal colors.

BZ#1131205

Previously, the graphics_cls() and graphics_init() calls did not correctly co-operate with GRUB. As a consequence, booting an ISO file with disabled VGA caused the system to encounter an exception and automatically reboot. With this update, the behavior of the mentioned calls has been corrected and the system now successfully boots with disabled VGA.

BZ#1094978, BZ#1074914, BZ#1048681

When the "splashimage" option parameter was commented out or a serial console was enabled in the /boot/EFI/redhat/grub.cfg file, the kernel did not initialize the efifb graphic back end when booting an EFI system. As a consequence, VGA text consoles displayed a blank screen instead of the intended output. With this update, booting an EFI system uses efifb regardless of whether GRUB splash image or a serial console are used, and the content of VGA consoles now displays as expected.

BZ#1129436

Prior to this update, if a splash image was not used when booting an EFI system, the serial console displayed a redundant grub_read() failure message during the boot process. With this update, the underlying code has been fixed and booting an EFI system without the GRUB splash image no longer generates redundant failure messages.

Users of grub are advised to upgrade to these updated packages, which fix these bugs.

8.78. GRUBBY

8.78.1. RHBA-2014:1575 — grubby bug fix update

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

grubby is a command line tool for updating and displaying information about the configuration files for the grub, lilo, elilo (ia64), yaboot (powerpc) and zipl (s390) boot loaders. It is primarily designed to be used from scripts which install new kernels and need to find information about the current boot environment.

Bug Fixes

BZ#1098846

Prior to this update, the Trusted Boot (tboot) module incorrectly used the tboot.gz multiboot image to search for a grub configuration file. As a consequence, running the "yum update" command led to grubby corrupting the grub.conf file when tboot was enabled and two or more kernels were updated. With this update, tboot uses specific kernel names to search for grub configuration, and corruption of grub.conf no longer occurs in the described scenario.

BZ#997934

Previously, enabling tboot caused the kernel configuration to not be displayed properly when running the "grubby --info=DEFAULT" command. With this update, multiboot module parameters have been included in the output of "grubby --info", and the configuration displays as expected when tboot is running.

Users of grubby are advised to upgrade to these updated packages, which fix these bugs.

8.79. GTK2

8.79.1. RHBA-2014:1554 — gtk2, gdk-pixbuf2, librsvg2, and libwmf bug fix and enhancement update

Updated gtk2, gdk-pixbuf2, librsvg2, and libwmf packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The gtk2 packages provide a multi-platform toolkit for creating graphical user interfaces, GIMP Toolkit (GTK+). GTK+ offers a complete set of widgets and is suitable for small projects as well as complete application suites.

In addition, this update fixes the following bugs:

NOTE

The gdk-pixbuf2 packages provide an image loading library that can be extended by loadable modules for new image formats. It is used by toolkits such as GTK+ or clutter.

The librsvg2 packages provide an SVG (Scalable Vector Graphics) library based on the libart library.

The libwmf packages provide a library for reading and converting Windows Metafile Format (WMF) vector graphics. The library is used by applications such as GIMP and ImageMagick.

The gtk2 packages have been upgraded to upstream version 2.24.23, which provides a number of bug fixes and enhancements over the previous version. (BZ#1100886)

In addition, this update fixes the following bugs:

Bug Fixes

BZ#909454

The gtk_cups_connection_test_new() function used the default IPP port instead of the real one. Consequently, the GTK print dialog failed to get printer information from remote CUPS servers with a non-standard port number. With this update, the correct port number is used and GTK no longer fails.

BZ#1015044

The rsvg-convert utility of the librsvg2 library did not respect the width and height specified with the viewBox attribute in SVG files. As a consequence, avatar icons were smaller than they were supposed to be. With this update, the utility uses the correct width and height.

BZ#1104681, BZ#1104684

The gdk-pixbuf loaders were moved to a separate directory as part of the separation of the gdk-pixbuf2 library to its own package. This update moves the loaders present in the librsvg2 and libwmf libraries to the new directory.

BZ#1126916

The newly-added GtkComboBoxText widget could cause applications that used it to terminate unexpectedly due to the incorrect initialization of one of the widget's properties. With this update, the initialization has been fixed and the applications no longer crash in the described scenario.

BZ#1127719

Missing forward declarations for various functions caused the compiler to assume an implicit 32-bit integer return type. Consequently, the compiler terminated unexpectedly because the string pointer was truncated to 32-bits and then extended back to 64-bits. With this update, the "#include" lines for the appropriate headers have been added at the top of the affected source files. As a result, the compiler no longer crashes.

BZ#1128798

Previously, the GTK+ print dialog failed to print to a file in the default directory due to an incorrect path generation of the file. The generation of the path has been fixed, and GTK+ prints to a file as intended.

The gdk-pixbuf2 packages provide an image loading library that can be extended by loadable modules for new image formats. It is used by toolkits such as GTK+ or clutter.

The librsvg2 packages provide an SVG (Scalable Vector Graphics) library based on the libart library.

The libwmf packages provide a library for reading and converting Windows Metafile Format (WMF) vector graphics. The library is used by applications such as GIMP and ImageMagick.

The gtk2 packages have been upgraded to upstream version 2.24.23, which provides a number of bug fixes and enhancements over the previous version. (BZ#1100886)

Users of gtk2, gdk-pixbuf2, librsvg2, and libwmf are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

8.80. GVFS

8.80.1. RHBA-2014:1499 — gvfs bug fix update

Updated gvfs packages that fix several 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 through the FTP, SFTP, WebDAV, CIFS, and SMB protocols, among others. GVFS integrates with the GIO (GNOME I/O) abstraction layer.

Bug Fixes

BZ#902448

Previously, when several clients using the same home directory located on remote NFS (Network File System) modified the gvfs-metadata database files, a conflict could occur. In addition, GVFS produced heavy traffic on the remote NFS server. With this update, countermeasures for possible conflicts have been put in place and metadata journal files have been relocated to a temporary directory, and GVFS no longer produces heavy traffic on the NFS mount.

BZ#1011835

Prior to this update, GVFS did not pass a mount prefix into the rename operation. Consequently, it was not possible to rename files on the WebDAV shares if mount prefix was specified, and the following message was displayed when attempting to do so:

The item could not be renamed. Sorry, could not rename "dir1" to "dir2": Thespecified location is not mounted

This bug has been fixed and the mount prefix is now passed into the rename operation as expected. As a result, the rename operation works correctly on the WebDAV shares.

BZ#1049232

When the GDesktopAppInfoLookup extension processed a URL scheme that contained invalid characters, for example from Thunderbird messages, a request for URL handlers was unsuccessful. Consequently, an error dialog notifying about the invalid character was shown. With this update, GDesktopAppInfoLookup has been modified to check the URL scheme for invalid characters before it is used. As a result, the aforementioned error no longer occurs.

BZ#883021

A previous GLib2 rebase

BZ#1118325

Previously, GVFS used the select() function to communicate with the OpenSSH utility. Due to changes introduced with the OpenSSH update, select() could return incomplete results. Consequently, mounting of SFTP locations failed with the following message:

Error mounting location: Error reading from unix: Input/output error

GVFS has been updated to use the poll() function instead of select(), thus fixing this bug.

BZ#1101389

A previous GLib2 rebase

caused a namespace conflict between GVFS and GIO. As a consequence, GVFS failed to build. To fix this bug, affected modules have been renamed, and the building process of GVFS now succeeds. (BZ#1071374)

marked the GDesktopAppInfo class as deprecated. Consequently, GVFS failed to compile. With this update, GdesktopAppInfo is not regarded as deprecated in this specific scenario. As a result, GVFS compiles as expected. (BZ#1118704)

Users of gvfs are advised to upgrade to these updated packages, which fix these bugs.

8.81. GZIP

8.81.1. RHBA-2014:0297 — gzip bug fix update

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

The gzip packages provide the GNU gzip data compression program.

Bug Fixes

BZ#949820

Previously, the "-h" option of the zgrep command was absent from the source code of the gzip utility. As a consequence, the output of running the "zgrep -h" command was not parsed, and the file name was printed. With this update, the possibility to use the short "-h" option besides the "--no-filename" option has been added. As a result, running the zgrep command with the "-h" option now prints the correct lines and suppresses the prefixing of the file names on output when multiple files are searched.

BZ#961810

Prior to this update, the time stamp of an archive was set by the futimesat() or utime() system calls when using the gzip utility. Consequently, the archived file had a lower time stamp than expected because only microsecond resolution was enabled, and a nanosecond time stamp was not provided. The underlying source code has been modified to attempt to use the utimensat() or futimens() system calls for nanosecond resolution. As a result, the archived file has exactly the same time stamp as the original file.

Users of gzip are advised to upgrade to these updated packages, which fix these bugs.

8.82. HAL

8.82.1. RHBA-2014:1460 — hal bug fix and enhancement update

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

The hal packages provide the Hardware Abstraction Layer (HAL) daemon. HAL collects and maintains information about the hardware on the system from several sources, and provides a live device list through D-BUS.

Bug Fixes

BZ#736415

Prior to this update, the HAL daemon did not properly handle the hot plug addition and removal events. Consequently, the HAL daemon terminated unexpectedly with a segmentation fault during device probing. With this update, hot plug events are properly handled and the HAL daemon no

longer crashes in the aforementioned scenario.

BZ#755209

Prior to this update, the /usr/libexec/hald-probe-smbios script, as well as certain other hald-probe scripts, terminated unexpectedly after they were manually started. This bug has been fixed and the aforementioned scripts can be started manually without complications.

In addition, this update adds the following

Enhancement

BZ#1076664

Previously, the HAL daemon did not recognize touchscreen monitors correctly. Consequently, these monitors were not added to the list of hot plugged devices in the Xorg window system. Support for touchscreen devices has been added to HAL and these devices are now recognized correctly.

Users of hal are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.83. HAPROXY

8.83.1. RHBA-2014:1509 — haproxy bug fix and enhancement update

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

The haproxy packages provide a reliable, high-performance network load balancer for TCP and HTTP-based applications.

NOTE

The haproxy package has been upgraded to upstream version 1.5.2, which provides a number of bug fixes and enhancements over the previous version, including support for SSL termination. (BZ#1081727)

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

8.84. HMACCALC

8.84.1. RHBA-2014:1584 — hmaccalc bug fix update

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

The hmaccalc packages contain tools to calculate HMAC (Hash-based Message Authentication Code) values for files. The names and interfaces were designed to mimic those of the sha1sum, sha256sum, sha384sum and sha512sum tools provided by the coreutils package.

Bug Fix

BZ#1016706

The .hmac files are used to check the kernel image at the boot time; if the check fails, the boot process is expected to be halted. Previously, the hmaccalc utility did not flag empty .hmac files as an error, allowing the system to boot even if the boot was supposed to fail. With this update, a patch has been provided to address this bug. As a result, the system is no longer allowed to boot in the described scenario.

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

8.85. HPLIP

8.85.1. RHBA-2014:0767 — hplip bug fix update

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

The hplip packages contain the Hewlett-Packard Linux Imaging and Printing Project (HPLIP), which provides drivers for Hewlett-Packard printers and multi-function peripherals.

Bug Fix

BZ#905143

Previously, the udev rules files were not in the correct location on the file system. As a consequence, permissions on the device node after connecting a device were insufficient. This update moves the udev rules files to the correct location, and udev rules now work correctly in the described situation.

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

8.86. HTTPD

8.86.1. RHBA-2014:1386 — httpd bug fix and enhancement update

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

The httpd packages provide the Apache HTTP Server, the most widely-used web server.

Bug Fixes

BZ#876626

Previously, the system did not initialize shared memory session cache when the Apache HTTP Server loaded the mod_ssl module for the first time during a configuration reload. As a consequence, the system terminated the httpd service unexpectedly in the described situation. With this update, the problem has been fixed, and httpd no longer crashes when loaded for the first time after a configuration reload.

BZ#972949

Previously, the bybusyness algorithm, contained in the mod_proxy_balancer module, did not balance the workload after a worker tried to send a request to a non-working node. Consequently, once the non-working node became working again, mod_proxy_balancer did not recover the worker that tried

to send the request because it still considered the worker busy. With this update, the algorithm has been fixed and mod_proxy_balancer now uses the worker after a node recovery as expected.

BZ#976644

Prior to this update, the mod_proxy module did not ignore the EINTR return value of the poll() function. As a consequence, mod_proxy broke the connection during an attempt to send a request using the CONNECT method when the child process was terminated. A patch has been applied to fix this problem, and mod_proxy now ignores EINTR and continues with the CONNECT request as expected in the described situation.

BZ#979129

Previously, the mod_cgi module did not correctly handle the situation when a client failed to send a request before timeout. Consequently, the client received the "500 Internal Server Error" HTTP status code instead of the "408 Request Timeout" HTTP status code. With this update, the problem has been fixed, and the client now receives "408 Request Timeout" after a failed attempt to send a request before timeout.

BZ#991556

Previously, the Apache Portable Runtime (APR) library bucket brigade in the mod_proxy_http module contained objects allocated from another APR pool that could be freed before the APR bucket brigade. Consequently, trying to free already freed objects in an APR bucket brigade cleanup could cause the httpd service to terminate unexpectedly. With this update, the APR bucket brigade in mod_proxy_http is now destroyed sooner than the APR pool from which the objects stored in the APR bucket brigade are allocated. As a result, httpd no longer crashes in mod_proxy_http during an APR bucket brigade cleanup.

BZ#1012766

Prior to this update, the mod_proxy_http module did not honor the ErrorLog directive defined in VirtualHost configuration for certain errors. As a consequence, the "proxy: error reading response" message could be logged into the global error log even though a VirtualHost-specific error log was configured. A patch has been applied to fix this bug, and mod_proxy_http now logs "proxy: error reading response" into the correct log file.

BZ#1032733

Prior to this update, the status line of an HTTP response message from server did not, under certain circumstances, include the HTTP reason phrase if it contained the status code. As a consequence, the server displayed only the status code to the HTTP client. With this update, the bug has been fixed, and the status line issued to the HTTP client now contains both the status code and the reason phrase as expected.

BZ#1034984

Previously, the mod_ssl module directives did not contain support for using the Transport Layer Security cryptographic protocol version 1.2 (TLSv1.2). As a consequence, the user could not set up mod_ssl to disable TLSv1.2. With this update, support for TLSv1.2 configuration options has been added to mod_ssl. As a result, it is now possible to set up mod_ssl to disable TLSv1.2.

BZ#1035666

Prior to this update, the mod_ssl module did not support wildcard certificates with the SSLProxy directive. As a consequence, SSLProxy did not work when a wildcard certificate was used, and the user had to set the SSLProxyCheckPeerCN directive to "off" as a workaround. A patch has been applied to fix this bug, and mod_ssl now supports wildcard certificates with SSLProxy.

BZ#1037832

Previously, the mod_ssl module stored all Certificate Revocation Lists (CRL) in cache, and the user could not disable the caching. Consequently, the httpd service could consume a lot of memory when a large amount of CRLs were stored in cache. To fix this problem, the DisableCRLCaching directive has been added to mod_ssl to disable CRL caching. As a result, mod_ssl can now be configured to no longer store CRLs in cache.

BZ#1048757

Previously, a function handling dynamic groups, which is included in the mod_ldap module, contained an incorrect pointer assignment. As a consequence, the system caused the httpd service to terminate unexpectedly with a segmentation fault when multiple dynamic groups were used. A patch has been applied to fix this bug, and httpd no longer crashes when more than one dynamic group is used.

BZ#1071883, 1100680

Prior to this update, the mod_ssl module only supported ephemeral Diffie-Hellman (DH) keys of 512-bit and 1024-bit lengths. Consequently, Secure Sockets Layer (SSL) cipher suites using ephemeral DH keys could not be used in FIPS mode. With this update, mod_ssl uses ephemeral DH keys of key lengths up to 8192 bits. As a result, mod_ssl now works as expected in FIPS mode.

BZ#1077336

Previously, when running the "apachectl status" command, the exit code failed to be changed when the httpd service was not running. As a consequence, "apachectl status" could return the exit code 0, indicating success, even when httpd was not running. A patch has been provided to fix this bug and "apachectl status" now exits with the correct exit code when httpd is not running.

BZ#1090445

Prior to this update, the SSLProtocol directive exposed by the mod_ssl module did not allow control over whether the TLSv1.1 or TLSv1.2 protocols were enabled. Consequently, the user could not set mod_ssl to disable TLSv1.1 or TLSV1.2. With this update, support for TLSv1.2 and TLSv1.2 configuration options has been added to mod_ssl, and mod_ssl now supports TLSv1.1 and TLSv1.2 in the SSLProtocol Directive.

BZ#1094990

Previously, the mod_cache module did not correctly handle requests to the back-end server due to a race condition between removing and renaming cached files and due to inconsistencies in generating the cache hash codes when handling the HTTP Range requests. Consequently, mod_cache could pass multiple requests to the back-end server to refresh the cache instead of a single request. With this update, the race condition has been fixed and hash codes for an object in cache are generated consistently even when handling Range requests. As a result, mod_cache now passes only a single request to the back-end server when refreshing the cache.

BZ#1103115

Prior to this update, the %post script of the mod_ssl module used an RSA key hard-coded to a 1024-bit length. As a consequence, the user could not install mod_ssl in FIPS mode. To fix this bug, the mod_ssl %post script has been updated to use 2048-bit RSA key. As a result, it is now possible to install mod_ssl in FIPS mode.

BZ#1111410

Previously, the mod_proxy module did not close the client connection when the back-end server connection was closed. Consequently, mod_proxy kept the client connection open until it timed out. A

patch has been provided to fix this bug and mod_proxy now closes the client connection immediately after mod_proxy closes connection to the back-end server.

Enhancements

BZ#1035818

This update introduces support for Elliptic Curve Cryptography (ECC) keys and Elliptic Curve Diffie-Hellman (ECDH) ciphers in Red Hat Enterprise Linux 6 because the OpenSSL toolkit in Red Hat Enterprise Linux 6 also supports ECDH.

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

8.87. HWDATA

8.87.1. RHEA-2014:1553 — hwdata enhancement update

An updated hwdata package that adds one enhancement is now available for Red Hat Enterprise Linux 6.

The hwdata package contains tools for accessing and displaying hardware identification and configuration data.

Enhancement

BZ#1064381

The PCI, USB, and vendor ID files have been updated with information about recently released hardware. Hardware utility tools that use these ID files are now able to correctly identify recently released hardware.

Users of hwdata are advised to upgrade to this updated package, which adds this enhancement.

8.88. I2C-TOOLS

8.88.1. RHBA-2014:1520 — i2c-tools bug fix update

Updated i2c-tools packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The i2c-tools packages contain a set of I2C tools for Linux: a bus probing tool, a chip dumper, register-level SMBus access helpers, EEPROM (Electrically Erasable Programmable Read-Only Memory) decoding scripts, EEPROM programming tools, and a python module for SMBus access.

Note: EEPROM decoding scripts can render your system unusable. Make sure to use these tools wisely.

This update fixes the following bug:

Bug Fix

BZ#914728

The i2cdetect utility requires the i2c-dev module to be loaded so that it can detect devices present on

a specified bus. Previously, this was not done automatically, and as a consequence, the user could be mistaken that no buses or devices existed when running i2cdetect. With this update, i2c-dev has been made automatically-loadable. Now, i2cdetect correctly scans an I2C bus for devices and outputs a table with detected devices as expected.

Note: EEPROM decoding scripts can render your system unusable. Make sure to use these tools wisely.

Users of i2c-tools are advised to upgrade to these updated packages, which fix this bug.

8.89. IBUS-TABLE

8.89.1. RHBA-2014:0572 — ibus-table bug fix update

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

The ibus-table packages contain a table engine for Intelligent Input Bus (IBus), which is an input method (IM) framework for multilingual input in Unix-like operating systems.

Bug Fix

BZ#983497

Previously, indexing for the compose.db and latex.db files was handled by the post-installation script. As a consequence, running the "rpm -V" command returned an unnecessary warning that the SQLite database files had been changed since the installation. With this update, the indexed files are already included in the packages, and no warning messages are displayed in the described situation.

Users of ibus-table are advised to upgrade to these updated packages, which fix this bug.

8.90. ICEDTEA-WEB

8.90.1. RHBA-2014:1417 — icedtea-web bug fix and enhancement update

Updated icedtea-web packages that fix several bugs and add various enhancements 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.

NOTE

The icedtea-web packages have been upgraded to upstream version 1.5.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#1075790)

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

8.91. INITSCRIPTS

8.91.1. RHBA-2014:1448 — initscripts bug fix and enhancement update

Updated initscripts packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The initscripts packages contain basic system scripts to boot the system, change runlevels, activate and deactivate most network interfaces, and shut down the system cleanly.

Bug Fixes

BZ#1018095

Previously, certain network device drivers did not accept ethtool commands right after they appeared in the user-space. As a consequence, the current setting of the specified device driver was not applied and an error message was returned. This update adds the ETHTOOL_DELAY variable, which makes sure the ethtool utility waits for some time before it tries to apply the options settings, thus fixing the bug.

BZ#1024561

When issuing a reboot or halt, the system sometimes killed the S01reboot process and never completed the reboot or shutdown. This update changes the regex for the sed utility to fix this bug, and the S01reboot process now completes successfully.

BZ#1053098

Previously, the ipcalc utility handled netmask parameters incorrectly using the "-c" option. As a consequence, invalid CIDR was ignored and netmask in allowed format was not accepted. The updated "-c" option validates IP addresses for specified address families as expected, invalid CIDR is no longer ignored, and allowed formats of netmask are accepted.

BZ#1086897

Due to a race condition, the "multicast_router" and "hash_max" BRIDGING_OPTS options failed to apply when creating the bridge. With this update, "multicast_router" and "hash_max" are applied after the bridge is up, and BRIDGING_OPTS options now work as intended.

BZ#1101795

Prior to this update, the udev device manager called the hotplug script when a VLAN network was added. However, because the VLAN network has the same default hardware address as the default network adapter device, hotplug reverted the network adapter's IP configuration to the values in the /etc/sysconfig/network-scripts/ directory, and in some cases disconnected the network adapter. This update removes the triggering of the hotplug script for VLAN networks and, as a result, the network adapter now retains its IP address, and thus no longer fails.

In addition, this update adds the following

Enhancements

BZ#1005355

Previously, the only way to set up VLAN ID was through the name of the new virtual device (vlan10 or eth0.10). With this update, the ID can be specified by the VID option in ifcfg file.

BZ#1023471

The saved seed size in the /etc/rc.sysinit file has been increased from 512 bytes to 4096 bytes to comply with the updated crypto requirements.

BZ#1082765, BZ#1099486

With this update, the user can set PRIO and AGEING options for bridges in ifcfg files, which allow ageing to be set in ifcfg-* scripts.

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

8.92. IPA

8.92.1. RHBA-2014:1383 — ipa bug fix and enhancement update

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

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.

Bug Fixes

BZ#1034478

Previously, the ipa-replica-install script tried to add the "A" and "PTR" records if the master managed Domain Name System (DNS). If the master did not manage the replica's zone, an error message "DNS zone not found" was returned, and the installation of a replica failed. With this update, the ipa-replica-install script has been fixed to properly handle the described situation, and the replica's installation now succeeds. Please note that the "A" and "PTR" records for the replica need to be added manually.

BZ#1083878

Previously, when Identity Management Public Key Infrastructure (PKI) clone in Red Hat Enterprise Linux 7 was being installed, an access to the /ca/ee/ca/profileSubmit URI on the Identity Management server, from which it was replicating, was required. However, Identity Management in Red Hat Enterprise Linux 6 did not export this URI in the httpd proxy configuration. As a consequence, the installation of Identity Management replica with the PKI component in Red Hat Enterprise Linux 7 failed when installed against a Red Hat Enterprise Linux 6 master. With this update, the /ca/ee/ca/profileSubmit URI has been added to Red Hat Enterprise Linux 6 Identity Management proxy configuration and a replica installation now succeeds in this scenario.

BZ#1022199

Prior to this update, disabling a sudo rule did not trigger the removal of its entry from the sudo compat tree in Lightweight Directory Access Protocol (LDAP). Consequently, the disabled sudo rules were still followed on clients using the sudo compat tree. This bug has been fixed, and the described problem no longer occurs.

BZ#1029921

Previously, an Identity Management password policy was not applied to passwords changed using the Directory Manager or PassSync agent. As a consequence, the default expiration time (90 days) was always applied even if the Identity Management administrator had defined a different policy. The Identity Management Password Change Extended Operation Plug-in has been updated, and the password changes made by the Directory Manager or PassSync agent now respect the "max lifetime" field of the user password policy.

BZ#905064

Previously, an intermittent race condition happened when the ipa-server-install utility tried to read the "preop.pin" value from the CS.cfg file, which was still unwritten to the disk by the pkicreate utility. As a consequence, the Identity Management server installation failed. With this update, ipa-server-install has been modified to anticipate such a race condition. Now, when ipa-server-install is unable to read from CS.cfg, it waits until it times out or the file is written to the disk. Additionally, these events are now properly logged in the installation log if they occur.

BZ#1040009

Prior to this update, a bug in the Python readline module caused a stray escape sequence to be prepended to the output of the script that the certmonger utility uses to acquire renewed certificates on the Certification Authority (CA) clones. Consequently, certmonger failed to parse the output of the script and the certificate was not renewed. A patch has been provided to address this bug and certmonger is now able to successfully parse the output of the script and complete the certificate renewal.

BZ#1082590

The ipa-client-automount utility uses the Remote Procedure Call (RPC) interface to validate the automount location. Previously, the RPC interface only allowed clients whose API version was earlier than or the same as the server API version to validate the automount location. As a consequence, running ipa-client-automount with a client whose API version was later than the server's failed with an incompatibility error message. With this update, ipa-client-automount has been modified to report a fixed API version in the RPC call and ipa-client-automount now runs successfully when the client API version is later than the server's.

BZ#1016042

Previously, the ipa-replica-manage utility contained a bug in the re-initialize command causing the MemberOf task to fail with an error message under certain circumstances. Consequently, when the ipa-replica-manage re-initialize command was run for a Windows Synchronization (WinSync) replication agreement, it succeeded in the re-initialization part, but failed during execution of the MemberOf task which was run after the re-initialization part. The following error message was returned:

```
Update succeeded
Can't contact LDAP server
```

However, the error was harmless as running the MemberOf task was not required in this case. A patch has been applied and the error message is no longer returned in the described scenario.

BZ#1088772

Users in Identity Management in Red Hat Enterprise Linux 7 can be added without the password policy explicitly defined in the "krbPwdPolicyReference" attribute in the user object. The User Lockout plug-in locks out users authenticating or binding through the LDAP interface after configured number of failed attempts. In Identity Management in Red Hat Enterprise Linux 7, the plug-in does not require this attribute to be present to correctly apply the lock-out policy. Previously, the Identity Management User Lockout plug-in in Red Hat Enterprise Linux 6 required this attribute to function properly.

Consequently, the password lock-out policy was not applied to users created in Identity Management in Red Hat Enterprise Linux 7 that were replicated to Red Hat Enterprise Linux 6. Such users had an unlimited number of authentication attempts in the LDAP interface. The User Lockout plug-in has been updated to respect users without the defined custom policy and to properly fall back to the defined global password policy, and now only a defined number of authentication attempts are allowed to users in the LDAP interface.

BZ#1095250

Previously, the validator in Identity Management did not allow slash characters in the DNS names. As a consequence, it was not possible to add reverse zones in the classless form. With this update, the DNS name validators allow slash characters where necessary, and thus the recommendations of RFC 2317 are now followed.

BZ#1108661

Prior to this update, Identity Management installers could call the ldapmodify utility without explicitly specifying the authentication method. Consequently, the installer could fail when the authentication method was set in the ldapmodify user configuration. This bug has been fixed, the installer now always calls ldapmodify with the authentication method explicitly specified, and the described problem no longer occurs.

BZ#1109050

Previously, when a Red Hat Enterprise Linux 6 master was being installed or upgraded, an extra default value was added to the "nsDS5ReplicaId" attribute of the LDAP entry "cn=replication,cn=etc". In Red Hat Enterprise Linux 7, Identity Management uses a stricter validation, which prevents installing a replica on such a system. As a consequence, after a Red Hat Enterprise Linux 6 master was installed or upgraded on a system with more than one master, installing a Red Hat Enterprise Linux 7 replica failed. This bug has been fixed, the extra value is no longer added, and Red Hat Enterprise Linux 7 replicas can be installed successfully in this scenario.

BZ#1015481

Identity Management administration framework API contains two checks on the server side to verify that a request on its API can be passed further:

1. A check to see if the client API version is not higher than the server API version. If it is, the request is rejected.

2. A check to see if the client API request does not use an attribute or a parameter unknown to the server. If it does, the request is rejected.

Prior to this update, the Identity Management server performed the checks in an incorrect order. First, the attribute and parameter check was done, then the API version check. As a consequence, when a client (for example, Red Hat Enterprise Linux 6.5) ran the ipa administration utility against a server with an earlier operating system (for instance, Red Hat Enterprise Linux 6.4), the command returned a confusing error message. For example, instead of stating API incompatibility, an error message regarding an unknown option was displayed. This bug has been fixed, the checks on the server are now performed in the correct order and a correct error message is displayed in this scenario.

Enhancements

BZ#1111121

Automated configuration of the sudo command has been added to the ipa-client-install utility. By default, ipa-client-install now configures sudo on Identity Management clients by leveraging the newly-added ipa provider in the sssd utility.

BZ#1095333

A set of Apache modules has been added to Red Hat Enterprise Linux 6.6 as a Technology Preview. The Apache modules can be used by external applications to achieve tighter interaction with Identity Management beyond simple authentication.

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

8.93. IPMITOOL

8.93.1. RHBA-2014:1624 — ipmitool bug fix update

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

The ipmitool packages contain a command line utility for interfacing with devices that support the Intelligent Platform Management Interface (IPMI) specification. IPMI is an open standard for machine health, inventory, and remote power control.

Bug Fix

BZ#1147593

Previously, the ipmitool default timeout values signified a time period which was too short. As a consequence, during retries, the ipmitool utility could terminate unexpectedly with a segmentation fault, or could produce a nonsensical error message. With this update, the ipmitool options passed from environment variable are parsed correctly from IPMITOOL_OPTS and IPMI_OPTS variables, IPMITOOL_* taking precedence over IPMI_* variables. As a result, ipmitool no longer crashes in the described situation.

Users of ipmitool are advised to upgrade to these updated packages, which fix this bug. After installing this update, the IPMI event daemon (ipmievd) will be restarted automatically.

8.93.2. RHBA-2014:1567 — ipmitool bug fix and enhancement update

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

The ipmitool packages contain a command line utility for interfacing with devices that support the Intelligent Platform Management Interface (IPMI) specification. IPMI is an open standard for machine health, inventory, and remote power control.

This update also fixes the following bug:

NOTE

The ipmitool utility has been upgraded to upstream version 1.8.14, which provides a number of bug fixes and enhancements over the previous version. (BZ#825194)

This update also fixes the following bug:

Bug Fix

BZ#1029529

The IPMI kernel code was missing aliases for the IPMI kernel modules. Consequently, not all of the IPMI kernel modules could be automatically loaded when the appropriate hardware was detected, and the hardware thus could not be used. To fix this problem, the module alias configuration file has been added to the /etc/modprobe.d/ directory, linking all of the separate IPMI modules to the IPI* device class alias. Note that the system must be rebooted for this change to take effect.

The ipmitool utility has been upgraded to upstream version 1.8.14, which provides a number of bug fixes and enhancements over the previous version. (BZ#825194)

In addition, this update adds the following

Enhancement

BZ#1056581

To improve usage of ipmitool as a part of the software stack, certain environment variables were unified and several new variables were introduced to ipmitool, specifically:

IPMITOOL_* variables now take precedence over IPMI_* variables.

The IPMITOOL_KGKEY variable has been added to unify the name space usage.

* Limited IPv6 support has been added to the ipmitool packages; the IPMI standard does not include the IPv6 data definitions, and therefore this change includes only IPv6 connectivity. The OEM-vendor-specific command values related to IPv6 are beyond the scope of this feature.

Users of ipmitool are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. After installing this update, the IPMI event daemon (ipmievd) will be restarted automatically.

8.94. IPRUTILS

8.94.1. RHBA-2014:1432 — iprutils bug fix and enhancement update

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

The iprutils packages provide utilities to manage and configure SCSI devices that are supported by the ipr SCSI storage device driver.

This update also fixes the following bug:

NOTE

The iprutils package has been upgraded to upstream version 2.4.2, which provides a number of bug fixes and enhancements over the previous version. Specifically, this update provides support for the new vRAID Serial Attached SCSI (SAS) adapters. (BZ#929292)

This update also fixes the following bug:

Bug Fix

BZ#1127825

Previously, information on "Read Intensive" disks did not display in the iprconfig menu. The underlying source code has been patched, and the disks information is now displayed correctly.

The iprutils package has been upgraded to upstream version 2.4.2, which provides a number of bug fixes and enhancements over the previous version. Specifically, this update provides support for the new vRAID Serial Attached SCSI (SAS) adapters. (BZ#929292)

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

8.95. IPSET

8.95.1. RHBA-2014:1543 — ipset bug fix update

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

The ipset packages provide IP sets, a framework inside the Linux 2.4.x and 2.6.x kernel, which can be administered by the ipset utility. Depending on the type, an IP set can currently store IP addresses, TCP/UDP port numbers or IP addresses with MAC addresses in a way that ensures high speed when matching an entry against a set.

Bug Fix

BZ#888571

Prior to this update, ipset initiation script which would load the ipset rules was missing. Consequently, security problems at system initiation could occur. This update provides all the files necessary to add an ipset systemd service, which starts up before iptables and stops afterwards. As a result, ipset rules can be started, stopped, and saved as intended.

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

8.96. IPTABLES

8.96.1. RHBA-2014:1547 — iptables bug fix and enhancement update

Updated iptables packages that fix two bugs and add one enhancement 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#1059214

Previously, when alternative packages were removed manually, it was impossible to uninstall the iptables-ipv6 packages. The underlying source code has been patched, and iptables-ipv6 can now be uninstalled regardless of manually modified alternatives.

BZ#1070123

When upgrading the Red Hat Enterprise Linux 6.5 minimal installation to version 7.0 using the redhat-upgrade-tool utility, the "%postun" scriptlet of iptables-ipv6 failed. Blocks preventing the old package from uninstalling have been removed, and iptables-ipv6 can now be uninstalled successfully.

In addition, this update adds the following

Enhancement

BZ#1033270

With this update, IPv6 support has been added to the ipset utility, and thus the user can now manage IPSets of IPv6 addresses.

Users of iptables are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.97. IPVSADM

8.97.1. RHBA-2014:1511 — ipvsadm bug fix update

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

The ipvsadm packages provide the ipsvadm tool to administer the IP Virtual Server services offered by the Linux kernel.

Bug Fix

BZ#1099687

Previously, the ipvsadm tool did not handle printing of existing sync daemons correctly under certain circumstances. Consequently, the "ipvsadm --list --daemon" command did not report the existence of a backup sync daemon when only a backup sync daemon was running on a node. A patch has been applied to address this bug, and "ipvsadm --list --daemon" now correctly shows the backup sync daemon even if it is the only daemon running.

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

8.98. IRQBALANCE

8.98.1. RHBA-2014:1504 — irqbalance bug fix update

Updated irqbalance packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The irqbalance packages provide a daemon that evenly distributes the interrupt request (IRQ) load across multiple CPUs for enhanced performance.

Bug Fixes

BZ#1039178

Previously, the irqbalance daemon did not consider the NUMA node assignment for an interrupt

request (IRQ) for the banned CPU set. Consequently, irqbalance set the affinity incorrectly when the IRQBALANCE_BANNED_IRQS variable was set to a single CPU. In addition, IRQs could be assigned to a node that had no eligible CPUs. Node assignment has been restricted to nodes that have eligible CPUs as defined by the unbanned_cpus bitmask, thus fixing the bug. As a result, irqbalance now sets the affinity properly, and IRQs are assigned to the respective nodes correctly.

BZ#987801

Prior to this update, the dependency of the irqbalance daemon was set incorrectly referring to a wrong kernel version. As a consequence, irqbalance could not balance IRQs on NUMA systems. With this update, the dependency has been fixed, and IRQs are now balanced correctly on NUMA systems. Note that users of irqbalance packages have to update the kernel to 2.6.32-358.2.1 or later in order to use the irqbalance daemon in the correct manner.

BZ#1079109

Prior to this update, irqbalance could not accurately determine the NUMA node it was local to or the device to which an IRQ was sent. The kernel affinity_hint values were created to work around this issue. With this update, irqbalance is now capable of parsing all information about an IRQ provided by the sysfs() function. IRQ balancing now works correctly, and the affinity_hint values are now ignored by default not to distort the irqbalance functionality.

Users of irqbalance are advised to upgrade to these updated packages, which fix these bugs.

8.99. ISCSI-INITIATOR-UTILS

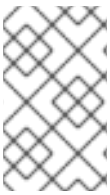
8.99.1. RHBA-2014:1580 — iscsi-initiator-utils bug fix and enhancement update

Updated iscsi-initiator-utils packages that fix several 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.

The QLogic ala4xxx drivers have been updated to the latest upstream version, which provides a number of bug fixes and enhancements over the previous version. (BZ#1053374, BZ#1140326)

This update also fixes the following bugs:



NOTE

The iSCSI UserSpace I/O driver (iscsiuio) has been updated to upstream version 0.7.8.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#1054587)

The QLogic ala4xxx drivers have been updated to the latest upstream version, which provides a number of bug fixes and enhancements over the previous version. (BZ#1053374, BZ#1140326)

This update also fixes the following bugs:

Bug Fixes

BZ#0009299, BZ#1052361

Due to changes in the addressing of inter-process communication (IPC) sockets, updating the isciadm administration utility caused it to be incompatible with the already-running iscsid processes. As a consequence, iscsiadm could no longer communicate with the running iscsid processes after the update. This update adds a retroactive compatibility IPC mode, which automatically triggers when a new IPC socket fails to connect. As a result, iscsiadm can now correctly be used to control pre-existing iscsid processes after an update.

BZ#1132490

Prior to this update, the uip_reset() function was in some cases called with an invalid ustack address. As a consequence, the iscsiuio process was terminated unexpectedly with a segmentation fault. With this update, the ustack address calling uip_reset() has been fixed and the described crash no longer occurs.

BZ#1076344

Prior to this update, the iscsid daemon could not handle more than 31 iSCSI asynchronous events. Consequently, when performing an iSCSI operation with 32 or more target protocol data units, iscsid entered an infinite loop and became unresponsive. With this update, iscsid can properly handle more than 31 iSCSI asynchronous events, and the described hang no longer occurs.

The iSCSI UserSpace I/O driver (iscsiuio) has been updated to upstream version 0.7.8.2, which provides a number of bug fixes and enhancements over the previous version. (BZ#1054587)

The QLogic ala4xxx drivers have been updated to the latest upstream version, which provides a number of bug fixes and enhancements over the previous version. (BZ#1053374, BZ#1140326)

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

8.100. JAVA-1.6.0-OPENJDK

8.100.1. RHBA-2014:1527 — java-1.6.0-openjdk bug fix and enhancement update

Updated java-1.6.0-openjdk packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The java-1.6.0-openjdk packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Java Software Development Kit.

Bug Fixes

BZ#1112806

A bug previously caused the LineBreakMeasurer class to produce the ArrayIndexOutOfBoundsException error when Java attempted to display certain characters in certain fonts. This update fixes the bug and Java now displays the affected characters correctly.

BZ#1098399

Prior to this update, an application accessing an unsynchronized HashMap could potentially enter an infinite loop and consume an excessive amount of CPU resources. As a consequence, the OpenJDK server became unresponsive. This update prevents unsynchronized HashMap access from causing an infinite loop and as a result, the OpenJDK server no longer hangs in the described scenario.

In addition, this update adds the following

Enhancement

BZ#1059925

Shared Java libraries have been modified to allow users to run Java with the cap_net_bind_service, cap_net_admin, and cap_net_raw capabilities granted.

Users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which fix these bugs. All running instances of OpenJDK Java must be restarted for the update to take effect.

8.101. JAVA-1.7.0-OPENJDK

8.101.1. RHSA-2014:1620 — Important: java-1.7.0-openjdk security and bug fix update

Updated java-1.7.0-openjdk packages that fix multiple security issues and one bug are now available for Red Hat Enterprise Linux 6 and 7.

Red Hat Product Security 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-1.7.0-openjdk packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Java Software Development Kit.

Security Fixes

CVE-2014-6506, **CVE-2014-6531**, **CVE-2014-6502**, **CVE-2014-6511**, **CVE-2014-6504**, **CVE-2014-6519**

Multiple flaws were discovered in the Libraries, 2D, and Hotspot components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass certain Java sandbox restrictions.

CVE-2014-6517

It was discovered that the StAX XML parser in the JAXP component in OpenJDK performed expansion of external parameter entities even when external entity substitution was disabled. A remote attacker could use this flaw to perform XML eXternal Entity (XXE) attack against applications using the StAX parser to parse untrusted XML documents.

CVE-2014-6512

It was discovered that the DatagramSocket implementation in OpenJDK failed to perform source address checks for packets received on a connected socket. A remote attacker could use this flaw to have their packets processed as if they were received from the expected source.

CVE-2014-6457

It was discovered that the TLS/SSL implementation in the JSSE component in OpenJDK failed to properly verify the server identity during the renegotiation following session resumption, making it possible for malicious TLS/SSL servers to perform a Triple Handshake attack against clients using JSSE and client certificate authentication.

CVE-2014-6558

It was discovered that the CipherInputStream class implementation in OpenJDK did not properly handle certain exceptions. This could possibly allow an attacker to affect the integrity of an encrypted stream handled by this class.

The CVE-2014-6512 was discovered by Florian Weimer of Red Hat Product Security.

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.

Bug Fix

BZ#1148309

The TLS/SSL implementation in OpenJDK previously failed to handle Diffie-Hellman (DH) keys with more than 1024 bits. This caused client applications using JSSE to fail to establish TLS/SSL connections to servers using larger DH keys during the connection handshake. This update adds support for DH keys with size up to 2048 bits.

The CVE-2014-6512 was discovered by Florian Weimer of Red Hat Product Security.

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.

8.102. KDESDK

8.102.1. RHBA-2014:0485 — kdesdk bug fix update

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

The kdesdk packages contain the KDE Software Development Kit (SDK) which is a collection of applications and tools used by developers. These applications and tools include - cervisia: a CVS frontend; kate: an advanced text editor; kbugbuster: a tool to manage the KDE bug report system; kcachegrind: a browser for data produced by profiling tools (for example cachegrind); kompare: a diff tool; kuiviewer: a tool for displaying a designer's UI files; lokalize: a computer-aided translation system focusing on productivity and performance; and umbrello: a UML modeller and UML diagram tool.

Bug Fixes

BZ#857002

Previously, the umbrello UML modeller used logic based on recursive calls. As a consequence if a user created a diagram that had dependency graph cycles, umbrello entered an infinite loop and terminated unexpectedly with a segmentation fault. With this update, the application logic has been changed to use stack-based parent resolution. As a result, umbrello no longer terminates in the described scenario.

BZ#908709

Prior to this update, the kompare utility hid underscore characters located at the bottom of a highlighted difference block when using certain fonts. This update fixes this bug. As a result, kompare correctly displays underscore characters in the described situation.

Users of kdesdk are advised to upgrade to these updated packages, which fix these bugs.

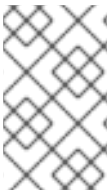
8.103. KEEPALIVED

8.103.1. RHBA-2014:1510 — keepalived bug fix and enhancement update

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

The keepalived packages provide 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 their state. The keepalived daemon also implements the Virtual Router Redundancy Protocol (VRRP), allowing router or director failover to achieve high availability.

This update also fixes the following bugs:



NOTE

The keepalived packages have been upgraded to upstream version 1.2.13, which provides a number of bug fixes and enhancements over the previous version. (BZ#1052380, BZ#1077201)

This update also fixes the following bugs:

Bug Fixes

BZ#967641

Previously, the VRRP alert emails sent by the keepalived daemon did not contain the "to" header, which complicated filtering and sorting such messages by email software. With this update, keepalived has been modified to include the "to" header into email alerts as expected.

BZ#1007575

Previously, when keepalived compared the local primary IP address with another IP address, these two addresses had different byte-ordering. Consequently, multiple routers were created in a master state. With this update, the local primary IP address is converted to network byte order before the comparison, thus fixing this bug.

The keepalived packages have been upgraded to upstream version 1.2.13, which provides a number of bug fixes and enhancements over the previous version. (BZ#1052380, BZ#1077201)

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

8.104. KERNEL

8.104.1. RHSA-2015:1081 — Important: kernel security, bug fix, and enhancement update

Updated kernel packages that fix several security issues and several bugs are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2015-1805, Important

It was found that the Linux kernel's implementation of vectored pipe read and write functionality did not take into account the I/O vectors that were already processed when retrying after a failed atomic access operation, potentially resulting in memory corruption due to an I/O vector array overrun. A local, unprivileged user could use this flaw to crash the system or, potentially, escalate their privileges on the system.

CVE-2015-3331, Important

A buffer overflow flaw was found in the way the Linux kernel's Intel AES-NI instructions optimized version of the RFC4106 GCM mode decryption functionality handled fragmented packets. A remote attacker could use this flaw to crash, or potentially escalate their privileges on, a system over a connection with an active AES-GCM mode IPSec security association.

CVE-2014-9419, Low

An information leak flaw was found in the way the Linux kernel changed certain segment registers and thread-local storage (TLS) during a context switch. A local, unprivileged user could use this flaw to leak the user space TLS base address of an arbitrary process.

CVE-2014-9420, Low

It was found that the Linux kernel's ISO file system implementation did not correctly limit the traversal of Rock Ridge extension Continuation Entries (CE). An attacker with physical access to the system could use this flaw to trigger an infinite loop in the kernel, resulting in a denial of service.

CVE-2014-9585, Low

An information leak flaw was found in the way the Linux kernel's Virtual Dynamic Shared Object (vDSO) implementation performed address randomization. A local, unprivileged user could use this flaw to leak kernel memory addresses to user-space.

Red Hat would like to thank Carl Henrik Lunde for reporting CVE-2014-9420. The security impact of the CVE-2015-1805 issue was discovered by Red Hat.

Bug Fixes

BZ#1201674

When repeating a Coordinated Universal Time (UTC) value during a leap second (when the UTC time should be 23:59:60), the International Atomic Time (TAI) timescale previously stopped as the kernel NTP code incremented the TAI offset one second later than expected. A patch has been provided, which fixes the bug by incrementing the offset during the leap second itself. Now, the correct TAI is set during the leap second.

BZ#1204626

Due to a race condition, deleting a cgroup while pages belonging to that group were being swapped in could trigger a kernel crash. This update fixes the race condition, and deleting a cgroup is now safe even under heavy swapping.

BZ#1207815

Previously, the open() system call in some cases failed with an EBUSY error if the opened file was also being renamed at the same time. With this update, the kernel automatically retries open() when this failure occurs, and if the retry is not successful either, open() now fails with an ESTALE error.

BZ#1208620

Prior to this update, cgroup blocked new threads from joining the target thread group during cgroup migration, which led to a race condition against exec() and exit() functions, and a consequent kernel panic. This bug has been fixed by extending thread group locking such that it covers all operations which can alter the thread group - fork(), exit(), and exec(), and cgroup migration no longer causes the kernel to panic.

BZ#1211940

The hrtimer_start() function previously attempted to reinsert a timer which was already defined. As a consequence, the timer node pointed to itself and the rb_insert_color() function entered an infinite loop. This update prevents the hrtimer_enqueue_reprogram() function from racing and makes sure the timer state in remove_hrtimer() is preserved, thus fixing the bug.

BZ#1144442

Previously, the bridge device did not propagate VLAN information to its ports and Generic Receive Offload (GRO) information to the connected devices. This resulted in lower receive performance of VLANs over bridge devices because GRO was not enabled. An attempt to resolve this problem was made with BZ#858198 by introducing a patch that allows VLANs to be registered with the participating bridge ports and adds GRO to the bridge device feature set. However, this attempt introduced a number of regressions, which broke the vast majority of stacked setups involving bridge devices and VLANs. This update reverts the patch provided by BZ#858198 and removes support for this capability.

BZ#1199900

Previously, the kernel initialized FPU state for the signal handler too early, right after the current state was saved for the sigreturn() function. As a consequence, a task could lose its floating-point unit (FPU) context if the signal delivery failed. The fix ensures that the drop_init_fpu() fuction is only called when the signal is delivered successfully, and FPU context is no longer lost in the described situation.

BZ#1203366

On mounting a Common Internet File System (CIFS) share using kerberos authentication, the CIFS module uses the request_key mechanism to obtain the user's krb5 credentials. Once the key has been used and is no longer needed, CIFS revoked it. This caused key revoked errors to be returned when attempting to refetch the key. To fix this bug, the key_invalidate() call has been backported from the upstream code to discard the key. This call renders the discarded key invisible to further searches and wakes up the garbage collector immediately to remove the key from the keyrings and to destroy it. As a result, discarded keys are immediately cleared and are no longer returned on key searches.

BZ#1203544

Previously, the fc_remote_port_del() call preceded the calls to re-establish the session with the Fibre Channel (FC) transport with the fc_remote_port_add() and fc_remote_port_rolechg() functiones. With

this update, the fc_remote_port_del() call has been removed before re-establishing the connection, which prevents the race condition from occurring.

BZ#1210593

Due to a race condition in the build_id_cache__add_s() function, system files could be truncated. This update fixes the race condition, and system files are no longer truncated in the aforementioned situation.

BZ#1212057

Prior to this update, the "--queue-balance" option did not distribute traffic over multiple queues as the option ignored a request to balance among the given range and only used the first queue number given. As a consequence, the kernel traffic was limited to one queue. The underlying source code has been patched, and the kernel traffic is now balanced within the given range.

Enhancements

BZ#1173501, BZ#1173562

This update introduces a set of patches with a new VLAN model to conform to upstream standards. In addition, this set of patches fixes other issues such as transmision of Internet Control Message Protocol (ICMP) fragments.

Users of kernel 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.

8.104.2. RHSA-2015:0864 — Important: 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.

Red Hat Product Security 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 below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2014-3215, Important

A flaw was found in the way seunshare, a utility for running executables under a different security context, used the capng_lock functionality of the libcap-ng library. The subsequent invocation of suid root binaries that relied on the fact that the setuid() system call, among others, also sets the saved set-user-ID when dropping the binaries' process privileges, could allow a local, unprivileged user to potentially escalate their privileges on the system. Note: the fix for this issue is the kernel part of the overall fix, and introduces the PR_SET_NO_NEW_PRIVS functionality and the related SELinux exec transitions support.

CVE-2015-1421, Important

A use-after-free flaw was found in the way the Linux kernel's SCTP implementation handled authentication key reference counting during INIT collisions. A remote attacker could use this flaw to crash the system or, potentially, escalate their privileges on the system.

CVE-2014-3690, Moderate

It was found that the Linux kernel's KVM implementation did not ensure that the host CR4 control register value remained unchanged across VM entries on the same virtual CPU. A local, unprivileged user could use this flaw to cause a denial of service on the system.

CVE-2014-7825, Moderate

An out-of-bounds memory access flaw was found in the syscall tracing functionality of the Linux kernel's perf subsystem. A local, unprivileged user could use this flaw to crash the system.

CVE-2014-7826, Moderate

An out-of-bounds memory access flaw was found in the syscall tracing functionality of the Linux kernel's ftrace subsystem. On a system with ftrace syscall tracing enabled, a local, unprivileged user could use this flaw to crash the system, or escalate their privileges.

CVE-2014-8171, Moderate

It was found that the Linux kernel memory resource controller's (memcg) handling of OOM (out of memory) conditions could lead to deadlocks. An attacker able to continuously spawn new processes within a single memory-constrained cgroup during an OOM event could use this flaw to lock up the system.

CVE-2014-9529, Moderate

A race condition flaw was found in the way the Linux kernel keys management subsystem performed key garbage collection. A local attacker could attempt accessing a key while it was being garbage collected, which would cause the system to crash.

CVE-2014-8884, Low

A stack-based buffer overflow flaw was found in the TechnoTrend/Hauppauge DEC USB device driver. A local user with write access to the corresponding device could use this flaw to crash the kernel or, potentially, elevate their privileges on the system.

CVE-2014-9584, Low

An information leak flaw was found in the way the Linux kernel's ISO9660 file system implementation accessed data on an ISO9660 image with RockRidge Extension Reference (ER) records. An attacker with physical access to the system could use this flaw to disclose up to 255 bytes of kernel memory.

Red Hat would like to thank Andy Lutomirski for reporting CVE-2014-3215 and CVE-2014-3690, Robert Święcki for reporting CVE-2014-7825 and CVE-2014-7826, and Carl Henrik Lunde for reporting CVE-2014-9584. The CVE-2015-1421 issue was discovered by Sun Baoliang of Red Hat.

Bug Fixes

BZ#1195747

Due to a regression, when large reads which partially extended beyond the end of the underlying device were done, the raw driver returned the EIO error code instead of returning a short read covering the valid part of the device. The underlying source code has been patched, and the raw driver now returns a short read for the remainder of the device.

BZ#1187639

Previously, a NULL pointer check that is needed to prevent an oops in the nfs_async_inode_return_delegation() function was removed. As a consequence, a NFS4 client could

terminate unexpectedly. The missing NULL pointer check has been added back, and NFS4 client no longer crashes in this situation.

BZ#1187666

A failure to leave a multicast group which had previously been joined prevented the attempt to unregister from the "sa" service. Multiple locking issues in the IPoIB multicast join and leave processing have been fixed so that leaving a group that has completed its join process is successful. As a result, attempts to unregister from the "sa" service no longer lock up due to leaked resources.

BZ#1187664

Due to unbalanced multicast join and leave processing, the attempt to leave a multicast group that had not previously completed a join became unresponsive. This update resolves multiple locking issues in the IPoIB multicast code that allowed multicast groups to be left before the joining was entirely completed. Now, multicast join and leave failures or lockups no longer occur in the described situation.

BZ#1188339

The kernel source code contained two definitions of the cpu_logical_map() function, which maps logical CPU numbers to physical CPU addresses. When translating the logical CPU number to the corresponding physical CPU number, the kernel used the second definition of cpu_logical_map(), which always used a one-to-one mapping of logical to physical CPU addresses. This mapping was, however, wrong after a reboot, especially if the target CPU was in the "stopped" state. Consequently, the system became unresponsive or showed unexpected latencies. With this update, the second definition of cpu_logical_map() has been removed. As a result, the kernel now correctly translates the CPU number to its physical address, and no unexpected latencies occur in this scenario.

BZ#1188838

Previously, the kernel could under certain circumstances provide the tcp_collapse() function with a socket buffer (SKB) whose "headroom" was equal to the value of the PAGE_SIZE variable. Consequently, the copy value was zero in the loop, which could never exit because it was not making forward progress. To fix this problem, the loop has been rewritten to avoid the incorrect calculation. Instead, the loop copies either the value of the PAGE_SIZE variable or the size of the buffer, whichever is bigger. As a result, the tcp_collapse() function is no longer apt to get stuck in the loop, because the copy is always non-zero as long as long as the "end" differs from the "start".

BZ#1188941

Prior to this update, when using the fibre channel driver, a race condition occurred in the rport scsi_remove_target() function. As a consequence, the kernel terminated unexpectedly when dereferencing an invalid address. To fix this bug, the changes to the reference counting infrastructure have been reverted, and the system no longer crashes.

BZ#1191916

On older systems without the QCI instruction, all possible domains are probed via TAPQ instruction. Prior to this update, a specification exception could occur when this instruction was called for probing values greater than 16; for example, during the execution of the "insmod" command or the reset of the AP bus on machines without the QCI instruction (z10, z196, z114). zEC12 and newer systems were not affected. Consequently, loading the z90crypt kernel module caused a panic. Now, the domain checking function has been corrected to limit the allowed range if no QCI information is available. As a result, users are able to successfully load and perform cryptographic functions with the z90crypt device driver.

BZ#1192055

Previously, KVM took a page fault with interrupts disabled. Consequently, the page fault handler tried to take a lock, but KSM sent an IPI while taking the same lock. Then KSM waited for the IPI to be processed, but KVM would not process it until it took the lock. KSM and KVM would eventually encounter a deadlock, each waiting for the other. With this update, the kernel avoids operations that can page fault while interrupts are disabled. As a result, KVM and KSM are no longer prone to a deadlock in the aforementioned scenario.

BZ#1192105

The USB core uses the "hcpriv" member of the USB request block to determine whether a USB Request Block (URB) is active, but the ehci-hcd driver was not setting this correctly when it queued isochronous URBs. This in combination with a defect in the snd-usb-audio driver could cause URBs to be reused without waiting for them to complete. Consequently, list corruption followed by system freeze or a kernel crash occurred. To fix this problem, the ehci-hcd driver code has been updated to properly set the "hcpriv" variable for isochronous URBs, and the snd-usb-audio driver has been updated to synchronize pending stop operations on an endpoint before continuing with preparing the PCM stream. As a result, list corruption followed by system freeze or a crash no longer occurs.

BZ#1193639

Previously, the Hewlett Packard Smart Array (HPSA) driver in conjunction with an older version of the HPSA firmware and the hp-snmp-agent monitoring software used the "system work queue" shared resource for an extensively long time. Consequently, random other tasks were blocked until the HPSA driver released the work queue, and messages such as the following were logged:

```
INFO: task sshd:6425 blocked for more than 120 seconds.
INFO: task ptymonitor:22510 blocked for more than 120 seconds.
```

With this update, the HPSA driver creates its own local work queue, which fixes this problem.

BZ#1198329

Prior to this update, the GFS2 file system's "Splice Read" operation, which is used for functions such as sendfile(), was not properly allocating a required multi-block reservation structure in memory. As a consequence, when the GFS2 block allocator was called to assign blocks of data, it tried to dereference the structure, which resulted in a kernel panic. Now, GFS2's "Splice read" operation has been changed so that it properly allocates the necessary reservation structure in memory prior to calling the block allocator. As a result, sendfile() now works properly for GFS2.

Users of kernel 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.

8.104.3. RHSA-2015:0087 — 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.

Red Hat Product Security 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 below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2014-7841, Important

A flaw was found in the way the Linux kernel's SCTP implementation validated INIT chunks when performing Address Configuration Change (ASCONF). A remote attacker could use this flaw to crash the system by sending a specially crafted SCTP packet to trigger a NULL pointer dereference on the system.

CVE-2014-4656, Moderate

An integer overflow flaw was found in the way the Linux kernel's Advanced Linux Sound Architecture (ALSA) implementation handled user controls. A local, privileged user could use this flaw to crash the system.

The CVE-2014-7841 issue was discovered by Liu Wei of Red Hat.

Bug Fixes

BZ#1161420

LVM2 thin provisioning is sensitive to I/Os within a full RAID stripe is issued to the controller's write-back cache in close proximity. This update improves LVM2 thin provisioning to work more efficiently on RAID devices.

BZ#1161421

Previously, under a heavy I/O load, a timeout of an unresponsive task could occur while using LVM2 thin provisioning. With this update, various infrastructure used by LVM2 thin provisioning have been improved to be more efficient and correct. This includes the use of more efficient data structures, throttling worker threads to prevent an application from sending more I/O than can be handled, and pre-fetching metadata. This update also fixes the eviction logic used by the metadata I/O buffering layer, which ensures that metadata blocks are not evicted prematurely.

BZ#1162072

Due to a malfunction in the USB controller driver, some data stream metadata was dropped. As a consequence, the integrated camera to failed to record with the following error message:

```
libv4l2: error turning on stream: No space left on device
```

This update fixes the data stream metadata handling, and the integrated camera works as expected.

BZ#1165986

Before this update, a race condition occurred in the spin-lock logic on the PowerPC platform. Consequently, workloads caused heavy use of Inter-Process Communication (IPC), and the kernel could terminate unexpectedly. This update adds proper synchronization to the PowerPC spin-lock framework. As a result, the kernel no longer crashes under heavy use of IPC.

BZ#1163214

Due to an overlooked piece of code that initializes the pre-operation change attribute, certain workloads could generate unnecessary cache invalidations and additional NFS read operations. This update fixes the initialization of the pre_change_attr field, which prevents unnecessarily cached data invalidation.

BZ#1165001

Previously, under certain error conditions gfs2_converter introduced incorrect values for the on-disk inode's di_goal_meta field. As a consequence, gfs2_converter returned the EBADSLT error on such

inodes and did not allow creation of the new files in directories or new blocks in regular files. The fix allows gfs2_converter to set a sensible goal value if a corrupt one is encountered and proceed with normal operations. With this update, gfs2_converter implicitly fixes any corrupt goal values, and thus no longer disrupts normal operations.

BZ#1165002

Previously, under certain error conditions using the semaphore utility caused the kernel to become unresponsive. With update a patch has been applied to fix this bug. As a result, the the kernel hangs no longer occur while using semaphore.

BZ#1165985

Before this update, due to a coding error in the e100 Ethernet driver update, physical layers (PHYs) did not initialize correctly. This could cause RX errors and decreased throughput, especially when using long UTP cabling. This update fixes the coding error, and as a result, the aforementioned scenario no longer occurs on the e100 Ethernet device.

BZ#1168129

Before this update, a flaw in the duplicate reply cache in the NFS daemon allowed entries to be freed while they were still used. Consequently, a heavily loaded NFS daemon could terminate unexpectedly if an RPC call took a long time to process. The cache has been fixed to protect such entries from freeing, and the server now functions normally in the aforementioned scenario.

BZ#1168504

Previously, external journal blocks were handled as blocks causing an increase of processor usage. Consequently, on the ext4 file systems configured with an external journal device, the df command could show negative values due to the subtraction of such journal blocks amount from the used blocks amount. With this update, the external journal blocks are handled properly, and therefore df no longer returns negative values.

BZ#1169433

Before this update, raising the SIGBUS signal did not include a siginfo structure describing the cause of the SIGBUS exception. As a consequence, applications that use huge pages using the libhugetlbfs library failed. The PACKAGE_NAME has been updated to raise SIGBUS with a siginfo structure, to deliver BUS_ADRERR as si_code, and to deliver the address of the fault in the si_addr field. As a result, applications that use huge pages no longer fail in the aforementioned scenario.

BZ#1172022

Previously, accessing a FUSE-based file system from kernel space could cause the kernel to become unresponsive during an inode look-up operation. To fix this bug, existing flags are verified before dereference occurs in the FUSE look-up handler. As a result, accessing a FUSE-based file system from kernel space works as expected.

BZ#1172024

Previously, hot plugging of a USB EHCI controller could cause the kernel to become unresponsive. This update fixes the handling of a race condition in the EHCI error path during the hot-plugging event, and the kernel no longer hangs.

BZ#1172025

Previously, the system functions semop() and semtimedop() did not update the time of the semaphore update located in the structure sem_otime, which was inconsistent with the function description in the man pages. With this update, a patch has been applied to fix this bug. As a result,

semop() and semtimedop() now properly update the sem_otime structure.

BZ#1172027

Before this update, when forwarding a packet, the iptables target TCPOPTSTRIP used the tcp_hdr() function to locate the option space. Consequently, TCPOPTSTRIP located the incorrect place in the packet, and therefore did not match options for stripping. With this update, TCPOPTSTRIP now uses the TCP header itself to locate the option space. As a result, the options are now properly stripped.

BZ#1172764

Prior to this update, the ipset utility computed incorrect values of timeouts from an old IP set, and these values were then supplied to a IP new set. As a consequence, a resize on a IP set with a timeouts option enabled could supply corrupted data from an old IP set. This bug has been fixed by properly reading timeout values from an old set before supplying them to a new set.

BZ#1172029

Previously, under certain conditions, a race condition between the semaphore creation code and the semop() function caused the kernel to become unresponsive. With this update, a patch has been applied, and the kernel hangs no longer occur.

BZ#1172030

Prior to this update, a NULL pointer dereference could occur when then usb_wwan device driver was performing a disconnect operation. The usb_wwan disconnect procedure has been replaced with the port_remove procedure and, as a result, the kernel no longer hangs when removing a WWAN USB device.

BZ#1175509

The usage of PCLMULQDQ instruction required the invocation of the kernel_fpu_begin() and kernel_fpu_end() functions. Consequently, the usage of the PCLMULQDQ instruction for the CRC32C checksum calculation incurred some increase of processor usage. With this update, a new function has been added in order to calculate the CRC32C checksum using the PCLMULQDQ instruction on processors that support this feature, which provides speedup over using the CRC32 instruction only.

Users of kernel 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.

8.104.4. RHSA-2014:1392 — Important: kernel security, bug fix, and enhancement update

Updated kernel packages that fix multiple 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 sixth regular update.

Red Hat Product Security 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 below.

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2014-5077, Important

A NULL pointer dereference flaw was found in the way the Linux kernel's Stream Control Transmission Protocol (SCTP) implementation handled simultaneous connections between the same hosts. A remote attacker could use this flaw to crash the system.

CVE-2013-2596, Important

An integer overflow flaw was found in the way the Linux kernel's Frame Buffer device implementation mapped kernel memory to user space via the mmap syscall. A local user able to access a frame buffer device file (/dev/fb*) could possibly use this flaw to escalate their privileges on the system.

CVE-2013-4483, Moderate

A flaw was found in the way the ipc_rcu_putref() function in the Linux kernel's IPC implementation handled reference counter decrementing. A local, unprivileged user could use this flaw to trigger an Out of Memory (OOM) condition and, potentially, crash the system.

CVE-2014-0181, Moderate

It was found that the permission checks performed by the Linux kernel when a netlink message was received were not sufficient. A local, unprivileged user could potentially bypass these restrictions by passing a netlink socket as stdout or stderr to a more privileged process and altering the output of this process.

CVE-2014-3122, Moderate

It was found that the try_to_unmap_cluster() function in the Linux kernel's Memory Managment subsystem did not properly handle page locking in certain cases, which could potentially trigger the BUG_ON() macro in the mlock_vma_page() function. A local, unprivileged user could use this flaw to crash the system.

CVE-2014-3601, Moderate

A flaw was found in the way the Linux kernel's kvm_iommu_map_pages() function handled IOMMU mapping failures. A privileged user in a guest with an assigned host device could use this flaw to crash the host.

CVE-2014-4653, CVE-2014-4654, CVE-2014-4655, Moderate

Multiple use-after-free flaws were found in the way the Linux kernel's Advanced Linux Sound Architecture (ALSA) implementation handled user controls. A local, privileged user could use either of these flaws to crash the system.

CVE-2014-5045, Moderate

A flaw was found in the way the Linux kernel's VFS subsystem handled reference counting when performing unmount operations on symbolic links. A local, unprivileged user could use this flaw to exhaust all available memory on the system or, potentially, trigger a use-after-free error, resulting in a system crash or privilege escalation.

CVE-2014-4608, Low

An integer overflow flaw was found in the way the lzo1x_decompress_safe() function of the Linux kernel's LZO implementation processed Literal Runs. A local attacker could, in extremely rare cases, use this flaw to crash the system or, potentially, escalate their privileges on the system.

Red Hat would like to thank Vladimir Davydov of Parallels for reporting CVE-2013-4483, Jack Morgenstein of Mellanox for reporting CVE-2014-3601, Vasily Averin of Parallels for reporting CVE-2014-5045, and Don A. Bailey from Lab Mouse Security for reporting CVE-2014-4608. The security impact of

the CVE-2014-3601 issue was discovered by Michael Tsirkin of Red Hat.

Bug Fixes

BZ#1065187

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#1063699

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#704190

Previously, when using a bridge interface configured on top of a bonding interface, the bonding driver was not aware of IP addresses assigned to the bridge. Consequently, with ARP monitoring enabled, the ARP monitor could not target the IP address of the bridge when probing the same subnet. The bridge was thus always reported as being down and could not be reached. With this update, the bonding driver has been made aware of IP addresses assigned to a bridge configured on top of a bonding interface, and the ARP monitor can now probe the bridge as expected. Note that the problem still occurs if the arp_validate option is used. Therefore, do not use this option in this case until this issue is fully resolved.

BZ#1063478, BZ#1065398, BZ#1065404, BZ#1043540, BZ#1096328

Several concurrency problems, that could result in data corruption, were found in the implementation of CTR and CBC modes of operation for AES, DES, and DES3 algorithms on IBM S/390 systems. Specifically, a working page was not protected against concurrency invocation in CTR mode. The fallback solution for not getting a working page in CTR mode did not handle iv values correctly. The CBC mode used did not properly save and restore the key and iv values in some concurrency situations. All these problems have been addressed in the code and the concurrent use of the aforementioned algorithms no longer cause data corruption.

BZ#1061873

A previous change in the Advanced Programmable Interrupt Controller (APIC) code caused a regression on certain Intel CPUs using a Multiprocessor (MP) table. An attempt to read from the local APIC (LAPIC) could be performed before the LAPIC was mapped, resulting in a kernel crash during a system boot. A patch has been applied to fix this problem by mapping the LAPIC as soon as possible when parsing the MP table.

BZ#1060886

A miscalculation in the "radix_tree" swap encoding corrupted swap area indexes bigger than 8 by truncating lower bits of swap entries. Consequently, systems with more than 8 swap areas could trigger a bogus OOM scenario when swapping out to such a swap area. This update fixes this problem by reducing a return value of the SWP_TYPE_SHIFT() function and removing a broken function call from the read_swap_header() function.

BZ#1060381

Previously some device mapper kernel modules, such as dm-thin, dm-space-map-metadata, and dm-bufio, contained various bugs that had adverse effects on their proper functioning. This update

backports several upstream patches that resolve these problems, including a fix for the metadata resizing feature of device mapper thin provisioning (thinp) and fixes for read-only mode for dm-thin and dm-bufio. As a result, the aforementioned kernel modules now contain the latest upstream changes and work as expected.

BZ#1059808

When an attempt to create a file on the GFS2 file system failed due to a file system quota violation, the relevant VFS inode was not completely uninitialized. This could result in a list corruption error. This update resolves this problem by correctly uninitializing the VFS inode in this situation.

BZ#1059777

In Red Hat Enterprise Linux 6.5, the TCP Segmentation Offload (TSO) feature is automatically disabled if the corresponding network device does not report any CSUM flag in the list of its features. Previously, VLAN devices that were configured over bonding devices did not propagate its NETIF_F_NO_CSUM flag as expected, and their feature lists thus did not contain any CSUM flags. As a consequence, the TSO feature was disabled for these VLAN devices, which led to poor bandwidth performance. With this update, the bonding driver propagates the aforementioned flag correctly so that network traffic now flows through VLAN devices over bonding without any performance problems.

BZ#1059586

Due to a bug in the mlx4_en module, a data structure related to time stamping could be accessed before being initialized. As a consequence, loading mlx4_en could result in a kernel crash. This problem has been fixed by moving the initiation of the time stamp mechanism to the correct place in the code.

BZ#1059402

Due to a previous change that was refactoring the Generic Routing Encapsulation (GRE) tunneling code, the ip_gre module did not work properly. As a consequence, GRE interfaces dropped every packet that had the Explicit Congestion Notification (ECN) bit set and did not have the ECN-Capable Transport (ECT) bit set. This update reintroduces the ipgre_ecn_decapsulate() function that is now used instead of the IP_ECN_decapsulate() function that was not properly implemented. The ip_gre module now works correctly and GRE devices process all packets as expected.

BZ#1059334

When removing an inode from a name space on an XFS file system, the file system could enter a deadlock situation and become unresponsive. This happened because the removal operation incorrectly used the AGF and AGI locks in the opposite order than was required by the ordering constraint, which led to a possible deadlock between the file removal and inode allocation and freeing operations. With this update, the inode's reference count is dropped before removing the inode entry with the first transaction of the removal operation. This ensures that the AGI and AGF locks are locked in the correct order, preventing any further deadlocks in this scenario.

BZ#1059325

Previously, the for_each_isci_host() macro was incorrectly defined so it accessed an out-of-range element for a 2-element array. This macro was also wrongly optimized by GCC 4.8 so that it was executed too many times on platforms with two SCU controllers. As a consequence, the system triggered a kernel panic when entering the S3 state, or a kernel oops when removing the isci module. This update corrects the aforementioned macro and the described problems no longer occur.

BZ#1067722

A previous change enabled receive acceleration for VLAN interfaces configured on a bridge interface.

However, this change allowed VLAN-tagged packets to bypass the bridge and be delivered directly to the VLAN interfaces. This update ensures that the traffic is correctly processed by a bridge before it is passed to any VLAN interfaces configured on that bridge.

BZ#844450

The Completely Fair Scheduler (CFS) did not verify whether the CFS period timer is running while throttling tasks on the CFS run queue. Therefore under certain circumstances, the CFS run queue became stuck because the CFS period timer was inactive and could not be restarted. To fix this problem, the CFS now restarts the CFS period timer inside the throttling function if it is inactive.

BZ#1069028

Due to a bug in the ixgbevf driver, the stripped VLAN information from incoming packets on the ixgbevf interface could be lost, and such packets thus did not reach a related VLAN interface. This problem has been fixed by adding the packet's VLAN information to the Socket Buffer (skb) before passing it to the network stack. As a result, the ixgbevf driver now passes the VLAN-tagged packets to the appropriate VLAN interface.

BZ#1069737

Previous patches to the CIFS code introduced a regression that prevented users from mounting a CIFS share using the NetBIOS over TCP service on the port 139. This problem has been fixed by masking off the top byte in the get_rfc1002_length() function.

BZ#880024

Previously, the locking of a semtimedop semaphore operation was not fine enough with remote non-uniform memory architecture (NUMA) node accesses. As a consequence, spinlock contention occurred, which caused delays in the semop() system call and high load on the server when running numerous parallel processes accessing the same semaphore. This update improves scalability and performance of workloads with a lot of semaphore operations, especially on larger NUMA systems. This improvement has been achieved by turning the global lock for each semaphore array into a per-semaphore lock for many semaphore operations, which allows multiple simultaneous semop() operations. As a result, performance degradation no longer occurs.

BZ#886723

A rare race between the file system unmount code and the file system notification code could lead to a kernel panic. With this update, a series of patches has been applied to the kernel to prevent this problem.

BZ#885517

A bug in the bio layer could prevent user space programs from writing data to disk when the system run under heavy RAM memory fragmentation conditions. This problem has been fixed by modifying a respective function in the bio layer to refuse to add a new memory page only if the page would start a new memory segment and the maximum number of memory segments has already been reached.

BZ#1070856

A bug in the qla2xxx driver caused the kernel to crash. This update resolves this problem by fixing an incorrect condition in the "for" statement in the qla2x00_alloc_iocbs() function.

BZ#1072373

A previous change that introduced global clock updates caused guest machines to boot slowly when the host Time Stamp Counter (TSC) was marked as unstable. The slow down increased with the number of vCPUs allocated. To resolve this problem, a patch has been applied to limit the rate of the

global clock updates.

BZ#1055644

A previously backported patch to the XFS code added an unconditional call to the xlog_cil_empty() function. If the XFS file system was mounted with the unsupported nodelaylog option, that call resulted in access to an uninitialized spin lock and a consequent kernel panic. To avoid this problem, the nodelaylog option has been disabled; the option is still accepted but has no longer any effect. (The nodelaylog mount option was originally intended only as a testing option upstream, and has since been removed.)

BZ#1073129

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 for 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#1073218

A bug in the vmxnet3 driver allowed potential race conditions to be triggered when the driver was used with the netconsole module. The race conditions allowed the driver's internal NAPI poll routine to run concurrently with the netpoll controller routine, which resulted in data corruption and a subsequent kernel panic. To fix this problem, the vmxnet3 driver has been modified to call the appropriate interrupt handler to schedule NAPI poll requests properly.

BZ#1075713

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#1053547

The SCTP sctp_connectx() ABI did not work properly for 64-bit kernels compiled with 32-bit emulation. As a consequence, applications utilizing the sctp_connectx() function did not run in this case. To fix this problem, a new ABI has been implemented; the COMPAT ABI enables to copy and transform user data from a COMPAT-specific structure to a SCTP-specific structure. Applications that require sctp_connectx() now work without any problems on a system with a 64-bit kernel compiled with 32-bit emulation.

BZ#1075805

Previously, if a hrtimer interrupt was delayed, all future pending hrtimer events that were queued on the same processor were also delayed until the initial hrtimer event was handled. This could cause all hrtimer processing to stop for a significant period of time. To prevent this problem, the kernel has been modified to handle all expired hrtimer events when handling the initially delayed hrtimer event.

BZ#915862

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#1045150

The code responsible for creating and binding of packet sockets was not optimized and therefore applications that utilized the socket() and bind() system calls did not perform as expected. A patch has been applied to the packet socket code so that latency for socket creating and binding is now significantly lower in certain cases.

BZ#919756

A race condition between completion and timeout handling in the block device code could sometimes trigger a BUG_ON() assertion, resulting in a kernel panic. This update resolves this problem by relocating a relevant function call and the BUG_ON() assertion in the code.

BZ#1044117

The context of the user's process could not be previously saved on PowerPC platforms if the VSX Machine State Register (MSR) bit was set but the user did not provide enough space to save the VSX state. This update allows to clear the VSX MSR bit in such a situation, indicating that there is no valid VSX state in the user context.

BZ#1043733

The kernel task scheduler could trigger a race condition while migrating tasks over CPU cgroups. The race could result in accessing a task that pointed to an incorrect parent task group, causing the system to behave unpredictably, for example to appear being unresponsive. This problem has been resolved by ensuring that the correct task group information is properly stored during the task's migration.

BZ#1043353

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#1043051

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#1042731

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#1040385

When utilizing SCTP over the bonding device in Red Hat Enterprise Linux 6.5 and later, SCTP assumed offload capabilities on virtual devices where it was not guaranteed that underlying physical devices are equipped with these capabilities. As a consequence, checksums of the outgoing packets

became corrupted and a network connection could not be properly established. A patch has been applied to ensure that checksums of the packages to the devices without SCTP checksum capabilities are properly calculated in software fallback. SCTP connections over the bonding devices can now be established as expected in Red Hat Enterprise Linux 6.5 and later.

BZ#1039723

A previous change in the TCP code that extended the "proto" struct with a new function, release_cb(), broke integrity of the kernel Application Binary Interface (kABI). If the core stack called a newly introduced pointer to this function for a module that was compiled against older kernel headers, the call resulted in out-of-bounds access and a subsequent kernel panic. To avoid this problem, the core stack has been modified to recognize a newly introduced slab flag, RHEL_EXTENDED_PROTO. This allows the core stack to safely access the release_cb pointer only for modules that support it.

BZ#1039534

A previous change removed the ZONE_RECLAIM_LOCKED flag from Linux memory management code in order to fix a NUMA node allocation problem in the memory zone reclaim logic. However, the flag removal allowed concurrent page reclaiming within one memory zone, which, under heavy system load, resulted in unwanted spin lock contention and subsequent performance problems (systems became slow or unresponsive). This update resolves this problem by preventing reclaim threads from scanning a memory zone if the zone does not satisfy scanning requirements. Systems under heavy load no longer suffer from CPU overloading but sustain their expected performance.

BZ#1082127

NFSv4 incorrectly handled a situation when an NFS client received an NFS4ERR_ADMIN_REVOKED error after sending a CLOSE operation. As a consequence, the client kept sending the same CLOSE operation indefinitely although it was receiving NFS4ERR_ADMIN_REVOKED errors. A patch has been applied to the NFSv4 code to ensure that the NFS client sends the particular CLOSE operation only once in this situation.

BZ#1037467

Due to recent changes in the Linux memory management, the kernel did not properly handle per-CPU LRU page vectors when hot unplugging CPUs. As a consequence, the page vector of the relevant offline CPU kept memory pages for memory accounting. This prevented the libvirtd daemon from removing the relevant memory cgroup directory upon system shutdown, rendering libvirtd unresponsive. To resolve this problem, the Linux memory management now properly flushes memory pages of offline CPUs from the relevant page vectors.

BZ#1037465

An incorrectly placed function call in the cgroup code prevented the notify_on_release functionality from working properly. This functionality is used to remove empty cgroup directories, however due to this bug, some empty cgroup directories were remaining on the system. This update ensures that the notify_on_release functionality is always correctly triggered by correctly ordering operations in the cgroup_task_migrate() function.

BZ#963785

Previously, NFSv4 allowed an NFSv4 client to resume an expired or lost file lock. This could result in file corruption if the file was modified in the meantime. This problem has been resolved by a series of patches ensuring that an NFSv4 client no longer attempts to recover expired or lost file locks.

BZ#1036972

Systems that use NFS file systems could become unresponsive or trigger a kernel oops due to a use-after-free bug in the duplicate reply cache (DRC) code in the nfsd daemon. This problem has been

resolved by modifying nfsd to unhash DRC entries before attempting to use them and to prefer to allocate a new DRC entry from the slab instead of reusing an expired entry from the list.

BZ#1036312

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#975248

A bug in the ixgbe driver caused that IPv6 hardware filtering tables were not correctly rewritten upon interface reset when using a bridge device over the PF interface in an SR-IOV environment. As a result, the IPv6 traffic between VFs was interrupted. An upstream patch has been backported to modify the ixgbe driver so that the update of the Multimedia Terminal Adapter (MTA) table is now unconditional, avoiding possible inconsistencies in the MTA table upon PF's reset. The IPv6 traffic between VFs proceeds as expected in this scenario.

BZ#1116947

Later Intel CPUs added a new "Condition Changed" bit to the MSR_CORE_PERF_GLOBAL_STATUS register. Previously, the kernel falsely assumed that this bit indicates a performance interrupt, which prevented other NMI handlers from running and executing. To fix this problem, a patch has been applied to the kernel to ignore this bit in the perf code, enabling other NMI handlers to run.

BZ#975908

Due to a bug in the mlx4 driver, Mellanox Ethernet cards were brought down unexpectedly while adjusting their Tx or 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#1083748

Previously, hardware could execute commands send by drivers in FIFO order instead of tagged order. Commands thus could be executed out of sequence, which could result in large latencies and degradation of throughput. With this update, the ATA subsystem tags each command sent to the hardware, ensuring that the hardware executes commands in tagged order. Performance on controllers supporting tagged commands can now increase by 30-50%.

BZ#980188

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#1086450

Previously, the Huge Translation Lookaside Buffer (HugeTLB) unconditionally allowed access to huge pages. However, huge pages may be unsupported in some environments, such as a KVM guest on

the PowerPC architecture when not backed by huge pages, and an attempt to use a base page as a huge page in memory would result in a kernel oops. This update ensures that HugeTLB denies access to huge pages if the huge pages are not supported on the system.

BZ#982770

The restart logic for the memory reclaiming with compaction was previously applied on the level of LRU page vectors. This could, however, cause significant latency in memory allocation because memory compaction does not require only memory pages of a certain cgroup but a whole memory zone. This performance issue has been fixed by moving the restart logic to the zone level and restarting the memory reclaim for all memory cgroups in a zone when the compaction requires more free pages from the zone.

BZ#987634

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#1034269

When a page table is upgraded, a new top level of the page table is added for the virtual address space, which results in a new Address Space Control Element (ASCE). However, the Translation Lookaside Buffer (TLB) of the virtual address space was not previously flushed on page table upgrade. As a consequence, the TLB contained entries associated with the old ASCE which led to unexpected program failures and random data corruption. To correct this problem, the TLB entries associated with the old ASCE are now flushed as expected upon page table upgrade.

BZ#1034268

A previous change in the Linux memory management on IBM System z removed the handler for the Address Space Control Element (ASCE) type of exception. As a consequence, the kernel was unable to handle ASCE exceptions, which led to a kernel panic. Such an exception was triggered, for example, if the kernel attempted to access user memory with an address that was larger than the current page table limit from a user-space program. This problem has been fixed by calling the standard page fault handler, do_dat_exception, if an ASCE exception is raised.

BZ#1104268

Due to a bug in the mount option parser, prefix paths on a CIFS DFS share could be prepended with a double backslash ('\\'), resulting in an incorrect "No such file" error in certain environments. The mount option parser has been fixed and prefix paths now starts with a single backslash as expected.

BZ#995300

Due to a bug in the Infiniband driver, the ip and ifconfig utilities reported the link status of the IP over Infiniband (IPoIB) interfaces incorrectly (as "RUNNING" in case of "ifconfig", and as "UP" in case of "ip") even if no cable was connected to the respective network card. The problem has been corrected by calling the respective netif_carrier_off() function on the right place in the code. The link status of the IPoIB interfaces is now reported correctly in the described situation.

BZ#995576

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#1032350

A bug in the Completely Fair Scheduler (CFS) could, under certain circumstances, trigger a race condition while moving a forking task between cgroups. This race could lead to a free-after-use error and a subsequent kernel panic when a child task was accessed while it was pointing to a stale cgroup of its parent task. A patch has been applied to the CFS to ensure that a child task always points to the valid parent's task group.

BZ#998625

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 (rgrp). 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 rgrp 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 rgrp. This improves GFS2 performance by avoiding unnecessary rgrp 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 rgrp's reservation tree when it was disqualified, which eventually triggered a BUG_ON() macro due to an incorrect count of reserved blocks.

BZ#1032347

Due to a race condition in the cgroup code, the kernel task scheduler could trigger a use-after-free bug when it was moving an exiting task between cgroups, which resulted in a kernel panic. This update avoids the kernel panic by introducing a new function, cpu_cgroup_exit(). This function ensures that the kernel does not release a cgroup that is not empty yet.

BZ#1032343

Due to a race condition in the cgroup code, the kernel task scheduler could trigger a kernel panic when it was moving an exiting task between cgroups. A patch has been applied to avoid this kernel panic by replacing several improperly used function calls in the cgroup code.

BZ#1111631

The automatic route cache rebuilding feature could incorrectly compute the length of a route hash chain if the cache contained multiple entries with the same key but a different TOS, mark, or OIF bit. Consequently, the feature could reach the rebuild limit and disable the routing cache on the system. This problem is fixed by using a helper function that avoids counting such duplicate routes.

BZ#1093819

NFS previously called the drop_nlink() function after removing a file to directly decrease a link count on the related inode. Consequently, NFS did not revalidate an inode cache, and could thus use a stale file handle, resulting in an ESTALE error. A patch has been applied to ensure that NFS validates the inode cache correctly after removing a file.

BZ#1002727

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#1030094

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#1030049

Due to a bug in the NFS code, the state manager and the DELEGRETURN operation could enter a deadlock if an asynchronous session error was received while DELEGRETURN was being processed by the state manager. The state manager became unable to process the failing DELEGRETURN operation because it was waiting for an asynchronous RPC task to complete, which could not have been completed because the DELEGRETURN operation was cycling indefinitely with session errors. A series of patches has been applied to ensure that the asynchronous error handler waits for recovery when a session error is received and the deadlock no longer occurs.

BZ#1030046

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.

BZ#1095796

Due to a bug in the nouveau kernel module, the wrong display output could be modified in certain multi-display configurations. Consequently, on Lenovo Thinkpad T420 and W530 laptops with an external display connected, this could result in the LVDS panel "bleeding" to white during startup, and the display controller might become non-functional until after a reboot. Changes to the display configuration could also trigger the bug under various circumstances. With this update, the nouveau kernel module has been corrected and the said configurations now work as expected.

BZ#1007164

When guest supports Supervisor Mode Execution Protection (SMEP), KVM sets the appropriate permissions bits on the guest page table entries (sptes) to emulate SMEP enforced access. Previously, KVM was incorrectly verifying whether the "smep" bit was set in the host cr4 register instead of the guest cr4 register. Consequently, if the host supported SMEP, it was enforced even though it was not requested, which could render the guest system unbootable. This update corrects the said "smep" bit check and the guest system boot as expected in this scenario.

BZ#1029585

If a statically defined gateway became unreachable and its corresponding neighbor entry entered a FAILED state, the gateway stayed in the FAILED state even after it became reachable again. This prevented routing of the traffic through that gateway. This update allows probing such a gateway automatically and routing the traffic through the gateway again once it becomes reachable.

BZ#1009332

Previously, certain network device drivers did not accept ethtool commands right after they were mounted. As a consequence, the current setting of the specified device driver was not applied and an

error message was returned. The ETHTOOL_DELAY variable has been added, which makes sure the ethtool utility waits for some time before it tries to apply the options settings, thus fixing the bug.

BZ#1009626

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#1029530

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 the module repeatedly, and a kernel panic no longer occurs.

BZ#1011214

The IPv4 and IPv6 code contained several issues related to the conntrack fragmentation handling that prevented fragmented packages from being properly reassembled. This update applies a series of patches and ensures that MTU discovery is handled properly, and fragments are correctly matched and packets reassembled.

BZ#1028682

The kernel did not handle environmental and power warning (EPOW) interrupts correctly. This prevented successful usage of the "virsh shutdown" command to shut down guests on IBM POWER8 systems. This update ensures that the kernel handles EPOW events correctly and also prints informative descriptions for the respective EPOW events. The detailed information about each encountered EPOW can be found in the Real-Time Abstraction Service (RTAS) error log.

BZ#1097915

The bridge MDB RTNL handlers were incorrectly removed after deleting a bridge from the system with more then one bridge configured. This led to various problems, such as that the multicast IGMP snooping data from the remaining bridges were not displayed. This update ensures that the bridge handlers are removed only after the bridge module is unloaded, and the multicast IGMP snooping data now displays correctly in the described situation.

BZ#1098658

A previous change to the SCSI code fixed a race condition that could occur when removing a SCSI device. However, that change caused performance degradation because it used a certain function from the block layer code that was returning different values compared with later versions of the kernel. This update alters the SCSI code to properly utilize the values returned by the block layer code.

BZ#1026864

A previous change to the md driver disabled the TRIM operation for RAID5 volumes in order to prevent a possible kernel oops. However, if a MD RAID volume was reshaped to a different RAID level, this could result in TRIM being disabled on the resulting volume, as the RAID4 personality is used for certain reshapes. A patch has been applied that corrects this problem by setting the stacking limits before changing a RAID level, and thus ensuring the correct discard (TRIM) granularity for the RAID array.

BZ#1025439

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#1025224

There was an error in the tag insertion logic, and the bonding handled cases when a slave device did not have a hardware VLAN acceleration. As a consequence, network packets were tagged twice when passing through slave devices without hardware VLAN tag insertion, and network cards using a VLAN over a bonding device did not work properly. This update removes the redundant VLAN tag insertion logic, and the unwanted behavior no longer occurs.

BZ#1024683

Due to a bug in the Emulex lpfc driver, the driver could not allocate a SCSI buffer properly, which resulted in severe performance degradation of lpfc adapters on 64-bit PowerPC systems. A patch addressing this problem has been applied so that lpfc allocates the SCSI buffer correctly and lpfc adapters now work as expected on 64-bit PowerPC systems.

BZ#1024631

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#1100127

A previous change to the Open vSwitch kernel module introduced a use-after-free problem that resulted in a kernel panic on systems that use this module. This update ensures that the affected object is freed on the correct place in the code, thus avoiding the problem.

BZ#1024024

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#1023897

A bug in the RSXX DMA handling code allowed DISCARD operations to call the pci_unmap_page() function, which triggered a race condition on the PowerPC architecture when DISCARD, READ, and WRITE operations were issued simultaneously. However, DISCARD operations are always assigned a DMA address of 0 because they are never mapped. Therefore, this race could result in freeing memory that was mapped for another operation and a subsequent EEH event. A patch has been applied, preventing the DISCARD operations from calling pci_unmap_page(), and thus avoiding the aforementioned race condition.

BZ#1023272

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#1021325

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#1034237

Due to the locking mechanism that the kernel used while handling Out of Memory (OOM) situations in memory control groups (cgroups), the OOM killer did not work as intended in case that many processes triggered an OOM. As a consequence, the entire system could become or appear to be unresponsive. A series of patches has been applied to improve this locking mechanism so that the OOM killer now works as expected in memory cgroups under heavy OOM load.

BZ#1104503

Due to a bug in the GRE tunneling code, it was impossible to create a GRE tunnel with a custom name. This update corrects behavior of the ip_tunnel_find() function, allowing users to create GRE tunnels with custom names.

BZ#1020685

When the system was under memory stress, a double-free bug in the tg3 driver could have been triggered, resulting in a NIC being brought down unexpectedly followed by a kernel panic. A patch has been applied that restructures the respective code so that the affected ring buffer is freed correctly.

BZ#1021044

If the BIOS returned a negative value for the critical trip point for the given thermal zone during a system boot, the whole thermal zone was invalidated and an ACPI error was printed. However, the thermal zone may still have been needed for cooling. With this update, the ACPI thermal management has been modified to only disable the relevant critical trip point in this situation.

BZ#1020461

Due to a missing part of the bcma driver, the brcmsmac kernel module did not have a list of internal aliases that was needed by the kernel to properly handle the related udev events. Consequently, when the bcma driver scanned for the devices at boot time, these udev events were ignored and the kernel did not load the brcmsmac module automatically. A patch that provides missing aliases has been applied so that the udev requests of the brcmsmac module are now handled as expected and the kernel loads the brcmsmac module automatically on boot.

BZ#1103471

Previously, KVM did not accept PCI domain (segment) number for host PCI devices, making it impossible to assign a PCI device that was a part of a non-zero PCI segment to a virtual machine. To resolve this problem, KVM has been extended to accept PCI domain number in addition to slot, device, and function numbers.

BZ#1020290

Due to a bug in the EDAC driver, the driver failed to decode and report errors on AMD family 16h processors correctly. This update incorporates a missing case statement to the code so that the EDAC driver now handles errors as expected.

BZ#1019578

Previous changes to the igb driver caused the ethtool utility to determine and display some capabilities of the Ethernet devices incorrectly. This update fixes the igb driver so that the actual link capabilities are now determined properly, and ethtool displays values as accurate as possible in dependency on the data available to the driver.

BZ#1019346

Previously, devices using the ixgbevf driver that were assigned to a virtual machine could not adjust their Jumbo MTU value automatically if the Physical Function (PF) interface was down; when the PF device was brought up, the MTU value on the related Virtual Function (VF) device was set incorrectly. This was caused by the way the communication channel between PF and VF interfaces was set up and the first negotiation attempt between PF and VF was made. To fix this problem, structural changes to the ixgbevf driver have been made so that the kernel can now negotiate the correct API between PF and VF successfully and the MTU value is now set correctly on the VF interface in this situation.

BZ#1024006

A chunk of a patch was left out when backporting a batch of patches that fixed an infinite loop problem in the LOCK operation with zero state ID during NFSv4 state ID recovery. As a consequence, the system could become unresponsive on numerous occasions. The missing chunk of the patch has been added, resolving this hang issue.

BZ#1018138

The kernel previously did not reset the kernel ring buffer if the trace clock was changed during tracing. However, the new clock source could be inconsistent with the previous clock source, and the result trace record thus could contain incomparable time stamps. To ensure that the trace record contains only comparable time stamps, the ring buffer is now reset whenever the trace clock changes.

BZ#1024548

When using Haswell HDMI audio controllers with an unaligned DMA buffer size, these audio controllers could become locked up until the next reboot for certain audio stream configurations. A patch has been applied to the Intel's High Definition Audio (HDA) driver that enforces the DMA buffer alignment setting for the Haswell HDMI audio controllers. These audio controllers now work as expected.

BZ#1024689

A previous change to the virtual file system (VFS) code included the reduction of the PATH_MAX variable by 32 bytes. However, this change was not propagated to the do_getname() function, which had a negative impact on interactions between the getname() and do_getname() functions. This update modifies do_getname() accordingly and this function now works as expected.

BZ#1028372

Previously, when removing an IPv6 address from an interface, unreachable routes related to that address were not removed from the IPv6 routing table. This happened because the IPv6 code used inappropriate function when searching for the routes. To avoid this problem, the IPv6 code has been

modified to use the ip6_route_lookup() function instead of rt6_lookup() in this situation. All related routes are now properly deleted from the routing tables when an IPv6 address is removed.

BZ#1029200

A bug in the statistics flow in the bnx2x driver caused the card's DMA Engine (DMAE) to be accessed without taking a necessary lock. As a consequence, previously queued DMAE commands could be overwritten and the Virtual Functions then could timeout on requests to their respective Physical Functions. The likelihood of triggering the bug was higher with more SR-IOV Virtual Functions configured. Overwriting of the DMAE commands could also result in other problems even without using SR-IOV. This update ensures that all flows utilizing DMAE will use the same API and the proper locking scheme is kept by all these flows.

BZ#1029203

The bnx2x driver handled unsupported TLVs received from a Virtual Function (VF) using the VF-PF channel incorrectly; when a driver of the VF sent a known but unsupported TLV command to the Physical Function, the driver of the PF did not reply. As a consequence, the VF-PF channel was left in an unstable state and the VF eventually timed out. A patch has been applied to correct the VF-PF locking scheme so that unsupported TLVs are properly handled and responded to by the PF side. Also, unsupported TLVs could previously render a mutex used to lock the VF-PF operations. The mutex then stopped protecting critical sections of the code, which could result in error messages being generated when the PF received additional TLVs from the VF. A patch has been applied that corrects the VF-PF channel locking scheme, and unsupported TLVs thus can no longer break the VF-PF lock.

BZ#1007039

When performing buffered WRITE operations from multiple processes to a single file, the NFS code previously always verified whether the lock owner information is identical for the file being accessed even though no file locks were involved. This led to performance degradation because forked child processes had to synchronize dirty data written to a disk by the parent process before writing to a file. Also, when coalescing requests into a single READ or WRITE RPC call, NFS refused the request if the lock owner information did not match for the given file even though no file locks were involved. This also caused performance degradation. A series of patches has been applied that relax relevant test conditions so that lock owner compatibility is no longer verified in the described cases, which resolves these performance issues.

BZ#1005491

Due to a previous change that altered the format of the txselect parameter, the InfiniBand qib driver was unable to support HP branded QLogic QDR InfiniBand cards in HP Blade servers. To resolve this problem, the driver's parsing routine, setup_txselect(), has been modified to handle multi-value strings.

BZ#994724

Due to a race condition that allowed a RAID array to be written to while it was being stopped, the md driver could enter a deadlock situation. The deadlock prevented buffers from being written out to the disk, and all I/O operations to the device became unresponsive. With this update, the md driver has been modified so this deadlock is now avoided.

BZ#1090423

Previously, recovery of a double-degraded RAID6 array could, under certain circumstances, result in data corruption. This could happen because the md driver was using an optimization that is safe to use only for single-degraded arrays. This update ensures that this optimization is skipped during the recovery of double-degraded RAID6 arrays.

BZ#1034348

NFS previously allowed a race between "silly rename" operations and the rmdir() function to occur when removing a directory right after an unlinked file in the directory was closed. As a result, rmdir() could fail with an EBUSY error. This update applies a patch ensuring that NFS waits for any asynchronous operations to complete before performing the rmdir() operation.

BZ#1034487

A deadlock between the state manager, kswapd daemon, and the sys_open() function could occur when the state manager was recovering from an expired state and recovery OPEN operations were being processed. To fix this problem, NFS has been modified to ignore all errors from the LAYOUTRETURN operation (a pNFS operation) except for "NFS4ERR_DELAY" in this situation.

BZ#980621

Previously, in certain environments, such as an HP BladeSystem Enclosure with several Blade servers, the kdump kernel could experience a kernel panic or become unresponsive during boot due to lack of available interrupt vectors. As a consequence, kdump failed to capture a core dump. To increase a number of available interrupt vectors, the kdump kernel can boot up with more CPUs. However, the kdump kernel always tries to boot up with the bootstrap processor (BSP), which can cause the kernel to fail to bring up more than one CPU under certain circumstances. This update introduces a new kernel parameter, disable_cpu_acipid, which allows the kdump kernel to disable BSP during boot and then to successfully boot up with multiple processors. This resolves the problem of lack of available interrupt vectors for systems with a high number of devices and ensures that kdump can now successfully capture a core dump on these systems.

BZ#1036814

The ext4_releasepage() function previously emitted an unnecessary warning message when it was passed a page with the PageChecked flag set. To avoid irrelevant warnings in the kernel log, this update removes the related WARN_ON() from the ext4 code.

BZ#960275

Previously, user space packet capturing libraries, such as libcap, had a limited possibility to determine which Berkeley Packet Filter (BPF) extensions are supported by the current kernel. This limitation had a negative effect on VLAN packet filtering that is performed by the tcpdump utility and tcpdump sometimes was not able to capture filtered packets correctly. Therefore, this update introduces a new option, SO_BPF_EXTENSIONS, which can be specified as an argument of the getsockopt() function. This option enables packet capturing tools to obtain information about which BPF extensions are supported by the current kernel. As a result, the tcpdump utility can now capture packets properly.

BZ#1081282

The RTM_NEWLINK messages can contain information about every virtual function (VF) for the given network interface (NIC) and can become very large if this information is not filtered. Previously, the kernel netlink interface allowed the getifaddr() function to process RTM_NEWLINK messages with unfiltered content. Under certain circumstances, the kernel netlink interface would omit data for the given group of NICs, causing getifaddr() to loop indefinitely being unable to return information about the affected NICs. This update resolves this problem by supplying only the RTM_NEWLINK messages with filtered content.

BZ#1040349

When booting a guest in the Hyper-V environment and enough of Programmable Interval Timer (PIT) interrupts were lost or not injected into the guest on time, the kernel panicked and the guest failed to boot. This problem has been fixed by bypassing the relevant PIT check when the guest is running

under the Hyper-V environment.

BZ#1040393

The isci driver previously triggered an erroneous BUG_ON() assertion in case of a hard reset timeout in the sci_apc_agent_link_up() function. If a SATA device was unable to restore the link in time after the reset, the isci port had to return to the "awaiting link-up" state. However in such a case, the port may not have been in the "resetting" state, causing a kernel panic. This problem has been fixed by removing that incorrect BUG_ON() assertion.

BZ#1049052

Due to several bugs in the network console logging, a race condition between the network console send operation and the driver's IRQ handler could occur, or the network console could access invalid memory content. As a consequence, the respective driver, such as vmxnet3, triggered a BUG_ON() assertion and the system terminated unexpectedly. A patch addressing these bugs has been applied so that driver's IRQs are disabled before processing the send operation and the network console now accesses the RCU-protected (read-copy update) data properly. Systems using the network console logging no longer crashes due to the aforementioned conditions.

BZ#1057704

When a network interface is running in promiscuous (PROMISC) mode, the interface may receive and process VLAN-tagged frames even though no VLAN is attached to the interface. However, the enic driver did not handle processing of the packets with the VLAN-tagged frames in PROMISC mode correctly if the frames had no VLAN group assigned, which led to various problems. To handle the VLAN-tagged frames without a VLAN group properly, the frames have to be processed by the VLAN code, and the enic driver thus no longer verifies whether the packet's VLAN group field is empty.

BZ#1058528

The dm-bufio driver did not call the blk_unplug() function to flush plugged I/O requests. Therefore, the requests submitted by dm-bufio were delayed by 3 ms, which could cause performance degradation. With this update, dm-bufio calls blk_unplug() as expected, avoiding any related performance issues.

BZ#1059943

A previous change that modified the linkat() system call introduced a mount point reference leak and a subsequent memory leak in case that a file system link operation returned the ESTALE error code. These problems have been fixed by properly freeing the old mount point reference in such a case.

BZ#1062494

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#1065304

A previous patch to the kernel scheduler fixed a kernel panic caused by a divide-by-zero bug in the init_numa_sched_groups_power() function. However, that patch introduced a regression on systems with standard Non-Uniform Memory Access (NUMA) topology so that cpu_power in all but one NUMA domains was set to twice the expected value. This resulted in incorrect task scheduling and some processors being left idle even though there were enough queued tasks to handle, which had a negative impact on system performance. This update ensures that cpu_power on systems with

standard NUMA topology is set to expected values by adding an estimate to cpu_power for every uncounted CPU.Task scheduling now works as expected on these systems without performance issues related to the said bug.

BZ#1018581

Microsoft Windows 7 KVM guests could become unresponsive during reboot because KVM did not manage to inject an Non-Maskable Interrupt (NMI) to the guest while the guest was running in user mode. To resolve this problem, a series of patches has been applied to the KVM code, ensuring that KVM handles NMIs correctly during the reboot of the guest machine.

BZ#1029381

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.

BZ#1080637

The turbostat utility produced error messages when used on systems with the fourth generation of Intel Core Processors. To fix this problem, the kernel has been updated to provide the C-state residency information for the C8, C9, and C10 C-states.

Enhancements

BZ#876275

The kernel now supports memory configurations with more than 1TB of RAM on AMD systems.

BZ#990694

Users can now set ToS, TTL, and priority values in IPv4 on per-packet basis.

BZ#1038227

Several significant enhancements to device-mapper have been introduced in Red Hat Enterprise Linux 6.6:

- The dm-cache device-mapper target, which allows fast storage devices to act as a cache for slower storage devices, has been added as a Technology Preview.
- The device-mapper-multipath ALUA priority checker no longer places the preferred path device in its own path group if there are other paths that could be used for load balancing.
- The fast_io_fail_tmo parameter in the multipath.conf file now works on iSCSI devices in addition to Fibre Channel devices.
- Better performance can now be achieved in setups with a large number of multipath devices due to an improved way in which the device-mapper multipath handles sysfs files.
- A new force_sync parameter in multipath.conf has been introduced. The parameter disables asynchronous path checks, which can help limit the number of CPU contention issues on setups with a large number of multipath devices.

BZ#922970

Support for the next generation of Intel's mobile platform has been added to Red Hat Enterprise Linux 6.6, and the relevant drivers have been updated.

BZ#922929

A future AMD processor provides a new bank of Model Specific Registers (MSRs) for L2 events which are be used for critical event types. These L2 cache performance counters are highly beneficial in performance and debugging.

BZ#1076147

The dm-crypt module has been modified to use multiple CPUs, which improves its encryption performance significantly.

BZ#1054299

The qla2xxx driver has been upgraded to version 8.05.00.03.06.5-k2, which provides a number of bug fixes over the previous version in order to correct various timeout problems with the mailbox command.

BZ#1053831

Keywords for the IPL device (ipldev) and console device (condev) on IBM System z has been enabled to ease the installation when the system uses the cio_ignore command to blacklist all devices at install time and does not have a default CCW console device number, has no devices other than the IPL device as a base to clone Linux guests, or with ramdisk based installations with no devices other than the CCW console.

BZ#872311

The cifs kernel module has been updated to handle FIPS mode cipher filtering efficiently in CIFS.

All Red Hat Enterprise Linux 6 users are advised to install these updated packages, which correct these issues, fix these bugs, and add these enhancements. The system must be rebooted for this update to take effect.

8.105. KEXEC-TOOLS

8.105.1. RHBA-2014:1502 — kexec-tools bug fix and enhancement update

Updated kexec-tools packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The kexec-tools packages contain the /sbin/kexec binary and utilities that together form the user-space component of the kernel's kexec feature. The /sbin/kexec binary facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. The kexec fastboot mechanism allows booting a Linux kernel from the context of an already running kernel.

Bug Fixes

BZ#806992

Previously, if the system had configured two or more network interfaces, where one of the devices was configured with a default gateway, and another with a static route to a private network, kdump ignored the non-default static route. As a consequence, kdump failed to dump a core file over NFS or

SSH because it did not configure the route to the private network. This bug has been fixed and now kdump successfully dumps the kernel over NFS or SSH as expected.

BZ#1061480

Previously, booting the crash kernel with more than one CPUs occasionally caused some systems to become unresponsive when the crash happened on an Application Processor (AP) and not on the Boot Strap Processor (BSP). To fix this bug, the initialization scripts were modified to include the disable_cpu_apicid kernel option automatically which acts as the BSP ID. Additionally, the user has to modify the value of the nr_cpus option to specify the number of CPUs used on the system. With this fix, the user can now successfully use the crash kernel with more than one CPUs on the system.

BZ#1128248

Due to a bug in the wait_for_multipath routine in the mkdumprd utility, kdump could fail to dump a core file on certain configurations with many multipath devices. This problem has been addressed with this update, and kdump now works as expected on systems with a large number of multipath devices.

BZ#1022871

Previously, kdump was unable to capture a core file on IBM System z machines with a DASD FBA device specified as a kdump target. This problem has been fixed by adding the necessary support for the DASD FBA type device to kdump, and a core file can now be captured as expected on the above configuration.

BZ#1122880

Due to an incorrect SELinux test condition in the mkdumprd utility, the kdump kernel could fail to load a SELinux policy and produce an unknown operand error. This update corrects the affected condition, and kdump now behaves as intended.

BZ#1122883

The mkdumprd utility could previously emit spurious warning messages about non-existent ifcfg files under certain circumstances. This problem has been fixed and kdump no longer emits these warning messages.

In addition, this update adds the following

Enhancements

BZ#929312, BZ#823561, BZ#1035156

The makedumpfile tool has been upgraded to version 1.5.6, which provides a number of bug fixes and enhancements over the previous version, including enhanced filtering and support for custom EPPIC macros in order to eliminate complex data structures, cryptographic keys, and any other specified sensitive data from dump files.

BZ#1083938

As a part of support for the kdump_fence agent in cluster environment, the new options, fence_kdump_nodes and fence_kdump_args, have been introduced to the kdump.conf file. The fence_kdump_nodes option is used to list the hosts to send notifications from the kdump_fence agent to. The fence_kdump_args is used for passing command-line arguments to the kdump_fence agent.

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

8.106. KEYUTILS

8.106.1. RHBA-2014:1610 — keyutils bug fix update

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

The keyutils packages provide utilities to control the Linux kernel key management facility and to provide a mechanism by which the kernel calls up to user space to get a key instantiated.

Bug Fix

BZ#1075652

Previously, the "keyctl show" command incorrectly displayed an abbreviated tree of nested keyrings and therefore the keyring trees that were more than two keyrings deep were not fully displayed. This bug has been fixed and "keyctl show" now displays entire keyring trees as expected.

Moreover, the "keyctl show" command did not expand the field width to show the full decimal key ID. With this update, the key ID field is expanded correctly.

Also, the maximum size of input data for the "keyctl padd" command and other pipe-in commands has been increased to 1MB.

Finally, the "keyctl padd" command as well as other pipe-in commands have been modified not to specially handle zero-value bytes in binary input.

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

8.107. KRB5

8.107.1. RHSA-2014:1389 — Moderate: krb5 security and bug fix update

Updated krb5 packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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.

Kerberos is a networked authentication system which allows clients and servers to authenticate to each other with the help of a trusted third party, the Kerberos Key Distribution Center (KDC).

Security Fixes

CVE-2013-1418, CVE-2013-6800

It was found that if a KDC served multiple realms, certain requests could cause the setup_server_realm() function to dereference a NULL pointer. A remote, unauthenticated attacker could use this flaw to crash the KDC using a specially crafted request.

CVE-2014-4344

A NULL pointer dereference flaw was found in the MIT Kerberos SPNEGO acceptor for continuation tokens. A remote, unauthenticated attacker could use this flaw to crash a GSSAPI-enabled server application.

CVE-2014-4345

A buffer overflow was found in the KADM5 administration server (kadmind) when it was used with an LDAP back end for the KDC database. A remote, authenticated attacker could potentially use this flaw to execute arbitrary code on the system running kadmind.

CVE-2014-4341, **CVE-2014-4342**

Two buffer over-read flaws were found in the way MIT Kerberos handled certain requests. A remote, unauthenticated attacker who is able to inject packets into a client or server application's GSSAPI session could use either of these flaws to crash the application.

CVE-2014-4343

A double-free flaw was found in the MIT Kerberos SPNEGO initiators. An attacker able to spoof packets to appear as though they are from an GSSAPI acceptor could use this flaw to crash a client application that uses MIT Kerberos.

Bug Fixes

BZ#922884

Previously, when connecting to a Key Distribution Center (KDC) over a Transmission Control Protocol (TCP) socket, the Kerberos client library was unable to detect cases when the server prematurely terminated the connection. Consequently, the client could stall, repeatedly attempting to read data from the closed connection's socket descriptor. This bug has been fixed, the client library now correctly detects connection failure and the processing continues as expected.

BZ#1070244

Previously, when called to accept ticket-based authentication from a client, a server was able to decrypt a ticket which was encrypted with one encryption type (for example, des-cbc-crc) as long as its keytab contained a key of a sufficiently-compatible encryption type (for example, des-cbc-md5). Due to a regression, servers became unable to verify client tickets in these cases unless the encryption types were identical. With this update, a backported fix has been introduced to restore the aforementioned behavior. As a result, servers now verify clients' tickets when the key distribution center (KDC) issues a ticket using an encryption type with sufficient compatibility.

BZ#965721

Prior to this update, on systems which were configured to use the Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) extension, issuing the "kinit -k" command to obtain credentials using keys in a keytab could fail if the "pkinit_identities" variable was set in the /etc/krb5.conf file. The problem occurred when the directive resolved to a smart card protected by a PIN or to an encrypted PEM or PKCS#12 format file. The client's PKINIT plug-in could attempt to prompt the user for a password or smart card PIN, which the kinit utility was unable to handle. Consequently, the kinit utility terminated unexpectedly with a segmentation fault. A patch has been applied, the PKINIT plug-in now checks that the invoking application provides a way to prompt for passwords and smart card PINs before attempting to prompt the user for them, and kinit no longer crashes in this scenario.

BZ#1055329

Prior to this update, the libkrb5 library sometimes attempted to free already freed memory when encrypting credentials intended for delegation. As a consequence, the calling process terminated

unexpectedly with a segmentation fault. With this update, libkrb5 frees memory correctly, which allows the credentials to be encrypted appropriately, preventing the crash.

BZ#1026721

Previously, using the ksu command without the "-n" or "-e" options caused ksu to discard the information about which principals were authorized to use it, as specified in the target user's .k5users file. Consequently, an "authorization failed" error message was displayed, even if the configuration indicated that user was authorized. This bug has been fixed and ksu no longer returns the incorrect error message in this situation.

BZ#1113652

Previously, when using Domain Name System (DNS) to locate KDCs while following referrals, if the Kerberos client library determined that it needed to locate a master KDC for a given realm along a referral path, it attempted to contact only master KDCs for any realms further along that path. As a consequence, an attempt to get credentials could fail if the client library needed to follow referrals from one realm to another and one of the realms contacted along the way did not have its master KDCs specifically named in DNS. A patch has been applied and the described problem no longer occurs.

BZ#1009389

The init script that launches the KDC runs a diagnostic helper first, attempting to diagnose a common upgrade-related error. Previously, when the default realm was configured only in the /etc/sysconfig/krb5kdc configuration file and not in the /etc/krb5.conf file, the realm was not passed to the helper. As a consequence, the attempt to start the KDC failed with an error message. With this update, the default realm set in /etc/sysconfig/krb5kdc file is correctly passed to the helper and the KDC is correctly started.

BZ#1059730

Prior to this update, when attempting to locate Kerberos servers using the DNS service location, the Kerberos client library did not correctly recognize all return codes from the resolver libraries. Consequently, the client library misinterpreted certain non-fatal return codes as fatal errors, and failed to locate any servers. A patch has been applied, the client library interprets the return codes correctly, and locating servers now works as expected.

BZ#1087068

Due to a regression, when using the Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) with multiple object identifiers (OID), the server applications did not always respond to clients using the same OID that the clients had specified. As a consequence, GSSAPI clients that attempted to use mechanisms which can be identified using more than one OID could fail to authenticate to such servers. With this update, when generating replies to clients, the GSSAPI library uses the OID specified by the client in its request, and client authentication no longer fails in this scenario.

All krb5 users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the krb5kdc daemon will be restarted automatically.

8.108. KSH

8.108.1. RHBA-2014:1381 — ksh bug fix update

Updated ksh packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

KornShell (ksh) is a Unix shell developed by AT&T Bell Laboratories, which is backward-compatible with the Bourne shell (Bash) and includes many features of the C shell. The most recent version is KSH-93. KornShell complies with the POSIX.2 standard (IEEE Std 1003.2-1992).

Bug Fixes

BZ#825520

Due to a race condition in the job list code, the ksh shell could terminate unexpectedly with a segmentation fault when the user had run custom scripts on their system. The race condition has been fixed, and ksh now works as expected when the users run custom scripts.

BZ#1117316

Due to a regression bug, a command substitution containing a pipe could return a non-zero exit code even though the command did not fail. A patch has been provided to fix this bug, and these command substitutions now return correct exit codes.

BZ#1105138

Previously, if a running function was unset by another function in a ksh script, ksh terminated unexpectedly with a segmentation fault. With this update, the ksh code skips resetting of the "running" flag if a function is unset, and ksh no longer crashes in the described scenario.

BZ#1036470

Previously, using the typeset command in a function in ksh resulted in a memory leak. This bug has been fixed and ksh no longer leaks memory when using the typeset command in a function.

BZ#1036802

Previously after upgrading ksh from version "ksh-20100621-19" to "ksh-20120801-10", the standard error output (stderr) got disconnected from the terminal, and the trace output in debug mode thus became invisible. As a consequence, the debugging of scripts on ksh was not always possible. This bug has been fixed and stderr now provides the correct output.

BZ#1066589

Previously, a substitution command failed to execute in ksh if the standard input (stdin), the standard output (stdout), or standard error (stderr) were closed in a certain manner. As a consequence, reading a file using command substitution did not work correctly and the substituted text failed to display under some circumstances. A patch has been applied to address this bug, and command substitution now works as expected.

BZ#1112306

Prior to this update, the compiler optimization dropped parts of the ksh job locking mechanism from the binary code. As a consequence, ksh could terminate unexpectedly with a segmentation fault after it received the SIGCHLD signal. This update ensures that the compiler does not drop parts of the ksh job locking mechanism and ksh works as expected.

BZ#1062296

When running a command that output a lot of data, and then setting a variable from that output, the ksh could become unresponsive. To fix this problem, the combination of I/O redirection and synchronization mechanism has been changed. Now, ksh no longer hangs in this case and commands with large data output complete successfully.

BZ#1036931

Previously, the ksh syntax analyzer did not parse command substitutions inside of here-documents correctly, which led to syntax error messages being reported on the syntactically correct code. A patch has been provided to fix this bug, and ksh now interprets substitutes as intended.

BZ#1116508

Previously, ksh could skip setting of an exit code from the last command of a function. As a result, the function could sometimes return a wrong exit code. This update ensures that ksh always uses the exit code from the last command of a function, and functions in ksh now return the correct exit codes as expected.

BZ#1070350

When rounding off a number smaller than 1, ksh incorrectly truncated too many decimals. As a consequence, numbers from the interval between 0.5 and 0.999 were incorrectly rounded to zero. This updated version of ksh ensures that all numbers are now rounded off correctly.

BZ#1078698

Previously, ksh did not handle the brace expansion option correctly and ignored it in most cases. As a result, it was not possible to turn the brace expansion off and braces in file names had to be always escaped to prevent their expansion. The brace expansion code has been updated to take no action when the brace expansion option is turned off, and brace expansion in ksh can now be turned off and on as needed.

BZ#1133582

Previously, ksh did not handle the reuse of low file descriptor numbers when they were not used for the standard input, output, or error output. As a consequence, when any of stdin, stdout, or stderr was closed and its file descriptor was reused in command substitution, the output from that substitution was empty. With this update, ksh has been updated to no longer reuse "low file descriptors" for command substitution. Command substitution in ksh now works correctly even if any of stdin, stdout or stderr is closed.

BZ#1075635

Previously, ksh did not mask exit codes and sometimes returned a number that was too high and could be later interpreted as termination by a signal. Consequently, if ksh was started from the "su" utility and it exited with a high-number exit code, "su" incorrectly generated a core dump. To prevent confusion of a parent process, ksh has been updated to mask exit codes when terminating.

BZ#1047506

Previously, after forking a process, ksh did not clear the argument list of the process properly. Consequently, when listing processes using the ps tool, the arguments field of the forked process could contain some old arguments. The code has been modified to always clear the unused space of the argument string, and the ps tool now prints correct arguments.

BZ#1102627

Previously, ksh did not verify whether it had the execute permission for a given directory before attempting to change into it. Consequently, ksh always assumed it was operating inside that directory, even though the attempt to access the directory was in fact unsuccessful. With this update, ksh checks for the execute permission and reports an error as expected if the permission is missing.

BZ#1023109

Ksh could set a wrong process group when running a script in monitor mode. As a consequence,

when such a script attempted to read an input, the ksh process stopped the script. With this update, ksh has been fixed to use the correct process group and the script executes as expected in the described scenario.

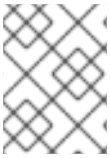
Users of ksh are advised to upgrade to these updated packages, which fix these bugs.

8.109. LEDMON

8.109.1. RHBA-2014:1614 — 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 utilities are user-space applications designed to control LEDs associated with each slot in an enclosure or a drive bay. There are two types of systems: 2-LED system (Activity LED, Status LED) and 3-LED system (Activity LED, Locate LED, Fail LED). Users must have root privileges to use this application.



NOTE

The ledmon packages have been upgraded to upstream version 0.79, which provides a number of bug fixes and enhancements over the previous version. (BZ#1030622)

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

8.110. LESS

8.110.1. RHBA-2014:0755 — less bug fix update

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

The "less" utility is a text file browser that resembles "more", but allows users to move backwards in the file as well as forwards. Since "less" does not read the entire input file at startup, it also starts more quickly than ordinary text editors.

Bug Fix

BZ#615303

Previously, the lesspipe script returned incorrect exit status codes. As a consequence, the less utility failed to decompress empty files that had been compressed with the gzip utility, and an unwanted message was displayed. With this update, a pipe character ("|") has been added in front of the LESSOPEN environment variable to enforce a new default behavior of lesspipe. For backward compatibility, lesspipe has the same behavior if LESSOPEN remains unchanged. As a result, the less utility now detects and displays empty files correctly.

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

8.111. LIBCGROUP

8.111.1. RHBA-2014:1480 — 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 manage and monitor control groups.

Bug Fixes

BZ#1022842

Previously, the cgset command failed to assign value to multiple subsystem parameters at once. This behavior occurred only when using the -r option more than once to tune parameters of a single subsystem. Configuring different subsystems simultaneously worked correctly. This bug has been fixed, and cgset can now set multiple parameters of a single subsystem without complications.

BZ#1028773

Previous libcgroup update introduced an unnecessary dependency on the redhat-lsb-core package. The redhat-lsb-core package subsequently pulled in a large number of other packages, which could cause problems on hardware with limited storage. With this update, the unnecessary dependency on the redhat-lsb-core package has been removed, and thus no unneeded packages are installed on system.

BZ#1057676

Prior to this update, the /src/config.c file contained the incorrectly specified cgroup_copy_cgroup() function. Consequently, certain user-specific resource limits set in the /etc/cgconfig.conf configuration file were not applied. This update fixes the syntax of the aforementioned function in /src/config.c. As a result, all settings in /etc/cgconfig.conf are applied as expected.

BZ#1060227

Previously applied patch that aimed to increase the performance of the pam_cgroup module contained a bug. Consequently, pam_cgroup failed to start and it did not produce an error message. With this update, the aforementioned patch has been reverted, and pam_cgroup now works as expected.

BZ#1080281

The cgset utility did not process all memory subsystem parameters passed to the --copy-from command-line option correctly. Consequently, these control group parameters were not transferred successfully and no warning message was issued. With this update, cgset has been modified to correctly process parameters of memory subsystem passed to --copy-from option, thus fixing this bug.

In addition, this update adds the following

Enhancement

BZ#1058363

This update adds the /etc/cgconfig.d/ hierarchy designed to store configuration files applicable to various services.

Users of libcgroup are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

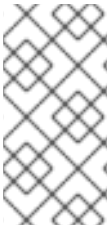
8.112. LIBGUESTFS

8.112.1. RHBA-2014:1458 — libguestfs bug fix update

Updated libguestfs packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The libguestfs packages contain a library, which is used for accessing and modifying virtual machine (VM) disk images.

This update also fixes the following bugs:



NOTE

The virt-sysprep packages have been upgraded to upstream version 1.24.6, which provides a number of enhancements over the previous version, namely new features such as removing unnecessary files, including the possibility to specify custom paths, and setting user passwords. (BZ#1037166)

This update also fixes the following bugs:

Bug Fixes

BZ#624335

The blockdev_setbsz API has been deprecated as the underlying implementation ("blockdev --setbsz") is no longer considered useful.

BZ#965495

Prior to this update, the gdisk utility was not available as a dependency on the libguestfs library. Consequently, gdisk was not available, and thus guestfs_part_get_gpt_type and guestfs_part_set_gpt_type APIs were not usable. This update adds gdisk as a dependency, and thus is now available as well as the aforementioned APIs.

BZ#982979

Due to the fstrim feature marked as available, calling the fstrim API returned errors. As fstrim does not work with both the kernel and QEMU available in Red Hat Enterprise Linux 6, this update disables fstrim. Now, calling the fstrim API reports that fstrim is no longer available.

BZ#1056558

Previously, when the virt-sparsify utility was run with a block or character device as output, the output device was overwritten by a file, or deleted. To fix this bug, if a block or character device is specified as output, virt-sparsify refuses to run.

BZ#1072062

Due to wrong implementation of the Guestfs.new() constructor in the Ruby binding, creating a new Guestfs instance often resulted in an error. With this update, the implementation of Guestfs.new() has been rewritten, and Guestfs.new now works correctly.

BZ#1091805

When running the tar-in guestfish command, or using the tar_in guestfs API, with a non-existing input tar or to a non-existing destination directory, the libguestfs appliance terminated unexpectedly. The error checking has been approved, and the tar-in now cleanly returns an error.

BZ#1056558

Previously, the virt-sparsify utility did not check for free space available in the temporary directory. Consequently, virt-sparsify became unresponsive if the temporary directory lacked enough free space. With this update, virt-sparsify checks by default for available space before the sparsification operation, and virt-sparsify now works as intended.

BZ#1106548

Previously, particular permission checks for the root user in the FUSE layer of the libguestfs library were missing. Consequently, mounting a disk image using guestmount and accessing a directory as root with permissions 700 and not owned by root failed with the "permission denied" error. With this update, permissions have been disabled, and root can now access any directory of a disk image mounted using guestmount.

BZ#1123794

The previous version of libguestfs library was not closing all the open file descriptors when forking subprocesses such as QEMU. Consequently, if the parent process or any non-libguestfs library did not atomically set the O_CLOEXEC flag on file descriptors, the parent process leaked into QEMU, In OpenStack, this bug also caused deadlocks, because Python 2 is unable to set O_CLOEXEC atomically. With this update, libguestfs closes all the file descriptors before executing QEMU, and deadlocks no longer occur.

BZ#1079182

Previously, the libguestfs library was skipping partitions with type 0x42, Windows Lightweight Device Mounter (LDM) volumes, when LDM was not available. Consequently, simple LDM volumes mountable as a single partition were ignored. With this update, the partition detection is not skipped if LDM is missing, and simple LDM volumes can now be recognized and mounted as plain NTFS partitions.

The virt-sysprep packages have been upgraded to upstream version 1.24.6, which provides a number of enhancements over the previous version, namely new features such as removing unnecessary files, including the possibility to specify custom paths, and setting user passwords. (BZ#1037166)

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

8.113. LIBHUGETLBFS

8.113.1. RHBA-2014:1485 — libhugetlbfs bug fix and enhancement update

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

The libhugetlbfs library interacts with the Linux Huge TLB file system to make large pages available to applications in a transparent manner.

NOTE

The libhugetlbfs packages have been upgraded to upstream version 2.16.0, which provides a number of bug fixes and enhancements over the previous version, including support for the IBM System z architecture. (BZ#823006)

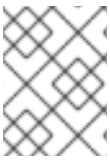
Users of libhugetlbfs are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

8.114. LIBICA

8.114.1. RHBA-2014:1497 — libica bug fix and enhancement update

Updated libica packages that fix several bugs and add various enhancements 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.



NOTE

The libica packages have been upgraded to upstream version 2.3.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#1053842)

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

8.115. LIBNL3

8.115.1. RHEA-2014:1532 — libnl3 enhancement update

Updated libnl3 packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The libnl packages contain a convenience library to simplify using the Linux kernel's Netlink sockets interface for network manipulation.

Enhancement

BZ#1052119

The libnl3 packages have been introduced into Red Hat Enterprise Linux 6, which allows for improved functionality of the oVirt application. In addition, this ensures compatibility with other future applications, since the previous version of the Netlink protocol library, libnl1, is no longer being developed.

Users of libnl3 are advised to upgrade to these updated packages, which add this enhancement.

8.116. LIBPROXY

8.116.1. RHBA-2014:1556 — libproxy bug fix update

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

The libproxy library handles all the details of proxy configuration. It provides a stable external API, dynamic adjustment to changing network topology, small core footprint, without external dependencies within libproxy core (though libproxy plug-ins may have dependencies).

Bug Fixes

BZ#802765

Previously, the libproxy utility attempted to locate the /etc/proxy.conf file from the current working directory. Consequently, the configuration file was not always found. This bug has been fixed and libproxy now locates /etc/proxy.conf as expected.

BZ#874492

A flaw was found in the way libproxy handled the downloading of proxy auto-configuration (PAC) files. Consequently, programs using libproxy terminated unexpectedly with a segmentation fault when processing PAC files that contained syntax errors. With this update, the handling of PAC files has been fixed in libproxy, thus preventing the segmentation fault.

BZ#979356

Due to a bug in the libproxy packages, the "reporter-upload" command used by Automatic Bug Reporting Tool terminated unexpectedly if given an "scp" URL that did not contain a password. This bug has been fixed, and reporter-upload no longer crashes in the aforementioned scenario.

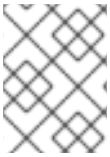
Users of libproxy are advised to upgrade to these updated packages, which fix these bugs.

8.117. LIBRELP

8.117.1. RHBA-2014:1505 — librelp bug fix and enhancement update

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

Librelp is an easy-to-use library for the RELP protocol. RELP (stands for Reliable Event Logging Protocol) is a general-purpose, extensible logging protocol.



NOTE

The librelp packages have been upgraded to upstream version 1.2.7, which provides a number of bug fixes and enhancements over the previous version. (BZ#966974)

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

8.118. LIBREOFFICE

8.118.1. RHBA-2014:1423 — libreoffice bug fix update

Updated libreoffice packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

LibreOffice is an open source, community-developed office productivity suite. It includes key desktop applications, such as a word processor, a spreadsheet, a presentation manager, a formula editor, and a drawing program. LibreOffice replaces OpenOffice and provides a similar but enhanced and extended office suite.

Bug Fixes

BZ#1012379

Previously, after including an audio file in a LibreOffice Impress presentation, this file was displayed as a gray square. With this update, an upstream patch has been backported to fix this bug. As a result, audio files are no longer displayed as a gray square in Impress presentations.

BZ#1012390

Prior to this update, when including an audio or video file to a LibreOffice Impress presentation, a message informing about a failed " rxAccessible.get() != NULL" assertion was displayed. Apart from this message, the file was imported correctly and the LibreOffice Impress application worked as expected. An upstream patch has been backported to correct this behavior, and the aforementioned message is no longer displayed.

BZ#1020712

Previously, when typing into a text box in a LibreOffice Impress presentation using any Indic locale, the text was not displayed until pressing the Backspace key. This bug has been fixed, and Indic fonts are now displayed immediately as the text is inserted.

BZ#1021915

For certain Indic locales, such as Odia, the drop-down lists from the main bar overlapped with the main menu bar, which restricted navigating LibreOffice applications. This bug has been fixed, and the aforementioned problem no longer occurs.

BZ#1035298

In a previous release of Red Hat Enterprise Linux 6, the libreoffice packages no longer obsoleted the openoffice packages, which created several conflicts when trying to download both sets of packages. With this update, libreoffice has been modified to obsolete openoffice again, thus preventing the conflicts.

BZ#1038189

Prior to this update, LibreOffice applications did not automatically recognize new printers created on a local print server while LibreOffice was running. With this update, the libreoffice packages have been modified, and now it is possible to work around this problem. To do so, open the "Printer settings" dialog window, and than close it. This operation refreshes the list of available printers.

BZ#1065629

Previously, LibreOffice applications did not correctly render imported RTF files written in a non-English language. An upstream patch has been backported to fix this bug.

BZ#1085420

Previously, the libreoffice packages incorrectly provided the liblcms2.so.2 package. With this update, libreoffice has been modified to provide the correct set of packages.

BZ#1097646

Previously, LibreOffice applications did not correctly handle multiple UNO connections. Consequently, LibreOffice terminated unexpectedly when multiple Univarsal Network Object (UNO) connections were open. With this update, an upstream patch has been backported to fix this bug. As a result, LibreOffice no longer crashes when more UNO connections are open.

BZ#1131428

Previously, LibreOffice applications failed to export charts to SVG format. Attempting to do so resulted in an empty SVG file. This bug has been fixed, and charts are now exported correctly from LibreOffice applications.

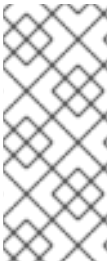
Users of libreoffice are advised to upgrade to these updated packages, which fix these bugs.

8.119. LIBRTAS

8.119.1. RHBA-2014:1427 — librtas bug fix and enhancement update

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

The librtas packages contain a set of libraries that allow access to the Run-Time Abstraction Services (RTAS) on 64-bit PowerPC architectures. The librtasevent library contains definitions and routines for analyzing RTAS events.



NOTE

The librtas packages have been upgraded to upstream version 1.3.10, which provides a number of bug fixes and enhancements over the previous version. Notably, this update adds RTAS support for PCI hot plug support on POWERPC 8 systems and improves support for RTAS Event parsing on little-endian POWERPC systems. In addition, the librtasevent library is now able to analyze hot plug events. (BZ#1073037)

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

8.120. LIBSELINUX

8.120.1. RHBA-2014:1469 — libselinux bug fix update

Updated libselinux packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The libselinux packages contain the core library of an SELinux system. The libselinux library provides an API for SELinux applications to get and set process and file security contexts, and to obtain security policy decisions. It is required for any applications that use the SELinux API, and used by all applications that are SELinux-aware.

Bug Fixes

BZ#753675

When attempting to run the virt-manager utility over SSH X11 forwarding, SELinux prevented the D-Bus system from performing actions even if SELinux was in permissive mode. As a consequence, such attempts failed and an AVC denial message was logged. With this update, a patch has been provided to fix this bug, and SELinux in permissive mode no longer blocks D-Bus in the described scenario.

BZ#1011109

Prior to this update, the selinux(8) manual page contained outdated information. This manual page has been updated, and SELinux is now documented correctly.

BZ#1025507

The Name Server Caching Daemon (nscd) uses SELinux permissions to check if a connecting user is allowed to query the cache. However, two permissions, NSCD__GETNETGRP and NSCD__SHMEMNETGRP, were missing from the SELinux list of permissions. Consequently, the netgroup caching worked only when SELinux was running in permissive mode. The missing permissions have been added to the list, and the netgroup caching now works as expected.

BZ#1091857

Previously, the matchpathcon utility did not handle non-existent files or directories properly; the "matchpathcon -V" command verified the files of directories instead of specifying that they did not exist. The underlying source code has been modified to fix this bug, and matchpathcon now correctly recognizes non-existent files or directories. As a result, an error message is returned when a file or directory do not exist.

BZ#1096816

It was not possible to add a new user inside a Docker container because SELinux in enforcing or permissive mode incorrectly blocked an attempt to modify the /etc/passwd file. With this update, when the /selinux/ or /sys/fs/selinux/ directories are mounted as read-only, the libselinux library acts as if SELinux is disabled. This behavior stops SELinux-aware applications from attempting to perform SELinux actions inside a container, and /etc/passwd can now be modified as expected.

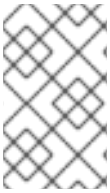
Users of libselinux are advised to upgrade to these updated packages, which fix these bugs.

8.121. LIBSERVICELOG

8.121.1. RHBA-2014:1430 — libservicelog bug fix and enhancement update

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

The libservicelog packages provide a library for logging service-related events to the servicelog database, and a number of command-line utilities for viewing the contents of the database.



NOTE

The libservicelog packages have been upgraded to upstream version 1.1.13, which provides a number of bug fixes and enhancements over the previous version, including support for SQL insert command input string. (BZ#739120)

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

8.122. LIBSOUP

8.122.1. RHBA-2014:1561 — libsoup bug fix and enhancement update

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

The libsoup packages provide an HTTP client and server library for GNOME.

NOTE

The libsoup packages have been upgraded to upstream version 2.34.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#869322, BZ#1101399)

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

8.123. LIBTIRPC

8.123.1. RHBA-2014:1419 — libtirpc bug fix update

Updated libtirpc packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The libtirpc packages contain SunLib's implementation of transport independent RPC (TI-RPC) documentation. This includes a library required by programs in the nfs-utils and rpcbind packages.

Bug Fixes

BZ#1082807

Previously, the libtirpc library included the authgss_get_private_data() system call, but not the authgss_free_private_data() system call. As a consequence, private data were obtained but not freed afterwards. This caused the authgss_destroy_context() call to send an incorrect RPCSEC_GSS_DESTROY request, and the client was in turn not able to clear the state data on the server. With this update, authgss_free_private_data() has been added to libtirpc, and the data is now freed correctly. As a result, the client can now reset the server state as expected.

BZ#1031498

Prior to this update, due to race conditions, using TI-RPC in the glibc library caused TI-RPC to terminate unexpectedly with a segmentation fault on some file operations, such as fclose() call and the endnetconfig() call. This update prevents the race conditions from occurring in the above scenario, and TI-RPC thus no longer crashes when used in glibc.

BZ#1056809

Due to buffer overruns in libtrpc, the rpcbind utility sometimes terminated unexpectedly with a segmentation fault. With this update, buffer is allocated by the svcauth_gss_validate() call, which avoids the buffer overruns and thus prevents the rpcbind crashes.

BZ#869397

Previously, the libtirpc-devel RPM incorrectly installed the /lib64/libtirpc.a and /lib64/libtirpc.la static libraries, which caused compiling software that linked libtirpc to fail. This update removes libtirpc.a and libtirpc.la and compiling with libtirpc.so now works as expected.

BZ#982064

Due to a code error in libtirpc, the automount utility sometimes terminated unexpectedly with a segmentation fault when a RPC was rejected with an invalid rejection status. This update fixes this bug and automount no longer crashes when receiving an invalid server rejection.

Users of libtirpc are advised to upgrade to these updated packages, which fix these bugs.

8.124. LIBVIRT

8.124.1. RHBA-2014:1374 — libvirt bug fix and enhancement update

Updated libvirt packages that fix numerous bugs and add various enhancements 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#1117177

Previously, the logic behind using the **`virsh`** command with the **`--config`** option, which handles the virtual domain configuration, was incorrect. Consequently, block devices were attached to both the domain configuration and the running domain. Both the handling logic and relevant technical documentation have been fixed, and **`virsh`** with **`--config`** now behaves correctly, attaching the block device to the domain configuration only.

BZ#999454

Prior to this update, the **libvirt** Python bindings for querying block job status could not distinguish between returning an error and no status available. As a consequence, the code that was polling for the completion of a block job had to deal with a Python exception, and could not distinguish it from an actual error. With this update, the bindings now successfully determine if there is no job and return an empty dictionary when that is the case. As a result, the bindings can be used more reliably when managing block jobs.

BZ#1078589

A previous update introduced an error where a **`SIG_SETMASK`** argument was incorrectly replaced by a **`SIG_BLOCK`** argument after the **`poll()`** system call. Consequently, the **`SIGCHLD`** signal could be permanently blocked, which caused signal masks not to return to their original values and defunct processes to be generated. With this update, the original signal masks are restored as intended, and **`poll()`** now functions correctly.

BZ#1066473

When hot unplugging a virtual CPU (vCPU) from a guest using libvirt, the current Red Hat Enterprise Linux **QEMU** implementation does not remove the corresponding vCPU thread. Consequently, **libvirt** did not detect the vCPU count correctly after a vCPU was hot unplugged, and it was not possible to hot plug a vCPU after a hot unplug. In this update, information from **QEMU** is used to filter out inactive vCPU threads of disabled vCPUs, which allows libvirt to perform the hot plug.

BZ#1076719

Prior to this update, the condition that checks whether **QEMU** successfully attached a new disk to a guest contained a typographical error. Due to the error, the **`libvirtd`** daemon terminated unexpectedly if the monitor command was unsuccessful: for example, when a virtual machine failed or when attaching a guest disk drive was interrupted. In this update, the error has been corrected, and **`libvirtd`** no longer crashes in the described circumstances.

BZ#1126393

The **libvirt** library has limits on Remote Procedure Call (RPC) messages to prevent Denial of Service

(DoS) attacks. Previously, however, the domain XML file could fail this limit test when it was encoded into an RPC message and sent to the target machine during migration. As a consequence, the migration failed even though the domain XML format was valid. To fix this bug, the RPC message limits have been increased, and the migration now succeeds, while **libvirt** stays resistant to DoS attacks.

BZ#1113828

Due to a regression caused by a prior bug fix, attempting to perform a block copy while another block copy was already in progress could cause **libvirt** to reset the information about the block copy in progress. As a consequence, **libvirt** failed to recognize if the copied file format was raw, and performed a redundant format probe on the guest disk. This update fixes the regression and **libvirt** no longer performs incorrect format probes.

BZ#947974

The UUID (Universally Unique Identifier) is a string of characters which represents the virtual guest. Displaying the UUID on a screen requires correct APIs to present the strings in a user-readable format. Previously, printing unformatted UUID data caused exceptions or incorrectly formatted output. For Python scripts, exceptions that were not handled could cause unexpected failures. For other logging methods or visual displays, the characters in the output were jumbled. With this update, the UUID strings are properly formatted and printing them no longer causes unexpected exceptions or jumbled characters on output.

BZ#1011906

When receiving NUMA (Non-Uniform Memory Access) placement advice, the current memory was used for the **`amount`** parameter. As a consequence, domain placement was not as precise as it could have been if the current memory changed for the live domain. With this update, the advice is queried with the maximum memory as the **`amount`** parameter, and the advised placement now fixes the domain even when the current memory changes for the live domain.

BZ#807023

Previously, **libvirt** reported success of the **`device_del`** command even when the device was not successfully detached. With this update, **libvirt** always verifies whether **`device_del`** succeeded, and when the command fails, **libvirt** reports it accordingly.

BZ#977706

Prior to this update, using the **`virsh pool-refresh`** command incorrectly caused **libvirt** to remove a storage pool if a storage volume was removed while the command was being processed. As a consequence, the storage pool became inactive, even though the NFS directory was mounted. With this update, refreshing a storage pool no longer removes a volume from it. As a result, **libvirt** does not cause the storage pool to become inactive.

Enhancements

BZ#1033984

A new **`pvpanic`** virtual device can now be attached to the virtualization stack and a guest panic can cause **libvirt** to send a notification event to management applications.

BZ#1100381

This update adds support for the following Broadwell microarchitecture processors' instructions: ADCX, ADOX, RDSEED, and PREFETCHW. This improves the overall performance of **KVM**.

Users of libvirt are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. After installing the updated packages, **libvirtd** will be restarted automatically.

8.125. LIBVIRT-CIM

8.125.1. RHBA-2014:1581 — libvirt-cim bug fix update

Updated libvirt-cim packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The libvirt-cim packages provide a Common Manageability Programming Interface (CMPI) CIM provider that implements the Distributed Management Task Force (DMTF) System Virtualization, Partitioning and Clustering (SVPC) virtualization model. These packages support most of the features of libvirt and enable management of multiple platforms with a single provider.

Bug Fixes

BZ#1010283

Due to incorrect string parsing, an attempt to access a store pool that contained a space in its name failed unexpectedly. This update provides a patch to fix this bug and such store pools can now be accessed as expected.

BZ#1046280

Prior to this update, the libvirt-cim provider did not allow customization of the "machine" and "arch" properties for the "type" attribute of the "os" element for the domain XML file. As a consequence, a default value was provided, overwriting a possible customization for libvirt-cim. To fix this bug, the code has been adjusted to allow modifications of the "machine" and "arch" properties of the "type" attribute for the "os" element. As a result, it is now possible to set the fields as desired using the "ModifySystemSettings" method and adjusting the "SystemSettings" values for the KVM_VirtualSystemSettingData "machine" field.

BZ#1119165

Previously, an incorrect variable was used when overwriting certain tags in domain XML files. Consequently, settings for the dumpCore attribute were ignored. With this update, a patch has been provided to fix this bug and the attribute is no longer ignored in the described scenario. In addition, the libvirt-cim provider now supports the dumpCore feature.

Users of libvirt-cim are advised to upgrade to these updated packages, which fix these bugs.

8.126. LIBVISUAL

8.126.1. RHBA-2014:0840 — libvisual bug fix update

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

Libvisual is an abstraction library that comes between applications and audio visualization plug-ins and provides a convenient API to enable the user to draw visualizations easily.

Bug Fix

BZ#658064

Previously, due to multilib file conflicts between certain packages in the Optional repository on Red

Hat Network, those packages could not have copies for both the primary and secondary architecture installed on the same machine. As a consequence, installation of the packages failed. A patch has been applied to resolve the file conflicts, and the packages can now be installed as expected in the described scenario.

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

8.127. LIBVPD

8.127.1. RHEA-2014:1429 — libvpd enhancement update

Updated libvpd packages that add various enhancements are now available for Red Hat Enterprise Linux 6.

The libvpd packages contain the classes that are used to access Vital Product Data (VPD) created by vpdupdate in the lsvpd package.

NOTE

The libvpd packages have been upgraded to upstream version 2.2.3, which provides a number of enhancements over the previous version. Specifically, the updated libvpd packages prevent segmentation faults from occurring when fetching the corrupted Vital Product Data (VPD) database. In addition, support for vpdupdate command automation has been added for cases of changes happening to device configuration on run time. During hot plugs, the changes made to the device configuration are now caught by an udev rule and are handled by libvpd correctly. (BZ#739122)

Users of libvpd are advised to upgrade to these updated packages, which add these enhancements.

8.128. LINUXPTP

8.128.1. RHBA-2014:1491 — linuxptp bug fix and enhancement update

Updated linuxptp packages that fix several bugs and add various enhancements are now available 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.

The notable bug fixes and enhancements are:

* The ptp4l application can be configured to select the delay mechanism automatically. However, this configuration did not work with the P2P delay mechanism so that the delay timer was not reset and the utility did not make any peer delay measurements. This update provides a patch to address this bug and ptp4l now correctly measures the peer delay in the described scenario. (BZ#1011022)

* Previously, the measured network delay was processed with a moving average algorithm, which is sensitive to outliers. This could for example negatively affect the time of recovery from an external clock step. This update adds a support for median filtering of the measured path delay. As a result, the

algorithm that is used to process the measured delay can now be configured. The median filter, which is less sensitive to outliers, is set by default. (BZ#1016356)

* When the phc2sys utility is used with a Pulse Per Second (PPS) device and the corresponding network interface or Precision Time Protocol (PTP) clock is not specified with the "-i" or "-s" option, the user has to enable the device manually by running the "echo 1 > /sys/class/ptp/ptp0/pps_enable" command before phc2sys starts. When the device is not enabled before phc2sys starts, the "failed to fetch PPS: Connection timed out" error is returned. However, this requirement was not properly documented, which could confuse the users. With this update, this information has been added to the phc2sys(8) manual page. (BZ#1019121)

In addition, this update adds the linuxptp packages to the PowerPC version of Red Hat Enterprise Linux 6. (BZ#1095400)

NOTE

The linuxptp packages have been upgraded to upstream version 1.4, which provides a number of bug fixes and enhancements over the previous version. (BZ#1067502)

The notable bug fixes and enhancements are:

* The ptp4l application can be configured to select the delay mechanism automatically. However, this configuration did not work with the P2P delay mechanism so that the delay timer was not reset and the utility did not make any peer delay measurements. This update provides a patch to address this bug and ptp4l now correctly measures the peer delay in the described scenario. (BZ#1011022)

* Previously, the measured network delay was processed with a moving average algorithm, which is sensitive to outliers. This could for example negatively affect the time of recovery from an external clock step. This update adds a support for median filtering of the measured path delay. As a result, the algorithm that is used to process the measured delay can now be configured. The median filter, which is less sensitive to outliers, is set by default. (BZ#1016356)

* When the phc2sys utility is used with a Pulse Per Second (PPS) device and the corresponding network interface or Precision Time Protocol (PTP) clock is not specified with the "-i" or "-s" option, the user has to enable the device manually by running the "echo 1 > /sys/class/ptp/ptp0/pps_enable" command before phc2sys starts. When the device is not enabled before phc2sys starts, the "failed to fetch PPS: Connection timed out" error is returned. However, this requirement was not properly documented, which could confuse the users. With this update, this information has been added to the phc2sys(8) manual page. (BZ#1019121)

In addition, this update adds the linuxptp packages to the PowerPC version of Red Hat Enterprise Linux 6. (BZ#1095400)

Bug Fixes

BZ#1011022

The ptp4l application can be configured to select the delay mechanism automatically. However, this configuration did not work with the P2P delay mechanism so that the delay timer was not reset and the utility did not make any peer delay measurements. This update provides a patch to address this bug and ptp4l now correctly measures the peer delay in the described scenario.

BZ#1016356

Previously, the measured network delay was processed with a moving average algorithm, which is sensitive to outliers. This could for example negatively affect the time of recovery from an external

clock step. This update adds a support for median filtering of the measured path delay. As a result, the algorithm that is used to process the measured delay can now be configured. The median filter, which is less sensitive to outliers, is set by default.

BZ#1019121

When the phc2sys utility is used with a Pulse Per Second (PPS) device and the corresponding network interface or Precision Time Protocol (PTP) clock is not specified with the "-i" or "-s" option, the user has to enable the device manually by running the "echo 1 > /sys/class/ptp/ptp0/pps_enable" command before phc2sys starts. When the device is not enabled before phc2sys starts, the "failed to fetch PPS: Connection timed out" error is returned. However, this requirement was not properly documented, which could confuse the users. With this update, this information has been added to the phc2sys(8) manual page.

The linuxptp packages have been upgraded to upstream version 1.4, which provides a number of bug fixes and enhancements over the previous version. (BZ#1067502)

The notable bug fixes and enhancements are:

In addition, this update adds the linuxptp packages to the PowerPC version of Red Hat Enterprise Linux 6. (BZ#1095400)

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

8.129. LSVPD

8.129.1. RHBA-2014:1442 — lsvpd bug fix and enhancement update

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

The lsvpd packages provide a set of tools to gather and display the Vital Product Data (VPD) information about hardware components. This information can be used by higher-level serviceability tools.

This update also fixes the following bugs:

NOTE

The lsvpd packages has been upgraded to upstream version 1.7.4, which provides a number of bug fixes and enhancements over the previous version. (BZ#739121)

This update also fixes the following bugs:

Bug Fixes

BZ#868757

Previously, the output from the lscfg command contained duplicate entries for various hardware components. This bug has been fixed and lscfg no longer returns duplicate entries.

BZ#1088401

Previously, it was not possible to link code between the libsvpd and librtas libraries, because libsvpd is distributed under the GNU General Public License (GPL) whereas librtas is under commercial

public license (CPL). This update grants a special permission to link part of the code for libsvpd against the librtas library and distribute linked combinations which include both libraries. You must obey the GNU General Public License in all respects for all of the code used other than librtas.

The lsvpd packages has been upgraded to upstream version 1.7.4, which provides a number of bug fixes and enhancements over the previous version. (BZ#739121)

In addition, this update adds the following

Enhancement

BZ#1006855

This update adds support for the Firmware Entitlement Checking on IBM PowerPC server systems.

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

8.130. LTRACE

8.130.1. RHBA-2014:1604 — ltrace bug fix update

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

The ltrace utility is a debugging program that runs a specified command until the command exits. While the command is executing, ltrace intercepts and records both the dynamic library calls called by the executed process and the signals received by the executed process. The ltrace utility can also intercept and print system calls executed by the process.

Bug Fixes

BZ#868280

Previously, the ltrace utility did not support the Position Independent Executables (PIE) binaries, which are linked similarly to shared libraries, and processes. Consequently, addresses found in images of those binaries needed additional adjustment for the actual address where the binary was loaded during the process startup. With this update, the support for the PIE binaries and processes has been added and ltrace now handles the additional processing for the PIE binaries correctly.

BZ#891607

When copying internal structures after cloning a process, the ltrace utility did not copy a string containing a path to an executable properly. This behavior led to errors in heap management and could cause ltrace to terminate unexpectedly. The underlying source code has been modified and ltrace now copies memory when cloning traced processes correctly.

Users of ltrace are advised to upgrade to these updated packages, which fix these bugs.

8.131. LUCI

8.131.1. RHSA-2014:1390 — Moderate: luci security, bug fix, and enhancement update

Updated luci 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. 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.

Luci is a web-based high availability administration application.

Security Fix

CVE-2014-3593

It was discovered that **luci** used **`eval()`** on inputs containing strings from the cluster configuration file when generating its web pages. An attacker with privileges to create or edit the cluster configuration could use this flaw to execute arbitrary code as the **luci** user on a host running **luci**.

This issue was discovered by Jan Pokorný of Red Hat.

Bug Fixes

BZ#855112

Previously, it was possible to use the following characters in the **luci** configuration file inside attribute values:

- the less-than sign (<)
- the greater-than sign (>)
- the quotation mark (")

Using such characters inside the attribute values could cause several problems. With this update, when the user attempts to use these special characters inside the attribute value, a warning is returned.

BZ#917738

The ***`prefer_interface`*** parameter was missing from the IP resource in the **`luci`** application. This parameter is used for adding an IP address to a particular network interface if a cluster node has multiple active interfaces that have IP addresses on the same subnetwork. The missing parameter has been added to **luci** with this update.

BZ#917771

Previously, the **`max_messages`**, **`netmtu`**, **`seqno_unchanged_const`**, and **`window_size`** configuration fields were missing from the **luci** configuration file when it was used in expert mode. This update adds the missing fields.

BZ#917780

The possibility to disable the Red Hat Resource Group Manager (**`rgmanager`**) was missing from the **luci** configuration. With this update, it is now possible to disable **`rgmanager`** in **luci** expert mode.

BZ#918795

Previously, **luci** was missing the Kdump fencing agent. The agent has been added with this update.

BZ#988446

Zooming the **luci** web interface in the Chrome and Firefox web browsers could cause the **Users and Permissions** tab to be displayed incorrectly. This bug has been fixed with this update, and the tab is now displayed properly.

BZ#999324

In previous releases, the **luci** application has been fixed to parse the cluster resource names with a suffix delimited by the period symbol (**.**) correctly. Due to this fix, the suffix was stripped off automatically. However, it is valid to specify a node name by referring to its IP address in the cluster configuration. When this was done, the node names ending with a suffix delimited by the period symbol, such as ".1" or ".sh", were not shown properly and could not be edited. Also, such a node was indicated as not being a cluster member. This bug has been fixed, and such nodes are now handled properly in the described scenario.

BZ#1003062

Previously, the **luci** application used the **10g** type as the default for the **type** attribute of the **oracledb** resource agent. This behavior was incorrect because **luci** was supposed to use the original configuration and do not set its own. With this update, the type field is not arbitrarily specified by **luci**.

BZ#1004011

Certain configurable parameters for the **fence_xvm** agent were missing from the **luci** application. This update adds the missing attributes, such as ***Timeout*** for expert and non-expert mode and ***Path to Key File***, ***IP Port***, ***Multicast Address***, ***Multicast Retransmit Time***, ***IP Family***, ***Authentication Type***, and ***Packet Hash Type*** for expert mode.

BZ#1004922

When creating a new cluster, the ***post_join_delay*** parameter in the cluster configuration was set to 3 or 6 seconds depending if the cluster was configured using the **cluster.conf** file or the cluster software. With this update, this inconsistent approach has been fixed. When no value is specified for ***post_join_delay***, the value is not set in the **cluster.conf** file but the cluster software specifies the value, which is set to 6 seconds.

BZ#1008510

The name for the **fence_enegera** agent in the fence list was **Egenera SAN Controller**. This name was outdated and thus misleading. With this update, the agent is listed correctly as **Egenera BladeFrame**.

BZ#1019853

Previously, the ***self_fence*** parameter was missing from the configuration of the **netfs** resource agent. Also in the GUI, there was no checkbox entry for the **Self-Fence If Unmount Fails** option. This update adds the missing parameter.

BZ#1026374

Due to previous changes in the **luci** application, SELinux no longer labeled the **luci** process with the confined **piranha_web_t** SELinux context type. This behavior was incorrect, thus a new script has been added to the luci packages to address this bug. Also the SELinux policy has been modified accordingly. As a result, the **luci** process now runs as **piranha_web_t** as expected.

BZ#1100817

Previously, the **luci** application did not list virtual machine resource agents in the **Resources** menu in the web UI. An attempt to manually add a virtual machine resource agent in the configuration file caused the error 500 to be returned. This update provides a patch to fix this bug and virtual machine resource agents are now correctly listed in the **Resources** menu.

Enhancements

BZ#919225

The **luci** application has been enhanced to display global cluster resources and sort them alphabetically and numerically by the resource name, IP address, and other significant resource attributes.

BZ#919243

With this update, the **luci** application validates whether an **`nfsclient`** resource is always associated with an **`nfsexport`** resource. Now, an attempt to create a service with an **`nfsclient`** resource that is not associated with an **`nfsexport`** resource causes the following error to be returned:

```
nfsclient resources must have a parent nfsexport resource
```

BZ#982771

With this update, the **luci** application checks whether the **`beaker.session.secret`** value consists of 20 or more characters. Therefore, the use of values containing less characters is not permitted to increase the security of the server-stored session data.

BZ#991575

This update enhances the **luci** application with the ability to configure the ciphers for SSL/TLS channel between **luci** and a connecting web browser, providing better security control for administrators.

BZ#1061786

This update adds the ability to specify a **`httpd`** binary in the Apache resource configuration screen. This new feature allows the user to use the Multi-Processing Module (MPM) worker with the **`httpd`** daemon in a cluster.

BZ#1070760

With this update, the **luci** application has been modified to allow the user to set static ports for all NFS-related ports.

BZ#1117398

With this enhancement, several changes have been made in the **luci** application:

- Support for configuring newly-added bind-mount resource agents has been added.
- Support for configuring the ***`power_timeout`***, ***`shell_timeout`***, ***`login_timeout`***, and ***`retry_on`*** attributes for the **`fence_brocade`** agent has been added.
- Support for the newly-added attribute ***`reboot_on_pid_exhaustion`*** for the **`<rm>`** tag has been added. This attribute is used in the Red Hat Resource Group Manager (**`rgmanager`**) to allow a service recovery when failing to fork a bash child process with a return code 254.

- The ***skip_undefined*** attribute was no longer needed and it was removed from the fencing configuration in advanced mode.
- Support for configuring the new ***startup_wait*** parameter for the **postgres-8** resource agent has been added. This parameter allows users to configure the sleep time according to their needs.
- Support for the ***ssh_options*** attribute for the **fence_apc**, **fence_virsh**, and **fence_rsa** agents has been added.
- Support for the newly-added ***no_kill*** attribute for the virtual machine (VM) resource agent has been added. This attribute is used to prevent the **rgmanager** utility from killing VMs that did not shut down properly.

All luci users are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements.

8.132. LVM2

8.132.1. RHBA-2014:1387 — 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#857064

Previously, proper handling of the "-A" ("--activevolumegroups") option for the vgdisplay utility was missing. Consequently, vgdisplay displayed inactive Volume Groups (VGs) even though "-A" was used displaying only active VGs, defined here as a VG that contains at least one active Logical Volume (LV). This update adds proper handling of "-A" for vgdisplay. Now, when using the "vgdisplay -A" command ("vgdisplay --activevolumegroups"), only active VGs are displayed.

BZ#878948

Prior to this update, concurrent activation of the same Logical Volume (LV) caused a race condition and the following error message to be returned:

```
Device or resource busy
```

With this update, concurrent activation and deactivation of LVs is prohibited and locking is performed, so that operations are now processed sequentially. As a result, the "lvchange -ay $lv" and "lvchange -an $lv" commands no longer cause this bug if issued concurrently.

BZ#892991

When using the lvmetad daemon, the dmeventd daemon took into consideration metadata that was not up-to-date at a time of a RAID LV repair. Based on the outdated information, the repair did not proceed. With this update, the repair code forces a metadata refresh for the Physical Volumes (PVs) that host the RAID volume, and automatic RAID volume repair using dmeventd and manual repair using "lvconvert --repair" now work as expected regardless of lvmetad being enabled or not.

BZ#905063

Previously, RAID LVs either activated or failed to activate depending on how badly their redundancy was compromised. A new "degraded" activation mode has been added to the lvchange and vgchange utilities to better handle activation of incomplete RAID LVs that still have sufficient level of redundancy. This activation mode is now used by default.

BZ#989174

If the lvm2app lvm_vg_reduce() function was called to remove most but not all physical volumes (PV) from a Volume Group (VG), it often destroyed the VG completely. Moreover, no error message was generated. With this update, lvm_vg_reduce() gains some additional validation, and lvm2app lvm_vg_reduce() now works as expected.

BZ#995157

If the user attempted to assign a clustered attribute to a Volume Group (VG) by running the "vgchange -cy VG" command, and the system was not yet properly configured for it, the user was not prompted to confirm the change. In addition, any subsequent LVM command skipped such clustered VG if system was not specifically configured for it. The bug has been fixed, and the lvm command now prompts and warns the user about enabling clustered attribute on VG provided that the clvmd daemon or cluster is not running. The user can also override this prompt by supplying the "--yes" argument.

BZ#1016218

Previously, Logical Volume Management (LVM) utilities tried to connect to the lvmetad daemon even though the utilities were run with the "--sysinit" option denoting the early system initialization. Nevertheless, lvmetad did not have to be running yet, and thus error messages were issued multiple times during system initialization. This update adds a check whether a LVM utility is running during early system initialization by checking the use of the "--sysinit" option. Now, if lvmetad socket is not present in early system initialization when using "--sysinit", LVM utilities automatically fallback to non-lvmetad mode silently.

BZ#1024347

When converting existing Logical Volume (LV) to a thin-pool LV, the lvm utility needed to open the volume temporarily to be initialized with zeroes at its start. However, this initialization step caused the WATCH udev rule to trigger. Consequently, all udev rules were reevaluated based on the WATCH rule, which caused subsequent scanning of the device for changes and LVM could try to close the device in parallel, which would end up with an error. With this update, lvm uses proper flags for temporary volumes which are used during conversions as intermediate step; these flags direct the udev utility to avoid setting the WATCH rule or initiate any scanning on such devices until they are properly initialized.

BZ#1049296

The lvm utility uses lock files to prevent incompatible operations from running simultaneously. Prior to this update, when forking sub-processes, such as the fsadm utility using the "lvresize -r" command, lvm could incorrectly drop these locks and incorrectly permit commands to run in parallel. This update fixes the exec_cmd() function responsible for the wrong behavior. Now, running "lvresize -r" in parallel with other lvm commands works correctly, and all Logical Volumes (LVs) are correctly resized.

BZ#1084157

Previously, the lvm2-cluster subpackage had a requirement of the same or higher version of the lvm2 package, but did not work unless the versions were exactly the same. As a consequence, lvm2-cluster did not work correctly. With this update, lvm2 and all its subpackages define strict version

dependencies among themselves, including a dependency between the lvm2-cluster subpackage and the lvm2 packages. This way the lvm2-cluster subpackage always depends on the right lvm2 packages and incompatible versions of lvm2-cluster cannot thus be installed at the same time.

BZ#1085553

Previously, information about Physical Volume (PV) availability could be out of date. Consequently, the status string in the output of the lvs command for a RAID LV could be different in identical situations depending on whether lvmetad was used or not. The dmeventd volume monitoring daemon now updates PV information in lvmetad for devices participating in a RAID array that have encountered an error. As a result, if dmeventd is active, which is recommended regardless of this bug, the lvs output is the same in both lvmetad and non-lvmetad cases. Note that when dmeventd is disabled, it is recommended to run the "lvscan --cache" command for faulty RAID arrays to ensure up-to-date information in the lvs output.

BZ#1089229

The device-mapper packages are merged inside lvm2. However, prior dependencies were not strict, and the user could update device-mapper without updating lvm2, leading to a version mismatch. The lvm2 packages and all their subpackages now define strict version dependencies among themselves, so that after updating any of these lvm2 subpackages the user receives consistent update of the main lvm2 packages as well. As there is only one debuginfo package for lvm2 and all its subpackages, this fix also resolves the problem of the user receiving unusable debuginfo if one of the subpackages has been updated to a newer version.

BZ#1113539

If a persistent filter was used, /etc/lvm/cache/.cache, and a new Physical Volume (PV) was created, filters were not reevaluated to acquire any changes that could correctly prevent the PV create process to succeed. Consequently, without up-to-date information, LVM could overwrite existing foreign signatures. With this update, filters are always reevaluated before PV creation. In addition, if a change is done outside the lvm utility after last filter evaluation, these changes are now properly considered before PV creation.

BZ#1121216

When a RAID logical volume mirror was created and then one of the Physical Volume (PV) devices was removed, the "lvconvert --repair" command refused to restore the mirror leg with a PV that was already used partly by another LV. An upstream patch has been applied to fix this bug, and "lvconvert --repair" now accepts a few additional arguments including "--alloc" and "--force", and the mirror leg with a PV is now correctly restored using "lvconvert --repair".

BZ#1124766

Previously, there was an incorrect check of the cluster status of non-clustered snapshot origin Logical Volume (LV) before local deactivation. Consequently, attempts to exclusively deactivate already inactive Logical Volume (LV) locally on a single host (non-clustered) led to the following incorrect error messages being issued:

- ```
  Cannot deactivate remotely exclusive device locally. (newer
  versions)
  ```
- ```
  Cannot deactivate <lv name> locally. (older versions)
  ```

With this update, the check is performed before local deactivation to properly check only clustered LVs, and misleading error messages no longer occur.

BZ#1125154

Previously, the check handling the vgcreate utility while using disks for new Volume Group (VG) for which Physical Volumes (PVs) had not yet been created was incorrect. Consequently, vgcreate several times created PVs with the following misleading error message:

```
Physical volume <pv name> not found
```

The check for existing PVs has been fixed in the vgcreate code not to issue any errors if the PV cannot be found, and is thus created by vgcreate.

BZ#1129311

Due to an incorrect persistent filter, /etc/lvm/cache/.cache, generated when using the pvcreate utility, pvcreate tried to refresh cache if MD filter was switched on. As a consequence, if the pvcreate utility was run against a device with an existing MD signature, signature detected and wiped, the device could continue to be filtered out, as if the signature had not been deleted. This update changes the filters, and the device is now correctly made available for immediate use after the signature is deleted.

BZ#1132547

When the volume_list configuration parameter was set to not allow activation of thin-pool and then a thin volume was created, the transaction_id parameter was moved forward, but the kernel target was not notified about it. As a consequence, future activation failures reporting a transaction ID mismatch could occur. The lvm2 metadata has been fixed, and the lvm utility no longer incorrectly expects that messages were sent to the kernel's thin pool driver when such interaction is forbidden due to activation of volume_list parameters.

BZ#1035871

The lvm2 utility calculates maximum space that a snapshot can use and restricts the user-supplied snapshot size, so that it is never larger than the maximum usable space. However, lvm2 previously calculated snapshot space incorrectly, and under certain circumstances could allocate a snapshot that was too small. As a consequence, when such a snapshot was filled up, it overflowed with modified blocks from origin device, and all data in the snapshot became lost. With this update, lvm2 respects the size specified by the user, and the snapshot no longer overflows.

BZ#1020877

In the cluster, the local activation of a volume was automatically converted into exclusive activation if the volume supported only exclusive mode. However this could cause that local activation activated the volume on a different (non-local) node in the cluster. With this update, automatic conversion has been fixed, and local activation is now converted into local-exclusive activation. In addition, if local activation is successful, the volume is now locally (and exclusively) active.

Enhancements

BZ#669111

With this update, a new command-line option, "--atomic", has been added to the pvmove utility. The "--atomic" option causes all identified Logical Volumes (LV) to be moved together. The commit that places each LV on its final destination is not performed unless the last LV is processed. Thus, the "pvmove abort" command ensures that all affected LVs remain on the source device.

BZ#815680

This update adds two manual pages to cover the Logical Volume (LVM) topics of thin-provisioning and caching, also called "tiered storage". These new man pages are lvmthin(7) and lvmcache(7).

BZ#821932

New reporting fields for each attribute from the original "lv_attr" field have been added. This update provides more descriptive and also more extensive information on logical volumes (LV) attributes. In addition, the attributes encoded in the original "lv_attr" field can now be reported independently.

BZ#829920

The "%FREE" argument can now be used to create RAID logical volumes (LVs); "%FREE" is used with the "-l" ("--extents") argument of the lvcreate command. The resulting size is approximately equal to the desired percentage including adjustments that need to be made for RAID metadata areas.

BZ#880395

With this update, the latest lvm2app library gains new functions to customize the parameters used to create Physical Volumes (PV), namely size, PV metadata copies, PV metadata size, data alignment and data alignment offset, and zeroing.

BZ#986687

With this update, the user is able to create Logical Volume Management (LVM) configuration profiles that contain settings related to LVM reporting. The user can apply these settings per each LVM command simply by using a the following schema: "<lvm command> --command_profile <profile_name>". Now, users are able to define LVM report formatting and settings for each usecase needed.

BZ#997223

This update adds support for erasing detected signatures on newly created Logical Volumes (LVs). When creating a new LV and a signature is detected, Logical Volume Management (LVM) tries to erase the signature first before properly activating the new LV. A prompt with a question has also been added for the user:

```
WARNING: <signature name> signature detected on <device name>. Wipe it?
[y/n]
```

This question confirms the deletion of the signature. In addition, a new lvm.conf option "allocation/wipe_signatures_when_zeroing_new_lvs" has been enabled by default to enable or disable this feature.

BZ#1112551

This update provides criteria-based Logical Volume Management (LVM) reporting by adding the new "-S" ("--select SelectionCriteria") option to LVM reporting commands: pvs, vgs, lvs, pvdisplay, vgdisplay, lvdisplay, and lvm devtypes. SelectionCriteria are criteria constructed by using reporting field names, restricting field values by using comparison operators and creating more complex criteria by using grouping and logical operators.

BZ#951600

A new command-line parameter, "--readonly", has been added to Logical Volume Management (LVM) commands that report the state of Logical Volumes (LVs), Volume Groups (VGs) or Physical Volumes (PVs). The parameter uses a special read-only mode that accesses on-disk metadata without needing locks.

BZ#1122698

Logical Volume Management (LVM) includes considerable improvements to the calculation of an appropriate amount of space to allocate when using percentages in commands such as "lvresize -l+50%FREE". The new behavior strives to be more intuitive; sizes specified are treated either as relating to Logical Extents or to Physical Extents as appropriate, and the new logical size desired for the Logical Volume (LV) is calculated. Rounding is then performed to make sure any parallel stripes or mirror legs are the same size.

BZ#1127451

This update adds new "lv_layout" and "lv_role" Logical Volume Management (LVM) reporting fields. These new fields have been created as part of decoupling existing bits in the "lv_attr" reporting field into separate reporting fields. This separate form is more readable as LVM reports values in full words instead of single characters. It also better suits LVM report output handling in scripts as well as using these new fields within selection criteria (the new "--select" lvm command option).

For more information, see also BZ#1112551 and BZ#821932.

BZ#1130168

With this update, the dmsetup utility gains a new flag, "--deferred". If specified and the device is open, the flag schedules the device to be deleted later after being closed.

Users of lvm2 are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

8.133. MAN-PAGES-FR

8.133.1. RHBA-2014:0637 — man-pages-fr bug fix update

An updated man-pages-fr package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The man-pages-fr package contains a collection of manual pages translated into French.

Bug Fix

BZ#891278

This update of the man-pages-fr package adds a warning that the French man page for the xinetd service includes options that are out of date.

Users of man-pages-fr are advised to upgrade to this updated package, which fixes this bug.

8.134. MAN-PAGES-JA

8.134.1. RHEA-2014:0681 — man-pages-ja enhancement update

An updated man-pages-ja package that adds various enhancements is now available for Red Hat Enterprise 6.

The man-pages-ja package contains manual pages in Japanese.

Enhancements

BZ#976137

The description of the syslog option in the Japanese version of the sudoers(5) manual page has been amended to correctly match the English version.

BZ#993511

The "Files" section in the Japanese version of the crontab(1) manual page has been amended to correctly match the English version.

BZ#1035088

The Japanese version of the nfs(5) manual page has been updated to reflect the current English version more closely.

BZ#1059046

The explanation of the sysconf(_SC_GETGR_R_SIZE_MAX) call in the getgrnam(3) manual page has been amended to describe the function of sysconf(_SC_GETGR_R_SIZE_MAX) clearly and correctly.

Users of man-pages-ja are advised to upgrade to this updated package, which adds these enhancements.

8.135. MAN-PAGES-OVERRIDES

8.135.1. RHBA-2014:1382 — man-pages-overrides bug fix update

Updated man-pages-overrides package that fixes numerous 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#1003511

The "-d", "-G", and "-U" options were removed from the rpc.idmapd command but were still presented in the rpc.idmapd(8) manual page. With this update, these unsupported options have been removed from the rpc.idmapd(8) manual page.

BZ#889049

Previously, an incorrect path to the implicit configuration file was presented in the vhostmd(8) manual page. The vhostmd(8) manual page has been updated to mention the correct path, "/etc/vhostmd/vhostmd.conf".

BZ#1099275

Previously, the mailx(1) manual page contained incomplete information about unsetting environment variables, which could confuse the user. This update adds the complete information to the mailx(1) manual page.

BZ#1087503

Prior to this update, the information in the nl_langinfo(3) and charsets(7) manual pages was

incomplete. The nl_langinfo(3) manual page has been updated to state that the code set for the en_US language defaults to Latin1. Additionally, a note has been added to the charsets(7) manual page that the recommended encoding in all settings and locales is UTF-8.

BZ#1078319

Previously, the core(5) manual page contained an incorrect default value for the coredump_filter value and incomplete descriptions of all bits. The core(5) manual page has been updated to include correct and complete information.

BZ#1112708

The bash(1) manual page did not mention that 512-byte blocks are used for the "-c" and "-f" options in POSIX mode. This update adds the missing piece of information to bash(1).

BZ#1075152

Previously, the xinetd(8) manual page contained incomplete information about what happens to services during the xinetd deamon reload. This update adds a paragraph about termination handling during the xinetd deamon reload to the xinetd(8) manual page.

BZ#1058100

Prior to this update, an incorrect default value for the "persistent" service was documented in the nscd.conf(5) manual page. The nscd.conf(5) manual page has been updated to state that the default value for the "persistent" service is "yes".

BZ#969502

Previously, the rpm(8) manual page did not clearly state that the "--setperms" and "--setugids" options were mutually exclusive. The rpm(8) manual page has been updated to contain complete information.

BZ#1114785

The host.conf(5) resolver library configuration manual page contained an incorrect default value for the "multi" value. The host.conf(5) manual page has been updated to state that the default value for "multi" is "on".

BZ#1066537

Previously, the zsh(1) manual page contained incomplete description concerning emulation mode of the Z shell. This update adds the letter "b" to the list of possible first letters invoking emulation.

BZ#1007865

Previously, the snmp_read(3) manual page was unavailable in Red Hat Enterprise Linux 6. This update adds the missing snmp_read(3) manual page.

BZ#781499

Prior to this update, the description of the "-l" option was missing in the makedeltarpm(8) manual page. This update adds the missing description to makedeltarpm(8).

BZ#1108028

Previously, the ciphers(1) manual page did not describe the following Elliptic Curve Cryptography (ECC) cipher suite groups: Elliptic Curve Diffie–Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA), or Transport Layer Security (TLS) version 1.2 specific features. This update adds the missing description of the ECDH and ECDSA cipher groups and TLSv1.2 features to ciphers(1), and the documentation is now complete.

BZ#964160

Previously, no manual pages for the cracklib-packer and cracklib-unpacker utilities were available. This update adds the cracklib-format(8) manual page, which describes cracklib-packer and cracklib-unpacker.

BZ#809096

The pkcs_slot utility was removed from the opencryptoki package but the manual page was still available. With this update, the pkcs_slot(1) man page has been removed.

BZ#1058793

Previously, the curl(1) and curl_easy_setopt(3) manual pages contained a link to the complete list of Network Security Services (NSS) ciphers that led to a non-existent page. This update adds the correct link to the curl(1) and curl_easy_setopt(3) manual pages.

BZ#988713

Previously, the "--rsyncable" option was not documented in the gzip(1) manual page. This update adds the description of "--rsyncable" and the documentation of the gzip utility is now complete.

BZ#1059828

Previously, the manual pages for the pthread_mutex utility were not available in Red Hat Enterprise Linux 6. This update adds the pthread_mutex_consistent(3), pthread_mutexattr_getrobust(3), and pthread_mutexattr_setrobust(3) manual pages.

BZ#1058738

The nscd.conf(5) manual page did not include information about netgroup caching. This update adds the description of netgroup caching to nscd.conf(5).

BZ#1075233

Previously, the pcregrep(1) manual page did not mention the pcresyntax(3) manual page. With this update, a note about pcresyntax(3) has been added to the description and the "See Also" section in the pcregrep(1) manual page.

BZ#818780

Previously, a manual page about configuring the oddjobd-mkhomedir utility was unavailable in Red Hat Enterprise Linux 6. This update adds the oddjobd-mkhomedir.conf(5) manual page.

BZ#816252

Prior to this update, a number of manual pages in Russian language were unreadable due to a redundant re-encoding. This bug has been fixed, no re-encoding is performed as the source pages are provided in the UTF-8 encoding, and the manual pages are now correctly readable.

BZ#1058349

The explanation of the sysconf(_SC_GETGR_R_SIZE_MAX) call in the getgrnam(3) manual page has been amended to describe the function of sysconf(_SC_GETGR_R_SIZE_MAX) clearly and correctly.

BZ#1017478

The flock(2) manual page contained insufficient information about locking files over NFS. With this update, a more precise description of this topic has been added to flock(2).

BZ#1011892

Previously, the documentation for the iconv utility was incomplete. This update adds the iconv(1) manual page.

BZ#1057712

When the openssh package was updated, its man pages were overridden by the man-pages-overrides package. This update removes the ssh_config(5) manual page from man-pages-overrides. The fixed manual pages are now part of the openssh package.

Users of man-pages-overrides are advised to upgrade to this updated package, which fixes these bugs.

8.136. MCELOG

8.136.1. RHBA-2014:1401 — mcelog bug fix and enhancement update

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

The mcelog packages contain a daemon that collects and decodes Machine Check Exception (MCE) data on AMD64 and Intel 64 machines.

This update also fixes the following bugs:

NOTE

The mcelog packages have been upgraded to upstream version 1.0.1, which provides a number of bug fixes and enhancements over the previous version. With this upgrade, mcelog correctly decodes MISC register when IO MCA error events occur. In addition, mcelog exits with an exit status 0, indicating success when stopped by signal. Finally, mcelog has been updated with a new NVR (Name, Version, Release) scheme to synchronize with rolling-release mechanism upstream. (BZ#1032283)

This update also fixes the following bugs:

Bug Fixes

BZ#849252

Prior to this update, log rotation for the /var/log/mcelog file was disabled, which could cause the file system to reach maximum capacity as the existing mcelog files could not be moved. The mcelog.logrotate file has been added to the mcelogd daemon, and the file system can no longer grow indefinitely.

BZ#1079360

Previously, the mcelog packages did not specify mcelogd chkconfig levels. As a consequence, the mcelogd daemon could not be enabled using the ntsysv interface. Default chkconfig levels have been added to /etc/init.d/mcelog, and mcelogd can now be enabled using ntsysv. (BZ1006293)

* Prior to this update, Intel Xeon E5 family processors were not identified uniquely, and the entry to the memory controller decode table was missing. A patch has been applied to fix this bug, and the mcelog packages have been updated to correctly identify Intel Xeon E5 family processors and to display corrected memory read errors.

BZ#1079501

Previously, the select_intel_cputype() function did not work. As a consequence, the following error message was returned on Intel Xeon E6 family processors:

mcelog: Family 6 Model 3f CPU: only decoding architectural errors

The mcelog utility has been updated to support Intel Xeon E6 family processors. Now, decoding on the CPUs with this microarchitecture works properly.

BZ#1059227

Previously, the mcelog packages included three files, intel.c.orig, intel.c.rej, and mcelog.c.orig which were copies of files used in development. The files are not required for the source to compile, or by the mcelog utility, and therefore have been removed.

The mcelog packages have been upgraded to upstream version 1.0.1, which provides a number of bug fixes and enhancements over the previous version. With this upgrade, mcelog correctly decodes MISC register when IO MCA error events occur. In addition, mcelog exits with an exit status 0, indicating success when stopped by signal. Finally, mcelog has been updated with a new NVR (Name, Version, Release) scheme to synchronize with rolling-release mechanism upstream. (BZ#1032283)

In addition, this update adds the following

Enhancement

BZ#872387

Previously, the mcelog utility required the use of the "--logfile" argument when specifying daemon mode in order to ensure that mcelog started with a logging mode. This configuration, however, prevented mcelog from starting with logging only to syslog. With this update, mcelog allows syslog only logging when "--logfile" is not specified.

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

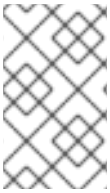
8.137. MDADM

8.137.1. RHBA-2014:1597 — mdadm bug fix and enhancement 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 multiple disk (MD) devices.

This update also fixes the following bugs:



NOTE

The mdadm packages have been upgraded to upstream version 3.3, which provides a number of bug fixes and enhancements over the previous version, including performance improvements. (BZ#1030606)

This update also fixes the following bugs:

Bug Fixes

BZ#1012505

Previously, the permissions on the /etc/cron.d/raid-check file were not sufficiently strict. This update modifies the permissions, allowing only the administrator to read the script stored in /etc/cron.d/raid-check.

BZ#1040006

Previously, the mdadm utility did not work correctly when a disk failed in an Intel Matrix Storage Manager (IMSM) RAID volume. Consequently, the failed disk was removed neither from the volume nor from the container, the volume was not in the "degraded" state, and the rebuild could not start. With this update, mdadm handles failed disks in RAID volumes properly.

BZ#1059193

Previously, the mdadm utility did not apply the "path=*" directive from the /etc/mdadm.conf file when working with SATA devices. Consequently, mdadm searched for the /dev/disk/by-path/ directory that was not created by the udev utility. The bug has been fixed and mdadm no longer ignores the "path=*" directive for SATA devices.

BZ#1059307

Prior to this update, the mdadm utility did not properly verify missing devices when creating an IMSM array. Consequently, when mdadm attempted to create an IMSM array with missing devices, it terminated unexpectedly with a segmentation fault. With this update, missing devices are verified correctly and creating an array with missing devices now works as intended.

BZ#1059316

Previously, when the mdadm thread that monitored the reshaping operation of a disk array was terminated by the SIGTERM signal, it did not clear the suspended data region of the array. As a consequence, the data on the array could become corrupted. With this update, the mdadm thread terminates cleanly and can no longer cause data corruption.

BZ#1075529

Previously, when installing on a system with only the second SATA controller having RSTe mode enabled in UEFI mode, mdadm would not detect the RAID volumes, and installation to them would not be possible. With this update, mdadm correctly detects the RAID volumes and installation to the volumes can happen.

BZ#1136868

Prior to this update, the mdadm utility failed to create an Intel RAID volume when component size was larger than 100GiB. This problem occurred on RAID level 1, 5, and 10. This bug has been fixed and Intel RAID volumes can now be created successfully in the described case.

BZ#1136880

Previously, when the mdadm utility was used to reshape RAID0 and RAID5 volumes created with the Intel Matrix Storage Manager (IMSM) utility, a race condition between the mdadm and mdmon utilities occurred. The reshape operation therefore failed to start. This update prevents the race condition and mdadn can now reshape IMSM modules without complications.

BZ#1136891

RAIDs created with the Intel Matrix Storage Manager (IMSM) utility do not support spanning between different controllers. Under certain circumstances, the mdadm utility allows to fully assemble IMSM RAIDs with disks under different controllers. With this update, a warning message about Host Bus Adapter mismatch is displayed in such a case.

BZ#1136903

Previously, if the system was rebooted or the Intel Matrix Storage Manager (IMSM) was restarted while reshaping an IMSM RAID, the reshape operation was not continued after reassembly. The following message was displayed:

reshape info is not in native format - cannot continue.

This bug has been fixed and reshape is now resumed after system reboot or after IMSM restart.

The mdadm packages have been upgraded to upstream version 3.3, which provides a number of bug fixes and enhancements over the previous version, including performance improvements. (BZ#1030606)

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

8.138. MICROCODE_CTL

8.138.1. RHEA-2014:1466 — microcode_ctl enhancement update

Updated microcode_ctl packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The microcode_ctl packages provide microcode updates for Intel and AMD processors.

Enhancement

BZ#1036240, BZ#1113394

The Intel CPU microcode file has been updated to version 20140624. This is the most recent version of the microcode available from Intel.

Users of microcode_ctl are advised to upgrade to these updated packages, which add this enhancement. Note that the system must be rebooted for this update to take effect.

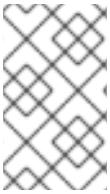
8.139. MIPV6-DAEMON

8.139.1. RHBA-2014:1571 — mipv6-daemon bug fix and enhancement update

Updated mipv6-daemon packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The mipv6-daemon packages contain a mobile IPv6 service for clients, which allows them to relocate within an IPv6-enabled network yet remain reachable.

This update also fixes the following bug:



NOTE

The mipv6-daemon packages have been upgraded to upstream version 1.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#804124)

This update also fixes the following bug:

Bug Fix

BZ#804124

Previously, the mip6d daemon wrote debugging log messages to the stderr output stream, especially during process termination. However, due to a bug in the code, mip6d wrote random data into the netlink socket instead of stderr. These netlink messages were rejected by the kernel and caused SELinux warnings about invalid netlink messages. This update fixes this bug and the described situation no longer occurs.

The mipv6-daemon packages have been upgraded to upstream version 1.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#804124)

Users of mipv6-daemon are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

8.140. MKSH

8.140.1. RHBA-2014:0533 — mksh bug fix

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

The mksh package provides the MirBSD enhanced version of the Public Domain Korn shell (pdksh), a Bourne-compatible shell, which is largely similar to the original AT&T Korn shell. Shift_JIS, also known as "SJIS", is a character encoding for the Japanese language. This package provides mksh support for the Shift_JIS encoding.

Bug Fix

BZ#771198

Previously, the mksh shell worked with bytes instead of characters when looking for the common part of a file name. As a consequence, the common part of the file name could contain only the beginning part of the border character, and only a part of the character was printed. With this update, mksh works with whole characters when looking for the longest common prefix, and tab completion prints the correct common part as expected.

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

8.141. MOBILE-BROADBAND-PROVIDER-INFO

8.141.1. RHBA-2014:0749 — mobile-broadband-provider-info bug fix update

An updated mobile-broadband-provider-info package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The mobile-broadband-provider-info package contains a database of service provider specific settings of mobile broadband (3G) providers in various countries.

Bug Fix

BZ#996599

Previously, the access point name (APN) string incorrectly contained a space at the end. As a consequence, a connection to the Israel Pelephone 3G provider could not be established. This update fixes the typographical error in the APN string, and the connection can now be established as expected.

Users of mobile-broadband-provider-info are advised to upgrade to this updated package, which fixes this bug.

8.142. MOD_AUTH_KERB

8.142.1. RHBA-2014:1557 — mod_auth_kerb bug fix update

Updated mod_auth_kerb packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The mod_auth_kerb packages provide a module for the Apache HTTP Server designed to provide Kerberos authentication over HTTP. The module supports the Negotiate authentication method, which performs full Kerberos authentication based on ticket exchanges.

Bug Fixes

BZ#970678

This update adds the missing description of the "KrbLocalUserMapping" option to the README file.

BZ#981248

Previously, the mod_auth_kerb module was not compatible with the way certain browsers, such as Mozilla Firefox, handled an expired Kerberos ticket. As a consequence, opening a Kerberos-protected page in these browsers with an expired Kerberos ticket caused mod_auth_kerb to fail. With this update, the error in mod_auth_kerb has been addressed and the mentioned problem no longer occurs.

BZ#1050015

Due to a bug in the underlying source code, when the "S4U2Proxy" extension was configured, the mod_auth_kerb module did not renew tickets that were not valid yet. This update applies a patch to fix this bug and the tickets are now correctly renewed as expected.

Users of mod_auth_kerb are advised to upgrade to these updated packages, which fix these bugs.

8.143. MOD_NSS

8.143.1. RHBA-2014:1548 — mod_nss bug fix update

Updated mod_nss packages that fix several bugs 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 Fixes

BZ#866703

Previously, the nss_var_lookup_nss_cert_PEM() function from the nss_engine_vars.c file occasionally caused a memory error. This bug has been fixed and the memory error no longer occurs.

BZ#1002733

Due to a bug in the nss-softokn package that is a dependency of the mod_nss package, the root process of the httpd daemon was occasionally terminated by a SIGTRAP signal. With this update, mod_nss has been updated to depend on a corrected version of nss-softokn and the root httpd process is no longer terminated by SIGTRAP.

BZ#1016628

Due to a bug in the nss-softokn package that is a dependency of the mod_nss package, the httpd daemon sometimes terminated unexpectedly with a segmentation fault and the following message was returned:

NSS_Initialize failed. Certificate database: /etc/httpd/alias

With this update, mod_nss has been updated to depend on a corrected version of nss-softokn and httpd no longer crashes in the described case.

Users of mod_nss are advised to upgrade to these updated packages, which fix these bugs. The httpd service must be restarted for this update to take effect.

8.144. MOD_WSGI

8.144.1. RHBA-2014:1612 — mod_wsgi bug fix update

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

The mod_wsgi adapter is an Apache module that provides a WSGI-compliant interface for hosting Python-based web applications within Apache.

Bug Fix

BZ#1008018

When stopping the httpd daemon with the mod_wsgi module, a short race condition occurred right after its start, during which httpd could terminate unexpectedly with errors. This bug has been fixed and httpd no longer crashes in the described conditions.

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

8.145. MODULE-INIT-TOOLS

8.145.1. RHBA-2014:1437 — 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 2.6 kernels, as well as other module management programs. Device drivers and file systems are two examples of loaded and unloaded modules.

Bug Fix

BZ#1045169

The modprobe utility did not previously recognize information about soft module dependencies in the modinfo section of the queried kernel modules. This update implements support for soft module dependencies, and the "modprobe --show-depends" command now returns this information as expected.

Users of module-init-tools are advised to upgrade to these updated packages, which fix this bug.

8.146. MUTT

8.146.1. RHBA-2014:0945 — mutt bug fix update

Updated mutt packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Mutt is a low resource, highly configurable, text-based MIME e-mail client. Mutt supports most e-mail storing formats, such as mbox and Maildir, as well as most protocols, including POP3 and IMAP.

Bug Fixes

BZ#674271

Prior to this update, an internal hash referencing a specific subject in each envelope referenced a non-existent one. As a consequence, mutt terminated with a segmentation fault when the user attempted to synchronize mailbox after removing one or more messages in threaded mode. With this update, the subject hash updates correctly and the crash no longer occurs.

BZ#690409

Previously, the array that stores mutt message headers did not properly handle empty header entries. This could cause mutt to terminate unexpectedly with a segmentation fault when a change of message IDs occurred on the IMAP server, for example when the IMAP server was connected with multiple clients while removing messages through one of them. In this update, the handling of empty headers has been optimized and sorting messages in the array has been streamlined. As a result, multiple connected clients now synchronize correctly.

BZ#750929

Prior to this update, mutt did not correctly parse certificate files when accessing accounts through IMAP and POP3 protocols. Consequently, mutt terminated unexpectedly with a segmentation fault when attempting to access an IMAP or POP3 account. This update fixes the parsing process and accessing an IMAP or POP3 account now functions as intended.

BZ#1083524

Previously, a bug prevented mutt's interactive certificate verification from working properly. As a consequence, mutt terminated unexpectedly with a segmentation fault when the user tried to send an e-mail message from the command line to a TLS server, for which mutt had not received the

certificate yet. With this update, mutt's interactive certificate verification has been fixed and the described crash no longer occurs.

Users of mutt are advised to upgrade to these updated packages, which fix these bugs.

8.147. NETCF

8.147.1. RHBA-2014:1475 — netcf bug fix and enhancement update

Updated netcf packages that fix several bugs and add various enhancements 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 the netcf library translates into changes to the system's "native" network configuration files.

This update also fixes the following bugs:

NOTE

The netcf package has been upgraded to upstream version 0.2.4, which provides a number of bug fixes and enhancements over the previous version. This includes a change ensuring that an interface with unplugged cable is not considered to be active. (BZ#851748)

This update also fixes the following bugs:

Bug Fixes

BZ#879055

The libvirtd service could terminate unexpectedly when retrieving a MAC address. This happened because the netcf code contained uninitialized data that could be accessed by libvirtd. With this update, netcf properly initializes this data and libvirtd no longer crashes in this case.

BZ#1052156

Previously, netcf added an additional set of quotes to the value of the BONDING_OPTS parameter while attempting to create a bond interface. Consequently, the attempt failed with an error similar to the following:

Error creating interface: 'Could not create interface: internal error failed to create (start) interface bond0: failed to execute external program - Running 'ifup bond0' failed with exit code 1: ./network-functions: line 457: /sys/class/net/bond0/bonding/'mode: No such file or directory

With this update, additional quotes are no longer added to BONDING_OPTS and bonding devices can now be created as expected with this parameter specified.

The netcf package has been upgraded to upstream version 0.2.4, which provides a number of bug fixes and enhancements over the previous version. This includes a change ensuring that an interface with unplugged cable is not considered to be active. (BZ#851748)

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

8.148. NETLABEL_TOOLS

8.148.1. RHBA-2014:0535 — netlabel_tools bug fix update

Updated netlabel_tools packages that fix three bugs are now available for Red Hat Enterprise Linux 6.

NetLabel is a kernel subsystem which implements explicit packet labeling protocols such as CIPSO. Packet labeling is used in secure networks to mark packets with the security attributes of the data they contain. This package provides the necessary user space tools to query and configure the kernel subsystem.

Bug Fixes

BZ#918763

Prior to this update, netlabelctl, the NetLabel management tool, incorrectly handled multi-part netlink messages that limited the number of static labels displayed. Consequently, running the "netlabelctl unlbl list -p" command did not provide the correct output when a large number of static labels were configured. This bug has been fixed, and netlabelctl now works correctly and lists all the configured static labels as expected.

BZ#1000177

Previously, netlabelctl did not allocate enough buffer space for large configuration messages from the kernel. In addition, netlabelctl could not adjust the buffer size in the cases where the buffer was not large enough. As a consequence, a large number of CIPSO level and category translations could not be used. With this update, the default message buffer has been increased, and the buffer is now increased dynamically as necessary. As a result, a large number of CIPSO level and category translations can be used as expected in this scenario.

BZ#1098082

Prior to this update, the file with the licence text was not included in the binary packages. This update adds the license text in the packages.

Users of netlabel_tools are advised to upgrade to these updated packages, which fix these bugs.

8.149. NFS-UTILS

8.149.1. RHBA-2014:1407 — nfs-utils bug fix and enhancement update

Updated nfs-utils packages that fix several bugs and add various enhancements 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, which provides better performance than the traditional Linux NFS server used by most users. These packages contain the mount.nfs, umount.nfs, and showmount programs.

Bug Fixes

BZ#1007195

Prior to this update, the nfsiostat utility was run in the background with the stdout stream redirected to a file. As a consequence, the data was not displayed in a timely matter. This update clears stdout periodically to ensure the buffered output of nfsiostat does not get lost if the nfsiostat process is terminated.

BZ#1033708

The nfs-utils packages were moved to an in-kernel keyring to store the ID mappings needed for NFSv4. However, the kernel key is too small for large enterprise environments. With this update, the nfsidmap utility, used by the kernel to do ID mapping, has been changed to use multiple keyrings.

BZ#1040135

Previously, the rpc.idmapd name mapping daemon returned a warning message after failing to open communication with a client mount. As the warning message was harmless and unnecessary, rpc.idmapd now displays the message only if the user passes the "--verbose" option on the command line.

BZ#1018358

The starting of the rpc.statd utility caused a creation of an extra privileged UDP socket. As a consequence, rpc.statd listened on a random port on all the interfaces, which is required only for internal communication with the rpc.lockd utility. With this update, rpc.statd no longer opens an extra socket in the described situation, and instead opens an extra random port on the loopback address only.

BZ#1075224

The starting of the rpc.statd utility caused messages being flooded to the log. With this update, the socket is kept open until another one is found. As a result, the same port is not reused, and messages are no longer flooding the log in the described situation.

BZ#1079047

When root squashing was enabled and world execute permissions were disabled, using the "-o remount" option of the mount utility caused the mount attempt to fail. This update fixes the chk_mountpoint() function, and the mount utility now checks only execute permissions for unprivileged users, thus fixing this bug.

BZ#1081208

When the rpc.gssd daemon was started, a zero lifetime was sent to the kernel, which then guessed and used the default lifetime. To fix this bug, the correct lifetime is now passed to the kernel, which uses it for timeouts in GSS contexts.

BZ#1087878

Previously, the rpcdebug utility did not work correctly when used with the NFS module and the "state" option. This update allows the "state" option to be used with the NFS module, and NFS state debugging can now be set as expected.

BZ#1113204

Previously, machines with multiple disks made the rpc.mountd utility use 100% of the CPU for 30 to 40 minutes, needlessly scanning the disks. The libblkid daemon usage has been optimized, and rpc.mountd no longer causes downtime in this scenario.

BZ#1136814

Due to a wrong indentation in its code, the nfsiostat utility failed to start. This update adds the correct indentation, and nfsiostat now starts as expected.

In addition, this update adds the following

Enhancements

BZ#918319

This update enhances the nfsmount.conf file manual page to include syntax for mount options. Now, the reader has a better understanding on how to set variables in the configuration file.

BZ#1112776

IPv6 is now a supported address type, and the exportfs utility can thus use IPv6 addresses to export file systems.

BZ#869684

This update adds descriptions on what each value of the column in the output of the nfsiostat utility means.

Users of nfs-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. After installing this update, the nfs service will be restarted automatically.

8.150. NFS-UTILS-LIB

8.150.1. RHBA-2014:1451 — nfs-utils-lib bug fix and enhancement update

Updated nfs-utils-lib packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

The nfs-utils-lib packages contain support libraries required by the programs in the nfs-utils packages.

Enhancement

BZ#1066153

Previously, when the chown utility was used on an NFSv4 mount, chown did not adhere to the no_root_squash option, and thus was not able to change the user and group ownership of each given file. With this update, libnfsidmap, a library to help mapping IDs mainly for NFSv4, has been patched, and chown now handles the user and group ownership as expected.

* The rpc.idmapd daemon has been enhanced to be able to parse fully-qualified user names, such as "user@subdomain". Without this enhancement, the UID or GID mappings were failing and clients were incorrectly listed as owned by "nobody".

Users of nfs-utils-lib are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

8.151. NMAP

8.151.1. RHBA-2014:0683 — nmap bug fix update

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

The nmap packages provide a network exploration utility and a security scanner.

Bug Fix

BZ#1000770

Previously, the ncat utility printed debug messages even in verbose mode. As a consequence, after connecting through an HTTP proxy, a debug message was displayed together with the received data, which could interfere with the automated processing of standard output. With this update, ncat prints debug messages only in verbose mode as expected.

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

8.152. NSS

8.152.1. RHBA-2014:1378 — nss bug fix and enhancement update

Updated nss packages that fix numerous 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. Applications built with NSS can support SSLv3, TLS, and other security standards.

NOTE

The nss and nss-util packges have been upgraded to upstream version 3.16.1 and the nspr package has been upgraded to upstream version 4.10.6, which provide a number of bug fixes and enhancements over the previous versions. (BZ#1099618, BZ#1099619)

Bug Fixes

BZ#606022

The manual pages for the NSS security utilities were missing. This update adds the missing manual pages.

BZ#895339

Previously, the **curl** utility failed to communicate with active FTP over Secure Sockets Layer (SSL) where both control and data connections were encrypted and authenticated by a client certificate with a password-protected private key. This was caused by the Privacy Enhanced Mail (PEM) module that pretended token removal whenever a key was being loaded from a file. Consequently, when the private key was loaded to authenticate the data connection, it caused the already authenticated control connection to fail with the following error code:

```
SSL_ERROR_TOKEN_INSERTION_REMOVAL.
```

The underlying source code in the **NSS PEM** module has been modified, and loading a single key multiple times no longer causes an SSL connection to fail.

BZ#993441, BZ#1004105

With this update, the **nss-softokn** module has been submitted for a FIPS-140 revalidation.

BZ#1031238

The code for removing token certificates from the cache caused a deadlock. Under certain conditions, when a server was processing multiple outgoing replication or windows sync agreements using TLS/SSL and processing incoming client requests that use TLS/SSL and Simple Paged Results, the server became unresponsive to new incoming client requests. With this update, the underlying source code has been modified to fix this bug and clients of NSS no longer become unresponsive in the described scenario.

BZ#1044666

The NSS libraries did not check whether the **NSS_SDB_USE_CACHE** environment variable was set to "yes" before calling the **sdb_measureAccess()** function. Consequently, when using the **cURL** or **libcurl** libraries that depend on NSS to make a HTTPS requests, there were many "access" system calls to paths, directories, and files that did not exist. This behavior led to excessive size of the directory entry cache. This update modifies NSS to avoid calling **sdb_measureAccess()** when **NSS_SDB_USE_CACHE** is set to "yes", thus limiting the system calls to the non-existent paths. As a result, **cURL** HTTPS requests no longer cause the cache to be too large.

BZ#1053437

Previously, an incorrect **CHECK_FORK()** call in the **nss-softokn** module prevented the Admin Server component of Red Hat Directory Server from recovering after an improper shutdown. As a consequence, the Red Hat Directory Server parent process was unable to shut down NSS. Therefore, when Red Hat Directory Server was configured on an SSL port, the Admin Server component terminated unexpectedly with a segmentation fault. With this patch, the problematic **CHECK_FORK()** calls have been removed and users can now start Red Hat Directory Server and use SSL-encrypted traffic as expected.

BZ#1057224, BZ#1057226

The section in the spec file that is used to set and export the **NSS_ENABLE_ECC** and **NSS_ECC_MORE_THAN_SUITE_B** build time environment variables was missing. Consequently, NSS was prevented from allowing external **pkcs #11** cryptographic modules to support Elliptic Curve Cryptography (ECC) algorithms beyond those specified in suite B, thus preventing support for pluggable ECC. The mentioned spec file has been fixed and pluggable ECC are now supported as expected.

BZ#1059176

Previously, the NSS libraries allowed users to disable the internal cryptographic module. When users set up an external cryptographic module, such as **opencryptoki**, as the preferred module and disabled the internal cryptographic module, NSS could terminate unexpectedly with a segmentation fault. NSS has been modified to prevent users from disabling the internal module and therefore no longer fails in the described scenario.

BZ#1090681

Due to a race condition in functions that manage user-defined slots, the **PK11_DoesMechanism()** call failed on the Red Hat Directory Server. The code that manages the user-defined slots now checks if the slot is present and skips any reinitialization, cached present values, and locking. If the module is not thread-safe, as is the case with the Privacy Enhanced Mail (PEM) module, the slot **sessionLock** is the same as the module reference lock and there is no need to use **sessionLock**. As a result, **PK11_DoesMechanism()** no longer crashes.

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

8.153. NUMACTL

8.153.1. RHBA-2014:1483 — numactl bug fix and enhancement update

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

The numactl packages add simple Non-Uniform Memory Access (NUMA) policy support. It consists of the numactl program to run other programs with a specific NUMA policy, and the libnuma library to perform allocations with NUMA policy in applications.

This update also fixes the following bugs:

NOTE

The numactl packages have been upgraded to upstream version 2.0.9, which provides a number of bug fixes and enhancements over the previous version. (BZ#1017048)

This update also fixes the following bugs:

Bug Fixes

BZ#812462

Prior to this update, the numa_parse_cpustring() function added an unallowed CPU into its bitmask. As a consequence, only the bits the user has access to were set. Consequently, every time the function was used led to different outcomes. With this update, the numa_parse_cpustring() code sets all bits in the "cpustring" argument regardless of current task's CPU mask, and the aforementioned scenario no longer occurs.

BZ#819133

Previously, the compiler was enforcing libnuma to provide a constant within the "char*" parameter, which led to the following warning message being returned:

testconst.c:10:45: warning: deprecated conversion from string constant to ‘char*’ [-Wwrite-strings]

The underlying source code has been fixed so that the string is handled as a constant, and the user no longer receives warning messages.

BZ#873456

Previously, when the user set the affinity of the shell to be a subset of available CPUs and then attempted to use the numactl utility to bind to something absent from that affinity mask, the attempt failed. An upstream patch has been applied to fix this bug, and the numactl environment has been extended so that the user can choose whether to allow for the affinity mask to determine available CPUs or not.

BZ#1100134

Due to incompatibilities emerging after the latest numactl packages update, virsh processes terminated unexpectedly when any virsh command was run. This bug has been fixed, and the virsh commands now work correctly.

The numactl packages have been upgraded to upstream version 2.0.9, which provides a number of bug fixes and enhancements over the previous version. (BZ#1017048)

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

8.154. NUMAD

8.154.1. RHBA-2014:1594 — numad bug fix update

Updated numad packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The numad packages provide a daemon for NUMA (Non-Uniform Memory Architecture) systems, monitors NUMA characteristics and manages placement of processes and memory to minimize memory latency. The packages also provide an interface that can be used to query the numad daemon for the best manual placement of an application.

Bug Fixes

BZ#872524

Previously, running the numad daemon on a system executing a process with very large resident memory, such as a Windows Server 2012 guest, could cause memory swapping. As a consequence, significant latencies under some circumstances occurred on the system, which could in turn lead to other processes, such as qemu-kvm, becoming unresponsive. With this update, numad no longer causes memory swapping in the above scenario, and the consequent latencies and hangs no longer occur.

BZ#999062

Prior to this update, when a process bound to a set of NUMA nodes depleted the system memory, the system started memory swapping instead of using other NUMA nodes for memory allocation. Consequently, the system experienced significant latencies or became unresponsive. With this update, numad unbinds memory nodes after moving the process memory, which allows for other nodes to be used for memory allocation, and thus prevents the described latencies and hangs.

BZ#1011908

Previously, the numad daemon ignored existing control groups when localizing QEMU threads, and as a consequence, it incorrectly consolidated all running threads into a single control group. This update introduces numad support for multiple control groups, and numad therefore no longer moves QEMU threads into undesired control groups.

Users of numad are advised to upgrade to these updated packages, which fix these bugs.

8.155. OPENCRYPTOKI

8.155.1. RHBA-2014:1613 — opencryptoki bug fix update

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

The opencryptoki packages contain version 2.11 of the PKCS#11 API, implemented for IBM Cryptocards, such as IBM 4764 and 4765 crypto cards. This package includes support for the IBM 4758 Cryptographic CoProcessor (with the PKCS#11 firmware loaded), the IBM eServer Cryptographic Accelerator (FC 4960

on IBM eServer System p), the IBM Crypto Express2 (FC 0863 or FC 0870 on IBM System z), and the IBM CP Assist for Cryptographic Function (FC 3863 on IBM System z). The opencryptoki package also brings a software token implementation that can be used without any cryptographic hardware. This package contains the Slot Daemon (pkcsslotd) and general utilities.

Bug Fixes

BZ#1027606

Previously, on the IBM System z architecture, the opencryptoki Common Cryptographic Architecture (CCA) token was sending incorrect information to the CKA_ECDSA_PARAMS attribute when generating an EC key pair. As a consequence, opencryptoki failed to verify the public key. This bug has been fixed and the CCA token now sends the correct information to CKA_ECDSA_PARAMS, and public keys are verified successfully.

BZ#1131745

Prior to this update, the IBM Crypto Accelerator (ICA) token did not handle the chunk size or tail calculation correctly in case of zero message sizes. As a consequence, an overflow occurred leading to a general protection fault (GPF). The underlying source code has been fixed, and GPFs no longer occur.

Users of opencryptoki are advised to upgrade to these updated packages, which fix these bugs.

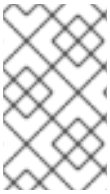
8.156. OPENLDAP

8.156.1. RHBA-2014:1426 — openldap bug fix and enhancement update

Updated openldap packages that fix several bugs and add various enhancements 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.

This update also fixes the following bug:



NOTE

The openldap packages have been upgraded to upstream version 2.4.39, which provides a number of bug fixes and enhancements over the previous version. Specifically, Memory-mapped database library (LMDB) support in OpenLDAP has been enabled. (BZ#923680)

This update also fixes the following bug:

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

8.157. OPENMOTIF

8.157.1. RHBA-2014:1542 — openmotif bug fix update

Updated openmotif packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The openmotif packages include the Motif shared libraries needed to run applications which are dynamically linked against Motif, as well as MWM, the Motif Window Manager.

Bug Fixes

BZ#869782, BZ#953938

Prior to this update, the size set in the GeometryManager() function based on the XmFormConstraint "preferred_width" field was not updated when the label was changed and still contained the previous label length. Consequently, if the label text was modified while the window was smaller than the actual label width, the resulting size was incorrectly computed and the label text truncated. With this update, the values are updated and the fault no longer occurs in the described scenario.

BZ#1000343

Previously, when the Motif Window Manager, or MWM, was used as the window manager and the Mwm*freezeOnConfig and Mwm*moveOpaque options were set to "False", only icons appeared while moving a window anywhere on the screen, and no frame border was drawn. Consequently, users were having problems navigating the applications on their touch screen monitors. A patch has been provided to fix this bug, and windows are now displayed correctly when being moved anywhere on the screen.

BZ#1058644

Due to a bug in the underlying source code, an attempt to use the XmEXTENDED_SELECT policy could cause the Motif libraries to terminate unexpectedly with a segmentation fault. This update applies a patch to fix this bug and Motif no longer crashes in the described scenario.

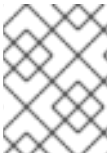
Users of openmotif are advised to upgrade to these updated packages, which fix these bugs.

8.158. OPENSLP

8.158.1. RHBA-2014:1482 — openslp bug fix and enhancement update

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

OpenSLP is an open source implementation of the Service Location Protocol (SLP) which is an Internet Engineering Task Force (IETF) standards track protocol and provides a framework to allow networking applications to discover the existence, location, and configuration of networked services in enterprise networks.



NOTE

The openslp packages have been upgraded to upstream version 2.0.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#1065558)

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

8.159. OPENSSH

8.159.1. RHSA-2014:1552 — Moderate: openssh security, bug fix, and enhancement update

Updated openssh packages that fix two security issues, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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.

OpenSSH is OpenBSD's SSH (Secure Shell) protocol implementation. These packages include the core files necessary for both the OpenSSH client and server.

Security Fixes

CVE-2014-2653

It was discovered that OpenSSH clients did not correctly verify DNS SSHFP records. A malicious server could use this flaw to force a connecting client to skip the DNS SSHFP record check and require the user to perform manual host verification of the DNS SSHFP record.

CVE-2014-2532

It was found that OpenSSH did not properly handle certain AcceptEnv parameter values with wildcard characters. A remote attacker could use this flaw to bypass intended environment variable restrictions.

Bug Fixes

BZ#993580

Based on the SP800-131A information security standard, the generation of a digital signature using the Digital Signature Algorithm (DSA) with the key size of 1024 bits and RSA with the key size of less than 2048 bits is disallowed after the year 2013. After this update, ssh-keygen no longer generates keys with less than 2048 bits in FIPS mode. However, the sshd service accepts keys of size 1024 bits as well as larger keys for compatibility reasons.

BZ#1010429

Previously, the openssh utility incorrectly set the oom_adj value to -17 for all of its children processes. This behavior was incorrect because the children processes were supposed to have this value set to 0. This update applies a patch to fix this bug and oom_adj is now properly set to 0 for all children processes as expected.

BZ#1020803

Previously, if the sshd service failed to verify the checksum of an installed FIPS module using the fipscheck library, the information about this failure was only provided at the standard error output of sshd. As a consequence, the user could not notice this message and be uninformed when a system had not been properly configured for FIPS mode. To fix this bug, this behavior has been changed and sshd now sends such messages via the syslog service.

BZ#1042519

When keys provided by the pkcs11 library were removed from the ssh agent using the "ssh-add -e" command, the user was prompted to enter a PIN. With this update, a patch has been applied to allow the user to remove the keys provided by pkcs11 without the PIN.

In addition, this update adds the following

Enhancements

BZ#953088

With this update, ControlPersist has been added to OpenSSH. The option in conjunction with the ControlMaster configuration directive specifies that the master connection remains open in the background after the initial client connection has been closed.

BZ#997377

When the sshd daemon is configured to force the internal SFTP session, and the user attempts to use a connection other than SFTP, the appropriate message is logged to the /var/log/secure file.

BZ#1028335

Support for Elliptic Curve Cryptography modes for key exchange (ECDH) and host user keys (ECDSA) as specified by RFC5656 has been added to the openssh packages. However, they are not enabled by default and the user has to enable them manually. For more information on how to configure ECDSA and ECDH with OpenSSH, see: https://access.redhat.com/solutions/711953

All openssh users are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements.

8.160. OPENSSL

8.160.1. RHBA-2014:1525 — openssl bug fix and enhancement update

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

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Datagram Transport Layer Security (DTLS) protocols, as well as a full-strength, general purpose cryptography library.

Bug Fixes

BZ#1057520

Previously, cipher suites based on the single-DES and RC2 algorithms were on the default list of cipher suites used by the SSL or TLS client and by the server in the OpenSSL library. This allowed for suboptimal cipher suites to be negotiated between the OpenSSL client or server and a third party client or server. In addition, a higher amount of supported cipher suites in the TLS ClientHello request impaired the inter-operability of the OpenSSL TLS client. This update removes single-DES-based and RC2-based cipher suites from the default list of cipher suites, improving the security and compatibility of the OpenSSL TLS client.

BZ#1056608

Cipher suites based on the Triple DES (3DES) algorithm had their bit strengths erroneously set to 168 bits when running under the SSL or TLS protocols. As a consequence, they were incorrectly sorted before cipher suites based on the AES-128 algorithm. This update sets the bit strength of 3DES-based cipher suites to 128 bits, and they will now be sorted after AES-128-based cipher suites as expected.

BZ#1090952

In TLS client applications that use the SSLv2 protocol, the TLS extension giving the list of supported Elliptic Curve Cryptography (ECC)-based cipher suites could not be sent. This caused a TLS connection to a server which used an ECC-based cipher suite not supported by the OpenSSL client to abort. With this update, the ECC-based cipher suites are not sent in the SSLv2 ClientHello request, and TLS connections are no longer aborted in the above circumstances.

BZ#1119800

The TLS extensions that were sent in the Datagram TLS (DTLS) ClientHello requests did not previously contain the list of the supported ECC-based cipher suites. As a consequence, the DTLS connections to servers using ECC cipher suites not supported by the OpenSSL client were aborted. With this update, the ECC-based cipher suite list is properly sent in the DTLS ClientHello requests, and DTLS connections are no longer aborted in the above circumstances.

In addition, this update adds the following

Enhancements

BZ#1002926, BZ#1039105, BZ#1002930, BZ#1015056

The openssl packages have been enhanced to allow for FIPS-140-2 validation of the OpenSSL library as a FIPS cryptographic module.

BZ#1057715

When connecting to a server using ECDHE-based or DHE-based cipher suites, the s_client utility now reports the size of ECDHE and DHE parameters selected by the server. This allows for easy verification whether the used configuration set is secure.

Users of openssl are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

8.161. OPENSWAN

8.161.1. RHBA-2014:1588 — openswan bug fix and enhancement update

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

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 that allow to build secure tunnels through untrusted networks.

Bug Fixes

BZ#739949

When using the protoport option in combination with the type=passthrough setting to exclude traffic from encryption, an incorrect inverse policy was installed and the exclusion was not successful. Now, the correct policy is installed in the described situation.

BZ#834397

Starting multiple connections with the leftsubnets= or auto=start options led to a crypto overload and subsequent restart of Openswan. The pluto cryptohelper has been fixed to prevent the overload.

BZ#970279

The ikev2=insist setting was not enforced on the responder side, allowing an IKEv1 connection to be established instead. This bug has been fixed and ikev2=insist is no longer ignored.

BZ#970349

This update fixes multiple lingering states after reestablishing IKEv2 keys.

BZ#988106

This update enforces the limits set with esp, phase1alg, and andphase2alg options. Previously, any algorithm of the default set (aes, 3des, sha1, md5) was always allowed, regardless of the above options.

BZ#993124

IKEv2 delete payloads were not always properly delivered to the remote peer, leaving the remote endpoint with lingering unused connections. Now, IKEv2 delete payloads are delivered as expected.

BZ#1002708

This update modifies the rightid=%fromcert option to load IDs from the local certificate when set for the local end, and from the certificate delivered by the remote peer when set for the peer end.

BZ#1019746

The "ipsec ikeping" command did not recognize the --exchangenum option. This option is now recognized correctly.

BZ#1021961

This update fixes a crash of the IKE pluto daemon when using the SHA2 encryption family with the ike= option with IKEv2.

BZ#1041576

Openswan no longer drops various privileges too soon, which prevented it from reading configuration files in directories not owned by root.

BZ#1050340

The IKE pluto daemon occasionally crashed and restarted when referencing missing IKEv2 payloads. The Openswan's state machine has been updated to reject packets with missing payloads.

BZ#1070356

This update fixes the compatibility problems with older versions of Cisco VPN introduced in the previous update of the openswan packages.

BZ#1088656

After restarting the remote endpoint, the sourceip option was not properly reset in the local route entry. This bug has been fixed.

BZ#1092913

If there was no NSS database available, the IKE pluto daemon created a nonfunctional replacement. A missing NSS database is now created before the pluto daemon starts and in the %post phase of the package install, which fixes this bug.

BZ#1098473

The "ipsec newhostkey" command did not return a correct non-zero exit code in case of failure, for example when generating keys of insufficient strength. Now, ipsec newhostkey returns the correct exit code.

BZ#1114683

Configuring an AH algorithm for IKEv2, or various non-standard ESP algorithms for IKEv1 or IKEv2 (such as CAST, RIPEMD160 or CAMELLIA) caused the IKE pluto daemon to terminate unexpectedly and restart. This bug has been fixed and pluto no longer crashes when AH or ESP algorithms are configured.

BZ#1126066

Using the "force_busy=yes" developer option to force anti-DDOS mode in IKEv2 caused the IKE pluto daemon to crash and restart. This bug has been fixed and pluto no longer crashes in the described situation.

In addition, this update adds the following

Enhancement

BZ#730975, BZ#1018327, BZ#1099871, BZ#1105179

This update enhances and clarifies man pages shipped with the openswan packages.

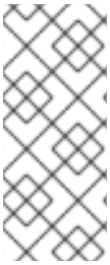
Users of openswan are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

8.162. OPROFILE

8.162.1. RHEA-2014:1473 — oprofile bug fix and enhancement update

An updated oprofile package that fix several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

OProfile is a system-wide profiler for Linux systems. The profiling runs transparently in the background and profile data can be collected at any time. OProfile uses the hardware performance counters provided on many processors, and can use the Real Time Clock (RTC) for profiling on processors without counters.



NOTE

The oprofile package has been upgraded to upstream version 0.9.9, which provides a number of bug fixes and enhancements over the previous version including added support for Intel Xeon Processor E5-XXXX v2, Intel Xeon Processor E3-XXXX v3, Intel Broadwell Microarchitecture and Intel Atom Processor CXXXX CPU architectures. (BZ#809709, BZ#818353, BZ#832160, BZ#1121437, BZ#1128627)

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

8.163. PACEMAKER

8.163.1. RHBA-2014:1544 — pacemaker bug fix update

Updated pacemaker packages that fix several bugs 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.

Bug Fixes

BZ#1036631

Previously, co-location constraints for cloned groups were not fully respected. As a consequence, members of cloned groups were not correctly stopped along with dependencies. Now, members of cloned groups are stopped whenever dependencies are also stopped.

BZ#1037423

Prior to this update, no information concerning the status of healthy members of a cloned resource group were displayed to the user. A new option has been added to allow the status of cloned groups to be shown in the output of the "pcs status --full" command.

BZ#1046131

Previously, Pacemaker did not correctly cancel the recurring monitor operation of LSB scripts it managed. Consequently, monitor operations failed after resources successfully stopped. This bug has been fixed, and recurring monitor operations are now correctly cancelled before the LSB resource is stopped.

BZ#1069279

Under some conditions, the default stop or start ordering of resources enabled violation of co-location constraints. As a consequence, resources could be temporarily active on the same node despite a colocation constraint that instructed them otherwise. With this update, ordering of resources respects configured colocation constraints, and resources are never on the same node if configured not to be.

BZ#1078954

Previously, Pacemaker could not start more than 10 instances of a cloned resource. As a consequence, clusters containing more than 10 nodes did not function correctly. This update fixes this bug, and Pacemaker can now properly start an unlimited number of instances of a cloned resource.

BZ#1086885

Due to a timing issue, nodes that rebooted too fast became stuck in the pending state and did not rejoin the cluster. With this update, the timing issue has been resolved, nodes now join the cluster, and are reported as online.

Users of pacemaker are advised to upgrade to these updated packages, which fix these bugs.

8.164. PAM

8.164.1. RHBA-2014:1579 — pam bug fix update

Updated pam packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Pluggable Authentication Modules (PAM) provide a system to set up authentication policies without the need to recompile programs to handle authentication.

Bug Fixes

BZ#947011

The pam_unix module contained an "off-by-one" error when comparing the date of user account expiration with the current date. In this situation, the real expiration of the account happened a day after the date specified by the "chage -E" command. This update fixes the "off-by-one" error and user accounts now expire on the date set by the "chage -E" command.

BZ#1120099

The pam_unix and pam_pwhistory modules did not properly handle missing fields in the entries in the /etc/security/opasswd file. As a consequence, if some of the fields were not present in a user's entry, changing the password for example with the passwd command could result in a segmentation fault. This bug has been fixed and pam_unix and pam_pwhistory now properly handle missing fields in the entries in /etc/security/opasswd.

BZ#1054936

Previously, the pam_limits module did not verify whether the process referenced in the /var/run/utmp file as the login process still existed. As a consequence, when the user had the "maxlogins" limit set in the limits.conf file and the login session process terminated unexpectedly and also did not update the utmp file correctly, the user did not have access to the system even if some of his previous login session no longer existed due to the crash. After this update, pam_limits tests whether the login process still exists on the system. As a result, the number of existing login sessions is counted more precisely when the "maxlogins" limit is applied by the pam_limits module.

BZ#1119289

Previously, the pam_userdb module handled the call to the crypt() function too strictly not to expect modern crypt hash formats. As a consequence, pam_userdb was not able to support any other hash algorithms supported by the glibc library for the user password hashes. This update improves the code handling the crypt() function. Now, pam_userdb supports any password hash formats supported by the glibc crypt() function.

Users of pam are advised to upgrade to these updated packages, which fix these bugs.

8.165. PAM_PKCS11

8.165.1. RHBA-2014:1474 — pam_pkcs11 bug fix update

Updated pam_pkcs11 packages that fix two bugs are now available for red Hat Enterprise Linux 6.

The pam_pkcs11 package allows X.509 certificate-based user authentication. It provides access to the certificate and its dedicated private key with an appropriate Public Key Cryptographic Standards #11 (PKCS#11) module.

Bug Fixes

BZ#887143

The pam_pkcs11 utility generated an incorrect Lightweight Directory Access Protocol (LDAP) URL when attempting to connect to port 636. As a consequence, the connection to that port failed. This update applies a patch to address this bug, and pam_pkcs11 now generates correct LDAP URL in the described scenario.

BZ#1012082

After adding the coolkey module manually using the full path by running the "modutil -add "CoolKey PKCS #11 Module" -dbdir /etc/pki/nssdb -libfile /usr/lib64/pkcs11/libcookeypk11.so" command, an attempt to log in using a smart card failed. The underlying source code has been modified to fix this bug and the user is now able to log in using the smart cards as expected.

Users of pam_pkcs11 are advised to upgrade to these updated packages, which fix these bugs.

8.166. PANGO

8.166.1. RHBA-2014:0585 — pango bug fix update

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

Pango is a library for laying out and rendering of text, with an emphasis on internationalization. Pango forms the core of text and font handling for the GTK+ widget toolkit.

Bug Fixes

BZ#885846

Prior to this update, the Pango library used an incorrect macro for specifying a location of its man pages. Consequently, after installing the pango packages, the man pages were placed in the wrong directory. This update fixes the relevant macro in the Pango spec file and the man pages are now located in the correct directory.

BZ#1086690

Previously, the pango RPM scriptlet did not mask harmless error messages. As a consequence, although the migration was successful, the scriptlet printed error messages related to missing directories after an upgrade from Red Hat Enterprise Linux 6 to Red Hat Enterprise Linux 7. This update determines the location of the directory with the cache file, and these harmless error messages no longer appear.

Users of pango are advised to upgrade to these updated packages, which fix these bugs.

8.167. PARTED

8.167.1. RHBA-2014:1450 — parted bug fix and enhancement update

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

The parted packages provide tools to create, destroy, resize, move, and copy hard disk partitions. The parted program can be used for creating space for new operating systems, reorganizing disk usage, and copying data to new hard disks.

Bug Fixes

BZ#1018075

Previously, parted wrongly assumed that a minor number of a device was always equal to its major number plus its partition number. However, this is not true with some devices, such as DM multipath devices. As a consequence, operations with parted on DM multipath devices were failing. With this update, parted verifies the mount status of a device by the path to the device instead of using the "minor:major" number.

BZ#929319

The parted program printed an unnecessary warning when used with disks that had the sector size of 4 KB. With this update, this confusing warning has been removed from parted.

BZ#975478

Previously, the align-check directive did not work correctly when used from parted in interactive mode. Users had to use parted in script mode in order to be able to utilize the align-check directive. This update corrects the relevant code, and align-check now works in interactive mode as expected.

BZ#1074069

The parted program could fail with an EBUSY error if it was rapidly called in a loop. To resolve this problem, this update modifies parted to keep retrying for up to 1 second when receiving an EBUSY error.

BZ#1139435

To prevent failures on systems that do not support partitioned loop devices, such as IBM S/390 systems, the t8000-loop.sh test has been modified to being no longer run on these systems.

In addition, this update adds the following

Enhancement

BZ#1054283

This update adds support for GUID Partition Table (GPT) disk labels on PreP partitions on the 64-bit PowerPC architectures.

Users of parted are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.168. PCIUTILS

8.168.1. RHBA-2014:1006 — pciutils bug fix update

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

The pciutils packages provide various utilities for inspecting and manipulating devices connected to the PCI bus.

Bug Fixes

BZ#1032827

Prior to this update, the lspci command did not correctly handle empty PCI slots. As a consequence, lspci printed a warning message when it was used on a system with one or more unused PCI slots. Following this update, lspci disregards empty PCI slots and the described problem no longer occurs.

BZ#998626

Previously, the source link for PCI IDs in the /usr/sbin/update-pciids file of the pciutils package was deprecated, and consequently invoked an outdated list of PCI devices. With this update, /usr/sbin/update-pciids has been amended and now links to the up-to-date PCI ID list.

Users of pciutils are advised to upgrade to these updated packages, which fix these bugs.

8.169. PCP

8.169.1. RHEA-2014:1477 — pcp enhancement update

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

Performance Co-Pilot (PCP) is a suite of tools, services, and libraries for acquisition, archiving, and analysis of system-level performance measurements. Its light-weight, distributed architecture makes it particularly well suited to centralized analysis of complex systems.

This enhancement update adds the pcp packages to Red Hat Enterprise Linux 6. (BZ#640150)

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

8.170. PCS

8.170.1. RHBA-2014:1526 — pcs bug fix and enhancement update

Updated pcs packages that fix several bugs and add one enhancement are 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.

Bug Fixes

BZ#1029129

The pcs utility was using an incorrect location to search for cluster node names, and the "pcs cluster standby" command therefore could not find the specified cluster node. As a a consequence, it was not possible to put cluster nodes in standby mode. With this update, pcs properly searches for node names in the /etc/cluster/cluster.conf file and putting cluster nodes in standby mode works correctly.

BZ#1025054

Previously, pcs was unable to create user ID (UID) and group ID (GID) entries in the cluster.conf file. Consequently, non-root users could not gain access to corosync.conf and therefore could not access corosync. Now, pcs support for configuring UID and GID entries in cluster.conf has been added, and non-root users can be granted access to corosync with the "pcs cluster uidgid" command.

BZ#1066927

When using the "pcs resource create" command with the "--group" option, pcs created a resource

and added it to a resource group in two separate steps instead of one. Consequently, a resource that was added to a pre-existing resource group sometimes initially started on an incorrect node. With this update, pcs creates a resource in a resource group as a single step when "--group" is used, and the created resource starts on the correct node.

BZ#1019410

When adding a STONITH fencing level, pcs sometimes mistakenly detected that some nodes were not a part of a cluster . As a consequence, it was not possible to add a STONITH level unless the "--force" option was used. Now, pcs correctly determines whether a node is a part of a cluster and, as long as a valid node is used, adding a pcs STONITH level no longer requires the use of the "--force" option.

BZ#1094517

Previously, pcs did not allow the use of the following attributes for STONITH fencing agents: pcmk_reboot_action, pcmk_monitor_action, and pcmk_status_action. As a consequence, using any of these attributes when configuring a STONITH agent caused the configuration to fail. With this update, pcs correctly allows the use of the attributes and the configuration no longer fails when they are used.

BZ#1108778, BZ#1107612

The pcs utility did not properly handle clones of a group when removing resources from the cloned group. As a consequence, the "pcs resource unclone" and "pcs resource delete" commands removed only the first resource in a group when they were supposed to remove the entire resource group. With this update, pcs handles resources in cloned groups correctly and removing cloned resource groups works as expected.

BZ#1107965

Due to an error in detecting whether resource groups are managed, pcs sometimes could not delete a cloned resource group or a master or slave resource group. With this update, pcs detects the status of resource groups correctly, and deleting the mentioned resource groups proceeds normally.

BZ#1094812

Previously, pcs attempted to use the corosync.conf file when listing cluster nodes using the "pcs status nodes corosync" command. However, corosync.conf does not exist in Red Hat Enterprise Linux 6. As a consequence, "pcs status nodes corosync" failed to execute. Now, cluster nodes on Red Hat Enterprise Linux 6 are listed using the cman_tool program and the /etc/cluster/cluster.conf file, and "pcs status nodes corosync" functions correctly.

In addition, this update adds the following

Enhancement

BZ#1035300

The pcsd daemon has been added to the pacemaker packages for Red Hat Enterprise Linux 6, which allows users to remotely start, stop, enable, or disable the cluster, and also to remotely set up the cluster configuration.

Users of pcs are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.171. PCSC-LITE

8.171.1. RHBA-2014:1463 — pcsc-lite bug fix and enhancement update

Updated pcsc-lite packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

PC/SC Lite provides a Windows SCard compatible interface for communicating with smart cards, smart card readers, and other security tokens.

Enhancement

BZ#1092751

This update allows the pcsc-lite packages to be combined with the pcsc-cyberjack packages from the Extra Packages for Enterprise Linux (EPEL) repository. This allows pcsc-lite to support the driver for Reiner SCT cyberJack RFID standard card reader that is included in pcsc-cyberjack.

Users of pcsc-lite are advised to upgrade to these updated packages, which add this enhancement.

8.172. PERL-AUTHEN-SASL

8.172.1. RHBA-2014:0641 — perl-Authen-SASL bug fix update

An updated perl-Authen-SASL package that fixes one bug is now available for Red Hat Enterprise Linux 6.

Simple Authentication and Security Layer (SASL) is a generic mechanism for authentication used by several network protocols. The Authen::SASL module provides an implementation framework that all protocols should be able to share.

Bug Fix

BZ#965739

Due to a bug in the Authen::SASL Perl module, the substr() function attempted to read data outside of the appropriate string. As a consequence, when the user was authenticated against an LDAP server over SASL, performing logical operations, such as search, with a Perl program on that server failed. With this update, the Authen::SASL module verifies the length of the string that is encrypted and written to a filehandle. As a result, performing a search returns correct results in the described situation.

Users of perl-Authen-SASL are advised to upgrade to this updated package, which fixes this bug.

8.173. PERL-CLASS-METHODMAKER

8.173.1. RHBA-2014:0534 — perl-Class-MethodMaker bug fix update

Updated perl-Class-MethodMaker packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The perl-Class-MethodMake packages provide the perl module Class::MethodMaker which solves the problem of having to continually write accessor methods for your objects that perform standard tasks.

Bug Fix

BZ#1064837

Previously, the perl-Class-MethodMake source package contained some source code used for testing that was licensed under a restrictive license. This bug fix removes all tests that used that source code. The binary packages have been updated to use this new source package. However, there has been no change in the functionality of these packages.

Users of perl-Class-MethodMaker are advised to upgrade to these updated packages, which fix this bug.

8.174. PERL-CRYPT-SSLEAY

8.174.1. RHBA-2014:0466 — perl-Crypt-SSLeay bug fix update

Updated perl-Crypt-SSLeay packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The perl-Crypt-SSLeay packages contain Perl modules that provide support for the HTTPS protocol under Library for WWW in Perl (LWP) so that LWP::UserAgent can make HTTPS GET, HEAD, and POST requests. The perl-Crypt-SSLeay packages contain Net::SSL module, which is automatically loaded by requests from the LWP::Protocol::https module, and provide the necessary SSL glue for the module to work.

Bug Fix

BZ#1059992

The perl-Crypt-SSLeay packages included their own certification authority's (CA) certificates bundle. As a consequence, the content provided by the /usr/share/doc/perl-Crypt-SSLeay-0.57/ca-bundle.crt file became out of date. With this update, /usr/share/doc/perl-Crypt-SSLeay-0.57/ca-bundle.crt has been replaced with a symbolic link to the /etc/pki/tls/certs/ca-bundle.crt file, which is a system-wide storage file for trusted CA certificates. As a result, the perl-Crypt-SSLeay documentation does not contain a bundle of CA certificates that is out of date and could confuse the user.

Users of perl-Crypt-SSLeay are advised to upgrade to these updated packages, which fix this bug.

8.175. PERL-TIMEDATE

8.175.1. RHBA-2014:1425 — perl-TimeDate bug fix update

An updated perl-TimeDate package that fixes one bug is now available for Red Hat Enterprise Linux 6.

perl-TimeDate is a perl library that parses time and date information.

Bug Fix

BZ#993222

Previously, some time zones were missing in the perl-TimeDate package, so the user could not set, for example, the Alaska Standard time zone. Support for the missing time zones has been added to the Time/Zone.pm module, namely the following:

AEDT Eastern Australian Daylight AEST Eastern Australian Standard AKDT Alaska Daylight AKST Alaska Standard METDST Middle European DST MSD Moscow Daylight MSK Moscow

As a result, the list of time zones in Time/Zone.pm is now complete.

Users of perl-TimeDate are advised to upgrade to this updated package, which fixes this bug.

8.176. PERL-WWW-CURL

8.176.1. RHBA-2014:0588 — perl-WWW-Curl bug fix update

Updated perl-WWW-Curl packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The perl-WWW-Curl packages provide a Perl extension interface for libcurl.

Bug Fix

BZ#984894

Previously, accessing the value of the CURLINFO_PRIVATE option caused a program to terminate unexpectedly with a segmentation fault. This update fixes this by ensuring that CURLINFO_PRIVATE is an accessible scalar string. As a result, programs can now access CURLINFO_PRIVATE as expected.

Users of perl-WWW-Curl are advised to upgrade to these updated packages, which fix this bug.

8.177. PHP

8.177.1. RHBA-2014:1465 — php bug fix update

Updated php packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Bug Fixes

BZ#1054953

Previously, an incorrect parameter type was used in internal calls. As a consequence, the execution of the php-mysql module requests did not work correctly on big-endian machines, such as 64-bit PowerPC and IBM System z. The parameter has been changed to match the expected type. As a result, php-mysql requests produce the expected output.

BZ#1069167

Prior to this update, a mysql link could be closed even when prepared statements still existed. Consequently, executing those statements caused a segmentation fault. With this update, a mysql link is only closed when all statements are freed, and the statements can be executed as expected.

BZ#1045019

Previously, the host HTTP header was missing from soap calls. As a consequence, HTTP requests were not RFC2616 compliant. This update adds the HTTP header to the soap calls. As a result, the requests are now RFC2616 compliant and can go through a proxy server.

BZ#1053982

Previously, the php packages contained a bug concerning the oci_lob_load() function. As a consequence, compiling the php OCI8 module failed. The underlying source code has been modified, and the OCI8 extension can now be compiled correctly.

BZ#954027

Prior to this update, dependency on the Spl extension for the Session extension was missing from the php packages. Consequently, Spl was uninitialized before Session, which made the autoload feature unavailable. With this update, Session requires Spl and the autoload feature is now available as expected.

BZ#953786

Previously, the php packages contained an inconsistency in the behavior of a static call in a non-static method. Consequently, a call from the context's class (name, static or self) inside a non-static method results in a static-call. This update restores the standard behavior. As a result, a call inside a non-static method is now non-static, and the called method inherits the $this variable.

Users of php are advised to upgrade to these updated packages, which fix these bugs. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

8.178. PKI-CORE

8.178.1. RHBA-2014:1622 — pki-core bug fix update

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

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.

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.

This update fixes the following bug:

Bug Fix

BZ#1146818

Several Java import statements specify wildcard arguments. However, due to the use of "wildcards arguments" in the import statements of the source code contained in the Red Hat Enterprise Linux 6 maintenance branch, a name space collision created the potential for a wrong class to be utilized. As a consequence, the Token Processing System (TPS) rebuild test failed with an error message. This update addresses the bug by supplying the fully named class in all of the contentious areas, and TPS rebuild test no longer fails.

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.

Users of pki-core are advised to upgrade to these updated packages, which fix this bug.

8.178.2. RHBA-2014:1549 — pki-core bug fix and enhancement update

Updated pki-core packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

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.

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.

This update fixes the following bugs:

Bug Fixes

BZ#1024462

Previously, the IPA CA certificate was created with SHA1 signing algorithm, instead of SHA256. A patch has been provided to fix this bug, and the certification is now correct.

BZ#1051382

Prior to this update, IPA Replica installation failed when using an external CA certificate. The interoperability problems have been fixed, and IPA again works with external CA certificates.

BZ#1055080

Previously, the pki utility generated copious debug log, filling up the /var/log file system with log messages. This update implements the log rotation functionality, thus fixing the bug.

BZ#1083170

When the LANG variable for specifying a locale was set to "tr_TR.UTF8", the installation of IPA became unresponsive. This update prevents Lightweight Directory Access Protocol (LDAP) attributes from being affected by LANG, and IPA no longer hangs.

BZ#1096142

Previously, the setup of the IPA replica failed during external CA Certificate setup with "unable to parse xml" error message. The underlying source code has been patched, and the setup of the replica system now works flawlessly.

BZ#1109181

Due to Access Vector Cache (AVC) denial messages in the audit.log file, the certmonger daemon could not start tracking Public Key Infrastructure (PKI) certificates. Consequently, errors during FreeIPA installation occurred. This update provides a patch for AVC, and certmonger now starts tracking PKI certificates as intended.

BZ#1123811

While installing the IPA Server, numerous Access Vector Cache (AVC) denial messages were stored in audit.log. However, AVC messages were not a blocker and installation proceeded successfully. The problematic source code has been patched, and IPA Public Key Infrastructure (PKI) clone certificate renewal no longer produces AVC denial messages.

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.

In addition, this update adds the following

Enhancement

BZ#1061442

With this update, the "CS.cfg" file is automatically backed up to "CS.cfg.bak" following a successful restart of any configured PKI instance.

Users of pki-core are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.179. PM-UTILS

8.179.1. RHBA-2014:1455 — 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#1025006

Previously, pm-utils did not support the Advanced Configuration and Power Interfaces (ACPI) S1 (Power on Suspend) power state. As a consequence, when BIOS supported the ACPI S3 (Suspend to RAM) power state but not the S1 power state, the "pm-suspend" command failed. This update introduces support for the S1 power state, and if the S3 power state is not supported by BIOS, pm-suspend now triggers the S1 power state.

Users of pm-utils are advised to upgrade to these updated packages, which fix this bug.

8.180. POLICYCOREUTILS

8.180.1. RHBA-2014:1625 — policycoreutils bug fix update

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

The policycoreutils packages contain the core utilities that are required for the basic operation of a Security-Enhanced Linux (SELinux) system and its policies.

Bug Fix

BZ#1148800

A new "noreload" option has been implemented for semanage commands in Red Hat Enterprise Linux 6.6. However, due to a missing reload initialization in the semanageRecords() function, users could not enable a Boolean directly using seobject python module coming from the policycoreutils-python utility. This bug has been fixed, and users can now set the Boolean correctly also using the seobject python module.

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

8.180.2. RHBA-2014:1569 — policycoreutils bug fix update

Updated policycoreutils packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The policycoreutils packages contain the core utilities that are required for the basic operation of a Security-Enhanced Linux (SELinux) system and its policies.

Bug Fixes

BZ#885526

An attempt to use the SELinux graphical utility to create a new SELinux policy with a name that contained the dash character ("_") failed with an error. The underlying source code has been modified to fix this bug and the error is no longer returned in the described scenario. As a result, it is possible to create SELinux policies with names containing "_".

BZ#913175

The "sandbox -M" command failed to start when the home directory was linked with a symbolic link. This bug has been fixed and sandbox now properly works with home directories linked with symbolic links.

BZ#961805

Certain option descriptions were missing from the sandbox(8) and restorecon(8) manual pages. The descriptions have been added to those manual pages.

BZ#1002209

The "semanage fcontext -a -e [source_directory] [target_directory]" command sets the same SELinux file context for the target directory as the source directory has. When the user specified the name of the source directory with the trailing slash character ("/") at the end, the command failed to change the context. This update applies a patch to fix this bug and the command now works as expected.

BZ#1028202

When running the "semanage permissive -a [type]" command with an incorrect domain type, an invalid .te file was generated and stored. Consequently, an attempt to execute the command again with the valid domain type failed because semanage tried to compile the previously generated invalid .te file. This bug has been fixed and semanage now works as expected.

BZ#1032828

The semanage "-N" option was not supported and an error was returned when trying to use the option. This update adds the support for the "-N" option.

BZ#1043969

The "fixfiles restore", "fixfiles check", and "fixfiles validate" commands can be executed with or without specifying a directory. Previously, when the aforementioned commands were run with no directory specified, they returned a non-zero value. This behavior is incorrect because no error was encountered. The underlying source code has been modified to fix this bug and the commands no longer return a non-zero value in the described scenario.

BZ#1086456

Due to an incorrect handling of parameters in the setfiles code, the setfiles command did not check the legality of all given parameters. With this update, the code has been modified and setfiles now correctly checks the legality of the given parameters.

BZ#1086572

When the setfiles utility was executed with a non-existent directory specified, the command was supposed to return an error message but it did not. The underlying source code has been modified to fix this bug and the command now properly returns the error message in the described scenario.

BZ#1091139

This update removes the incorrectly working sandbox "-c" option.

BZ#1098062

The setfiles "-d" option shows what specification matches each file. The setfiles "-q" option suppresses a non-error output. Previously, it was possible to specify both options in one setfiles command, even though the options were contrary to each other. With this update, the options have been marked as mutually exclusive. As a result, an attempt to execute them at once fails and an error message is returned.

BZ#1119726

An attempt to run the semanage command with the "-i" argument specified failed with a traceback. The underlying source code has been modified to fix this bug and "semanage -i" now works as expected.

Users of policycoreutils are advised to upgrade to these updated packages, which fix these bugs.

8.181. POLKIT

8.181.1. RHBA-2014:1533 — polkit bug fix and enhancement update

The updated polkit packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

PolicyKit is a toolkit for defining and handling authorizations.

Bug Fixes

BZ#628862

Previously, running the pkaction command with invalid arguments opened the corresponding manual page instead of generating a warning, or giving any other indication of erroneous behavior. With this update, the user is informed by an error message.

BZ#864613

Prior to this update, in PolicyKit local authority, the order of processing configuration files within a directory depended only on file system specifics. The ordering has been made consistent to avoid surprising changes in behavior but remains unspecified and may change in future updates of Red Hat Enterprise Linux; use the documented ordering of directory names if your configuration relies on ordering of the .pkla configuration files.

BZ#1132830

Prior to this update, if a process subject to an authorization query became a zombie before completing the authorization, the polkitd daemon could terminate unexpectedly. Handling of zombie processes has been improved to fix this crash.

In addition, this update adds the following

Enhancements

BZ#927406

With this update, all polkit binary files have been compiled with the RELRO option, and where applicable, with the PIE option, to increase resilience against various attacks.

BZ#812684

With this update, more flexibility in polkit rules is allowed. In addition to the existing “unix-user:" and “unix-group:” identity specifications, a new specification “default” can be used to specify authorization result for users that do not match either of the ”unix-user:” or “unix-group:” specifications.

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

8.182. POLKIT-GNOME

8.182.1. RHBA-2014:0425 — polkit-gnome bug fix update

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

The polkit-gnome packages provide an authentication agent for the polkit authentication manager, which is an application-level toolkit for defining and handling the policy that allows non-privileged processes communicate with privileged ones.

* Due to a bug in the source code, the authentication dialog of the polkit GNOME authentication manager could send an invalid time stamp to the window manager when the dialog was displayed for the first time. Consequently, the dialog did not receive focus for keyboard input, and the input was sent to the previously-focused window instead. This bug has been fixed, and valid time stamps are now obtained and sent to the window manager. As a result, keyboard input is always sent to the displayed authentication dialog as expected. (BZ#872918)

Bug Fix

BZ#872918

Due to a bug in the source code, the authentication dialog of the polkit GNOME authentication manager could send an invalid time stamp to the window manager when the dialog was displayed for the first time. Consequently, the dialog did not receive focus for keyboard input, and the input was sent to the previously-focused window instead. This bug has been fixed, and valid time stamps are now obtained and sent to the window manager. As a result, keyboard input is always sent to the displayed authentication dialog as expected.

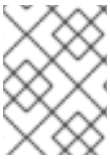
Users of polkit-gnome are advised to upgrade to these updated packages, which fix this bug.

8.183. POSTGRESQL-JDBC

8.183.1. RHBA-2014:1489 — postgresql-jdbc bug fix update

The updated postgresql-jdbc package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

PostgreSQL is an advanced Object-Relational database management system. The postgresql-jdbc package includes the .jar files needed for Java programs to access a PostgreSQL database.



NOTE

The postgresql-jdbc package has been upgraded to upstream version 8.4.704, which provides a number of bug fixes over the previous version. (BZ#873972)

Users of postgresql-jdbc are advised to upgrade to this updated package, which fixes these bugs.

8.184. POWERPC-UTILS

8.184.1. RHBA-2014:1454 — powerpc-utils bug fix and enhancement update

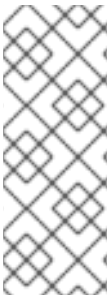
Updated powerpc-utils packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The powerpc-utils packages provide various utilities for the PowerPC platform.

* The update_flash utility now supports Firmware Entitlement Checking. (BZ#1006777)

* The ofpathname utility now supports virtio-blk disks. (BZ#1039462)

In addition, this update fixes the following bug:



NOTE

The powerpc-utils packages have been upgraded to upstream version 1.2.20, which provides a number of bug fixes and enhancements over the previous version. Among others, the powerpc-utils packages now provide the following new features:

* Support for Dynamic CPU Affinity using the Platform Resource Reassignment Notifications (PRRN) interface from user space has been added. (BZ#1021522)

* The update_flash utility now supports Firmware Entitlement Checking. (BZ#1006777)

* The ofpathname utility now supports virtio-blk disks. (BZ#1039462)

In addition, this update fixes the following bug:

Bug Fixes

BZ#1021522

Support for Dynamic CPU Affinity using the Platform Resource Reassignment Notifications (PRRN) interface from user space has been added.

BZ#1006777

The update_flash utility now supports Firmware Entitlement Checking.

BZ#1039462

The ofpathname utility now supports virtio-blk disks.

BZ#1064496, BZ#1087723

Previously, the kernel was not notified before and after an update of a device tree during a partition migration. As a consequence, the lpar utility terminated unexpectedly upon resuming after the migration. With this update, the kernel is notified as expected and lpar no longer crashes in the described scenario.

The powerpc-utils packages have been upgraded to upstream version 1.2.20, which provides a number of bug fixes and enhancements over the previous version. Among others, the powerpc-utils packages now provide the following new features:

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

8.185. PPC64-DIAG

8.185.1. RHBA-2014:1445 — 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.

This update also fixes the following bug:

NOTE

The ppc64-diag packages have been upgraded to upstream version 2.6.6, which provides a number of bug fixes and enhancements over the previous version. (BZ#929278)

This update also fixes the following bug:

Bug Fix

BZ#988237

Previously, there were file conflicts between the ppc64-diag and powerpc-utils packages. As a consequence, installation of Red Hat Enterprise Linux which contained recent versions of these packages failed. This update fixes the conflicts between ppc64-diag and powerpc-utils, and installation of Red Hat Enterprise Linux now completes successfully.

The ppc64-diag packages have been upgraded to upstream version 2.6.6, which provides a number of bug fixes and enhancements over the previous version. (BZ#929278)

In addition, this update adds the following

Enhancement

BZ#949612

This update adds the LightPath Diagnostics framework to the ppc64-diag tool set. This new feature helps identify failed hardware components through LED lights and then facilitate replacement.

All users of ppc64-diag are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

8.186. PROCPS

8.186.1. RHBA-2014:1595 — procps bug fix and enhancement update

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

The procps packages contain a set of system utilities that provide system information. The procps packages include the following utilities: ps, free, skill, pkill, pgrep, snice, tload, top, uptime, vmstat, w, watch, and pwdx.

Bug Fixes

BZ#950748

The /lib64/libproc.so development symbolic link was present in both the main procps package and its devel sub-package. This caused file conflicts when installing the devel sub-package. This update removes the duplicate symbolic link from the main package so that the devel sub-package can be installed without problems.

BZ#963799

The 'free' command always displayed zero in the 'shared' column as the procps-ng library was attempting to read from non-existent 'MemShared' field in /proc/meminfo file. With this update, the 'shared' column is reused for a value representing the 'MemShared' field, thus fixing this bug.

This update also introduces a new '-a' option for the free command that enables a new column that represents a recently added field called 'MemAvailable'. The kernel does not export this field by default, so it needs to be explicitly enabled. Refer to the free(1) man page for more details.

In addition, this update adds the following

Enhancements

BZ#977467

Previously, only one configuration file could be passed to the 'sysctl' tool with the '-p' option. This update allows users to pass multiple configuration files with this option. As a result, users can perform shell expansion by using braces and wildcard characters.

BZ#1105125

With this update, the 'top' and 'watch' tools accept floating point numbers representing the polling or refresh intervals. Both widely used floating point separators ('.' and ',') can be applied, regardless of the locale settings in use.

BZ#1034337

This update introduces man pages for the openproc(), readproc() and readproctab() functions available in the libproc library. These manuals help writing applications that utilize the aforementioned functions.

BZ#1060681

This update introduces a new 'q' option (alternatively '-q' or '--quick-pid') to the 'ps' command. This option is essentially a speed-optimized enhancement of the 'p' option. The new option is recommended in cases where users only need to specify a list of PIDs to be shown, and do not need other selection and sorting options.

BZ#1011216, BZ#1082877, BZ#1089817

This update also enhances several man pages.

Users of procps are advised to upgrade to these updated packages, which fix these bugs.

8.187. PULSEAUDIO

8.187.1. RHBA-2014:0750 — pulseaudio bug fix update

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

PulseAudio is a sound server for Linux, UNIX, and similar operating systems.

Bug Fix

BZ#1095750

Due to limited support of the pulseaudio server for multiple High-Definition Multi-media Interface (HDMI) devices per sound card, audio would previously sometimes not function properly on specific Intel and Nvidia configurations, such as the Haswell microarchitecture processors. With this update, the support for multiple HDMI devices per sound card has been implemented for pulseaudio, and HDMI audio output now works in the described scenarios as expected.

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

8.188. PYKICKSTART

8.188.1. RHBA-2014:1541 — pykickstart bug fix and enhancement update

An updated pykickstart package that fixes one bug and adds two enhancements is now available for Red Hat Enterprise Linux 6.

The pykickstart package contains a python library for manipulating kickstart files.

Additionally, this update adds the following enhancement:

NOTE

The pykickstart package has been upgraded to upstream version 1.74.15, which provides one bug fix and one enhancement over the previous version. This version of pykickstart, or higher, is required for the latest version of Anaconda to work properly. (BZ#1108543)

Additionally, this update adds the following enhancement:

Enhancement

BZ#1125410

The pykickstart package has been modified to support installation of Docker images in Anaconda.

Users of pykickstart are advised to upgrade to this updated package, which fixes this bug and adds these enhancements.

8.189. PYTHON-KERBEROS

8.189.1. RHBA-2014:1600 — python-kerberos bug fix update

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

The python-kerberos packages contain a high-level wrapper for Kerberos Generic Security Service Application Program Interface (GSSAPI) operations.

Bug Fixes

BZ#973379

Previously, the name of the egg-info file contained an incorrect version of the python-kerberos packages. As a consequence, the module dependency resolution did not work correctly. With this update, the egg-info file name contains the correct version, and resolving dependencies works as expected.

BZ#1057333

Prior to this update, the authenticate_gss_client_wrap() function miscalculated the length of the username string when wrapping it. Consequently, the Kerberos user name was not properly encoded into a GSSAPI message, and the authentication failed. This patch fixes the calculation of the username string length, and the authentication no longer fails.

Users of python-kerberos are advised to upgrade to these updated packages, which fix these bugs.

8.190. PYTHON-LINUX-PROCFS

8.190.1. RHBA-2014:1615 — python-linux-procfs bug fix update

Updated python-linux-procfs packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The python-linux-procfs package enables the extraction of information from the /proc file system.

Bug Fix

BZ#1133700

Previously, there was a bug in the tuna packages; when the scheduler priority was not specified, the "tuna -t $PID -p OTHER" command failed with an error. Fixing this bug in tuna required an update of the python-linux-procfs package. Therefore, python-linux-procfs has been updated to the newer version with this update to address the tuna bug.

Users of python-linux-procfs are advised to upgrade to these updated packages, which fix this bug.

8.191. PYTHON-VIRTINST

8.191.1. RHBA-2014:1444 — python-virtinst bug fix and enhancement update

Updated python-virtinst package that fixes several bugs and add various enhancements are 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 Fixes

BZ#853386

Due to a bug in the python-virtinst package, the "virt-install --graphics spice" command did not create a spicevmc channel. This bug has been fixed and the aforementioned command now works as expected.

BZ#873545

Due to a bug in the python-virtinst package, the "sparse=false" parameter of the virt-install command was ignored and the newly crated storage was not fully allocated. This bug has been fixed and the "virt-install sparse=false" command now works correctly.

BZ#1000980

Prior to this update, when the allocation of a new lvm volume was set to 0 with the virt-install utility, no error message was returned. With this update, virt-install has been modified to display an error message in the aforementioned case.

BZ#1055225

The virt-manager utility failed to clone virtual machines (VMs) with fully allocated logical volumes. After clicking the Clone button in virt-manager GUI, the following message was displayed:

Sparse logical volumes are not supported

This bug has been fixed and VMs with fully allocated logical volumes can now be cloned successfully with virt-manager GUI.

BZ#1077232

When the virt-install command was executed with the "device=lun" option, it terminated with the following message:

Unknown device type 'lun'

This bug has been fixed, and lun device type is now recognized correctly by virt-install.

BZ#1085499

When selecting a PCI device to be assigned to a virtual machine, the virt-manager GUI did not display the domain of PCI devices. Consequently, it was impossible to assign a PCI device in any domain other than zero. This bug has been fixed and virt-manager now displays domains correctly in the described case.

In addition, this update adds the following

Enhancements

BZ#855740

This update adds support for the MacVTap device driver to the python-virtinst package. MacVTap, which facilitates virtualized bridged networking, can now be used when installing new virtual guest machines.

BZ#1001999

This update adds options for USB redirection to the python-virtinst package.

BZ#1011290

The list of operating system variants displayed by the "virt-install --os-variant list" command has been updated.

BZ#1017423

This update enables the startup_policy parameter for the --disk option of the virt-install command. This parameter allows to specify what to do with the disk if the source file is not accessible. It accepts the same parameters as the startupPolicy domain XML attribute.

Users of python-virtinst are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

8.192. QEMU-KVM

8.192.1. RHBA-2014:1490 — 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. The qemu-kvm package provides the user-space component for running virtual machines using KVM.

Bug Fixes

BZ#1067576

Repeated creation of virtual machine (VM) image snapshots gradually increases the string size of the image filename. However, the number of characters in the filename strings for virtual VM images was previously limited to 1024. Consequently, when the size limit was reached, creating an image snapshot failed to be executed or the VM did not successfully boot. With this update, the filename string size limit has been increased to 4096, and the described problems only occur with an extremely high amount of snapshots.

BZ#1113917

Vendor-specific SCSI commands issued from a KVM guest did not reach the target device because QEMU regarded such commands as invalid. This bug has been fixed and vendor-specific SCSI commands are now properly propagated to the target device.

BZ#1092117

Previously, the bdrv_is_allocated() function returned "True" for unallocated sectors. Consequently, when performing live incremental migration, the disk size was in some cases considerably expanded due to unintended transfer of unallocated sectors beyond the end of the base image. With this update, the bdrv_is_allocated() returns "False" for unallocated sectors. As a result, the disk size no longer changes in the mentioned scenario.

BZ#1017858

When hot unplugging a virtual CPU (vCPU) from a guest using libvirt, the current Red Hat Enterprise Linux QEMU implementation does not remove the corresponding vCPU thread. Consequently, libvirt did not detect the vCPU count correctly after a vCPU was hot unplugged, and it was not possible to hot plug a vCPU after a hot unplug. In this update, information from QEMU is used to filter out inactive vCPU threads of disabled vCPUs, which allows libvirt to perform the hot plug.

BZ#1035162

The "dump-guest-memory" command did not correctly support memory compression, which caused crash dump files to take up excessive hard drive space. The memory compression of "dump-guest-memory" has now been fixed, and the crash dump files now have the expected size.

In addition, this update adds the following

Enhancements

BZ#1106420

The ioeventfd mechanism has been enabled in the virtio-scsi-pci controller. This allows QEMU to process I/O requests outside of the vCPU thread, which reduces the latency of submitting requests and improves single task throughput.

BZ#786407

A new device, virtio-rng, can be configured for guests, which makes the entropy from the host available to guests. By default, this information is sourced from the host's /dev/random file, but hardware random number generation (RNG) available on hosts can be used as the source as well.

BZ#826266

The dump-guest-memory.py script has been introduced into QEMU, which makes it possible to analyze a guest memory dump from the QEMU-KVM core in case of a guest kernel failure.

BZ#845667

KVM now supports the use of a virtualized Performance Monitoring Unit (vPMU). This allows users to run performance monitoring tools on Linux guests, as well as to perform a live guest migration while using PMU.

BZ#1006159, BZ#1097021

The qemu-img utility is now able to create images in the VHD and VHDX format, which can be used with the Microsoft Hyper-V hypervisor.

BZ#1007708

The support for version 3 of the Virtual Machine Disk (VMDK) format has been added to the qemu-img utility. This allows qemu-img to read image info and convert the format of VMDK3 image files.

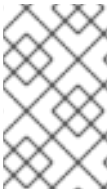
Users of qemu-kvm are advised to upgrade to these updated packages, which fix these bugs and add these enhancement. After installing this update, shut down all running virtual machines. Once all virtual machines have shut down, start them again for this update to take effect.

8.193. QL2400-FIRMWARE

8.193.1. RHBA-2014:1452 — ql2400-firmware bug fix and enhancement update

An updated ql2400-firmware package that fixes several 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

The ql2400-firmware package has been upgraded to upstream version 7.03.00, which provides a number of bug fixes and enhancements over the previous version. (BZ#1054301)

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.

8.194. QL2500-FIRMWARE

8.194.1. RHBA-2014:1453 — ql2500-firmware bug fix and enhancement update

Updated ql2500-firmware package that fixes several 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

The ql2500-firmware package has been upgraded to upstream version 7.03.00, which provides a number of bug fixes and enhancements over the previous version. (BZ#1076497)

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.

8.195. RDMA

8.195.1. RHBA-2014:1551 — rdma bug fix and enhancement update

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

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.

Several components provided by the rdma packages have been upgraded to newer upstream versions that provide a number of bug fixes and enhancements. The following components have been upgraded: infiniband-diags, libmlx4, libmlx5, libibverbs, libibverbs-utils, librdmacm, librdmacm-utils, ibutils, libibmad, libibumad, libipathverbs, libmthca, infiniband-diags, libibcommon, mstflint, mvapich2, openmpi, opensm, osu-micro-benchmarks, perftest, qperf, and srptools. (BZ#1053488, BZ#1087968, BZ#1093468, BZ#1087968, BZ#1053500, BZ#1051290, BZ#1051211, BZ#1055654, BZ#1053391, BZ#1059093, BZ#1056662, BZ#1059093, BZ#1059094, BZ#1059095, BZ#102730, BZ#1082730)

This update also fixes the following bugs:

Bug Fixes

BZ#828074

Prior to this update, the rping utility from the librdmacm-utils package failed to establish an RDMA connection after accepting a connection request from the client. This bug has been fixed and rping now creates connections as expected in the described case.

BZ#828082

Under certain circumstances, the udaddy utility from the librdmacm-utils package became unresponsive while receiving data transfers. This bug has been fixed and udaddy no longer hangs in the aforementioned scenario.

BZ#1024903

Previously, the ib_qib kernel module initialized certain mezzanine cards using a kernel module parameter. However, the support for this method of initialization has been deprecated and removed upstream, and was therefore removed from the Red Hat kernel in a previous update. As a consequence, the initialization of certain mezzanine cards no longer succeeded. With this update, a modprobe configuration file is provided by the libipathverbs library that enables the proper configuration of the ib_qib module from user space. As a result, the affected mezzanine cards now initialize as expected.

BZ#1097290

Previously, the shared OpenType font library “libotf.so.0” was provided by both the openmpi package and the libotf package. Consequently, when an RPM spec file requested libotf.so.0 in order to operate properly, Yum could install either openmpi or libotf to satisfy the dependency. However, as these two packages do not provide compatible libotf.so.0 libraries, the program either worked or not depending on whether or not the right provider was selected. The libotf.so.0 in openmpi is not intended for other applications to link against, it is an internal library. With this update, libotf.so.0 in openmpi is excluded from RPM library identification searches. As a result, applications linking against libotf will get the right libotf, and openmpi will not accidentally be installed to satisfy the need for libotf.

Several components provided by the rdma packages have been upgraded to newer upstream versions that provide a number of bug fixes and enhancements. The following components have been upgraded: infiniband-diags, libmlx4, libmlx5, libibverbs, libibverbs-utils, librdmacm, librdmacm-utils, ibutils, libibmad, libibumad, libipathverbs, libmthca, infiniband-diags, libibcommon, mstflint, mvapich2, openmpi, opensm,

osu-micro-benchmarks, perftest, qperf, and srptools. (BZ#1053488, BZ#1087968, BZ#1093468, BZ#1087968, BZ#1053500, BZ#1051290, BZ#1051211, BZ#1055654, BZ#1053391, BZ#1059093, BZ#1056662, BZ#1059093, BZ#1059094, BZ#1059095, BZ#102730, BZ#1082730)

In addition, this update adds the following

Enhancements

BZ#854655

This update adds XRC support to InfiniBand stack and ConnectX devices from the libibverbs package.

BZ#1005352

This update adds support for the InfiniBand specification to the openmpi package.

BZ#1080183

This update adds a libocrdma package that provides a device-specific userspace driver for Emulex One Command RoCE Adapters to be used with the libibverbs library.

BZ#1091537, BZ#1100557, BZ#1130083

This update adds the mpich package that provides a high-performance and widely portable implementation of the MPI standard (MPI-1, MPI-2 and MPI-3).

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

8.196. REDHAT-RELEASE-SERVER

8.196.1. RHBA-2014:1405 — redhat-release-server bug fix and enhancement update

An updated redhat-release-server package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The redhat-release-server package contains the Red Hat Enterprise Linux Server release file.

This updated redhat-release-server package reflects changes made for the release of Red Hat Enterprise Linux 6.6.

Users of Red Hat Enterprise Linux 6 are advised to upgrade to this updated redhat-release-server package.

8.197. REDHAT-SUPPORT-LIB-PYTHON

8.197.1. RHBA-2014:1590 — redhat-support-lib-python and redhat-support-tool update

Updated redhat-support-lib-python and redhat-support-tool packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

The redhat-support-lib-python package provides a Python library that developers can use to easily write software solutions that leverage Red Hat Access subscription services.

The redhat-support-tool utility facilitates console-based access to Red Hat's subscriber services and gives Red Hat subscribers more venues for accessing the content and services available to them as Red Hat customers. Further, it enables Red Hat customers to integrate and automate their helpdesk services with our subscription services.

This update fixes the following bugs:

Bug Fixes

BZ#1054445

When the debuginfo packages had not been already installed, the "btextract ./vmcore" command did not work. As a consequence, the redhat-support-tool utility ran but did not install the debuginfo packages. The non-interactive mode of btextract has been fixed to download kernel debug symbols when they are needed, and redhat-support-tool now installs the debuginfo packages as intended.

BZ#1036921

When the "redhat-support-tool getcase [case-number]" command was issued, the "Version" field was not displayed in the Case Details section. A patch has been provided to fix this bug, and the product version now shows when viewing case details.

BZ#1060916

Prior to this update, the redhat-support-tool diagnose feature did not work on simple oops messages or RIP strings from kernel crashes. In addition, redhat-support-tool results differed from the results returned by the respective API. With this update, diagnostics for simple oops messages and RIP strings from kernel crashes have been improved. As a result, the redhat-support-tool diagnose [oops.txt] command points at the same article as the API "Diagnose" button does, and a simple RIP.txt file pulls up the same articles as putting the RIP on the sfdc search bar.

BZ#1036711

Due to poor logging in the kernel download code, non-root users were not informed about lacking the necessary root privileges to download kernel debug symbols. To fix this bug, logging which explains that root privileges are required to execute findkerneldebugs and getkerneldebug commands has been added. In addition, the help for these two commands has been expanded to indicate that root privileges are required. Now, the non-root user has a better indication of which commands require root permissions.

The redhat-support-tool utility facilitates console-based access to Red Hat's subscriber services and gives Red Hat subscribers more venues for accessing the content and services available to them as Red Hat customers. Further, it enables Red Hat customers to integrate and automate their helpdesk services with our subscription services.

In addition, this update adds the following

Enhancement

BZ#1036699

Issues such as low disk space or connectivity problems can cause the downloading of kernel debug symbols from Red Hat Network to fail. Nevertheless, the user was not informed properly about the cause of this failure. With this update, error messages are returned explaining why the kernel debug

symbols failed to download.

Users of redhat-support-lib-python and redhat-support-tool are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

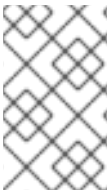
8.198. RESOURCE-AGENTS

8.198.1. RHBA-2014:1428 — 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.

This update also fixes the following bugs:



NOTE

The resource-agents packages have been upgraded to upstream version 3.9.5, which provides a number of bug fixes and enhancements over the previous version. (BZ#993431)

This update also fixes the following bugs:

Bug Fixes

BZ#1025909

Previously, the IPaddr2 agent did not send out unsolicited neighbor advertisements to announce a link-layer address change. Consequently, floating IPv6 addresses, which require this functionality, could not work correctly. To fix this bug, the "send_ua" internal binary required for IPaddr2 agent to drive IPv6 addresses has been added. As a result, the floating IPv6 addresses now work correctly. Nevertheless, IPv4 addresses are left unaffected by this change.

BZ#1025504

Previously, when an oracledb.sh resource was created without the "listener_name" option, the rgmanager oracledb resource agent failed to start. With this update, the oracledb.sh file has been modified to operate correctly when no "listener_name" is given, and thus oracledb now starts correctly.

BZ#1024065

Prior to this update, the netfs agent could become unresponsive during a stop operation, even with the "self_fence" option enabled. With this update, the self fence operation is executed sooner in the process, which ensures that NFS client detects server leaving if umount can not succeed, and self fencing occurs.

BZ#1054327

Previously, the virtual machine (VM) instances managed by the VirtualDomain agent failed during the monitor operation if the libvirtd daemon was not available. This caused the Pacemaker resource manager to unnecessarily recover healthy VM resources when libvirtd failed. With this update, the

VirtualDomain agent is capable of monitoring KVM virtual machines without requiring libvirtd to be accessible. As a result, Pacemaker no longer mismanages VM resources in case of a libvirtd failure.

BZ#993329

Previously, the "no_unmount" functionality was missing in the netfs.sh file. Consequently, the netfs resource agent did not allow an NFS share to remain mounted after a service was relocated. This update adds back the missing functionality, and the file system is now left mounted when the service relocates.

BZ#1022793

The following agents were shipped in error, and thus have now been dropped: nginx, rsyslog, mysql-proxy, and slapd.

BZ#1023340

Previously, the SAPInstance resource agent for Pacemaker did not behave correctly on nodes where the corosync node name did not match the host name. The check provided by the sapinstance_notify() function has been modified to fix this bug. The SAPInstance agent now works correctly regardless of the match between the corosync node name and host name.

BZ#1091101

Previously, Pacemaker's nfsserver resource agent was unable to properly perform NFSv3 network status monitor (NSM) state notifications. As a consequence, NFSv3 clients could not reclaim file locks after server relocation or recovery. This update introduces the nfsnotify resource agent, thanks to which NSM notifications can be sent correctly, thus allowing NFSv3 clients to reclaim file locks.

The resource-agents packages have been upgraded to upstream version 3.9.5, which provides a number of bug fixes and enhancements over the previous version. (BZ#993431)

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

8.199. RGMANAGER

8.199.1. RHBA-2014:1586 — rgmanager bug fix and enhancement update

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

The rgmanager packages contain the Red Hat Resource Group Manager, which is used to create and manage high-availability server applications in the event of system downtime.

Bug Fixes

BZ#952729

When moving services around a cluster, it was not possible to refer to virtual machines without the "vm:" prefix. With this update, the virtual machines can be controlled both with and without the "vm:" prefix.

BZ#1812079

When a custom resource agent was configured without the primary attribute, the rgmanager utility terminated unexpectedly with a segmentation fault. The underlying source code has been modified to address this bug, and an error is logged instead of the crash of rgmanager in the described scenario.

BZ#1033162

Previously, the rg_test utility did not handle exit codes correctly; when rg_test failed, the zero exit code was returned instead of a non-zero exit code. This update applies a patch to fix this bug and if rg_test crashes, the zero exit code is returned as expected.

BZ#1036652

When the "time_t" values were not configured correctly in the cluster.conf file, the rgmanager could terminate unexpectedly. This update provides a patch to fix this bug, and rgmanager now properly handles the incorrectly configured values.

BZ#1053739

When more instances were configured for a resource address than were specified with the "maxinstances" attribute, no message was logged. With this update, a warning is returned in such a case.

In addition, this update adds the following

Enhancement

BZ#982820

When a resource start or status operation failed to execute due to resource starvation on the node, the user had to reboot the node manually. With this enhancement, a new reboot_on_pid_exhaustion flag has been added. The flag allows to set up rgmanager to reboot the node automatically in the described scenario.

Users of rgmanager are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.200. RHN-CLIENT-TOOLS

8.200.1. RHBA-2014:1537 — rhn-client-tools bug fix update

Updated rhn-client-tools packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

Red Hat Network Client Tools provide programs and libraries that allow a system to receive software updates from Red Hat Network.

Bug Fixes

BZ#873784

Previously, when specifying multiple server URL values in the /etc/sysconfig/rhn/up2date config file and the string did not end with a semicolon character, the last server URL value could not be used by Yum. With this update, Yum can use all valid URL values even if the string does not end with a semicolon.

BZ#1019184

Several translation errors for the ko_KR, pt_BR, ru_RU, and zh_CN locales have been corrected.

Users of rhn-client-tools are advised to upgrade to these updated packages, which fix these bugs.

8.201. RICCI

8.201.1. RHBA-2014:1539 — ricci bug fix and enhancement update

Updated ricci packages that fix several bugs and add two enhancements 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#996195

When starting a cluster with the "ccs --start[all]" command or stopping a cluster with the "--stop[all]" command, resources were enabled or disabled automatically. Consequently, if the user wanted a cluster service to start on startup, a cluster could not be started without enabling the service. This update adds "--nodisable" and "--noenable" flags to allow users to start a cluster without enabling or disabling the services on the node. As a result, the user can stop and start nodes on a cluster without affecting their startup services.

BZ#1025053

Previously, the user was unable to configure UID and GID entries for the corosync utility in the cluster.conf file. As a consequence, the user could not configure access to corosync with the User Manager GUI. With this update, "--setuidgid" and "--rmuidgid" options have been added to the ccs utility, which can configure UID and GID entries.

BZ#1090642

Prior to this update, the ccs utility did not properly dispose of temporary files created when editing the cluster.conf file locally with the "-f" option. Consequently, a large number of temporary files could be left in the temporary directory. With this update, ccs properly removes temporary files it creates, and the file system temporary directory no longer fills up with a large number of files if multiple ccs commands using the "-f" option are executed.

BZ#1044122

Due to a bug in the design of the reboot_now.xml file and persisting state of the task batch, the ricci daemon could cause an unintentional reboot loop and unnecessary clutter in the directory with batches. This update fixes the task scheduling before reboot and addresses the problem with stale files. As a result, ricci no longer causes reboot loops and no longer leaves stale files from finished batch processing behind needlessly.

In addition, this update adds the following

Enhancements

BZ#1055424

The cluster schema in the ricci packages, used by the ccs utility for offline validation, has been updated. This update includes new options in resource and fence agents packages, and in the rgmanager utility and fenced cluster daemons.

BZ#917809

As users use CCS on the local node most frequently, the "ccs -h localhost [command]" command has been shortened to "ccs [command]".

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

8.202. RP-PPPOE

8.202.1. RHEA-2014:0424 — rp-pppoe enhancement update

Updated rp-pppoe packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The rp-pppoe packages provide the Roaring Penguin PPPoE (Point-to-Point Protocol over Ethernet) client, a user-mode program that does not require any kernel modifications. This client is fully compliant with RFC 2516, the official PPPoE specification.

Enhancement

BZ#1009268

In Red Hat Enterprise Linux 6, the adsl-setup script in the rp-pppoe packages was renamed to pppoe-setup. To assist users migrating from Red Hat Enterprise Linux 5 to Red Hat Enterprise Linux 6, a symbolic link has been created to allow the old script name to continue to work.

Users of rp-pppoe are advised to upgrade to these updated packages, which add this enhancement.

8.203. RRDTOOL

8.203.1. RHBA-2014:0356 — rrdtool bug fix update

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

The round robin database (RRD) system stores and displays time-series data, such as network bandwidth, machine-room temperature, and server load average. RRDtool is a high performance data logging and graphing utility, which can be easily integrated with shell scripts, or used to create applications using its Perl, Python, Ruby, Lua, Tcl, and PHP bindings. The data is stored in a compact manner that does not expand over time, and RRDtool provides the user with useful graphs by processing the data to enforce a certain data density.

Bug Fix

BZ#914688

Prior to this update, the RRDtool utility did not reduce data after the "fetch" operation. Consequently, some data could not be plotted or processed under certain circumstances. With this update, the data is reduced to at least the chart resolution after the "fetch" operation, and all the data is now plotted or processed as expected in the described scenario.

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

8.204. RSH

8.204.1. RHBA-2014:0795 — rsh bug fix update

Updated rsh packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The rsh packages contain programs which allow users to run commands on remote machines, log in to other machines, copy files between machines (rsh, rlogin and rcp), and provide an alternate method of executing remote commands (rexec). All of these programs are run by the xinetd daemon and can be configured using the Pluggable Authentication Modules (PAM) system and configuration files in the /etc/xinetd.d/ directory.

Bug Fixes

BZ#749283

Previously, the rshd daemon performed redundant calls of the setpwent() and endpwent() functions. As a consequence, rshd queried Network Information Security (NIS) servers on every remote shell (rsh) access. With this update, these redundant calls have been removed and rshd no longer contacts NIS servers unnecessarily.

BZ#802367

Prior to this update, the maximum number of command line arguments for the rsh application was not limited. However, the volume of data buffer allocated to the arguments is always finite. Consequently, rshd terminated unexpectedly when it attempted to allocate the buffer to commands with a vast number of arguments. This update implements a limit for command-line arguments in rsh, and the described rshd crash no longer occurs.

BZ#1098955

Previously, the pam_close_session() function was not called when a remote copy (rcp) connection completed. As a consequence, the PAM session did not terminate correctly. With this update, pam_close_session() is called and the PAM session terminates as intended.

BZ#1094360

Prior to this update, the rsh application was optimized through strict aliasing rules, even though it is not a performance-sensitive application. As a consequence, the GNU compiler collection (GCC) generated warning messages about breaking the strict-aliasing rules, despite correct functionality being the priority for rsh. With this update, strict aliasing has been disabled for rsh. Therefore, GCC now ignores the strict aliasing rules and no longer interrupts rsh processes with warning messages. However, this may also lead to a slight decrease in performance.

Users of rsh are advised to upgrade to these updated packages, which fix these bugs.

8.205. RSYNC

8.205.1. RHBA-2014:0451 — rsync bug fix update

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

The rsync tool is used to copy and synchronize files locally or across a network. The rsync tool works very fast because it uses delta encoding and sends just differences in files instead of whole files. Also, rsync can be used as a powerful mirroring tool.

Bug Fix

BZ#981797

Previously, the rsync tool changed the file ownership after, not before, setting security attributes. As a consequence, the security attributes on the target were missing, and running the "rsync -X" command did not work correctly under certain circumstances. With this update, the order of the operations has been switched, and rsync now changes the ownerships before setting the security attributes. As a result, the security attributes are present as expected in the described situation.

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

8.206. RUBY

8.206.1. RHBA-2014:1470 — ruby bug fix and enhancement update

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

Ruby is an extensible, interpreted, object-oriented scripting language. It has features to process text files and to do system management tasks.

This update also fixes the following bugs:

NOTE

The ruby package has been upgraded to upstream version 1.8.7, which provides a number of bug fixes and enhancements over the previous version. (BZ#830098)

This update also fixes the following bugs:

Bug Fixes

BZ#784766

The Tracer module introduced with SystemTap probes in a previous release of the ruby package collided with native Tracer class implemented in Ruby. Consequently, when using Ruby with debugger or tracer, the following exception was raised:

/usr/lib/ruby/1.8/tracer.rb:16: Tracer is not a class (TypeError)

With this update, the Tracer module has been renamed to SystemTap, or DTrace alternatively. To apply this fix, instances of the Tracer.fire method should be changed to SystemTap.fire or DTrace.fire in previously written Ruby code.

BZ#802946

Prior to this update, ruby failed to start a SSL server in FIPS mode due to usage of a forbidden MD5 algorithm. With this update, MD5 has been replaced by SHA256, thus fixing this bug.

BZ#997886, BZ#1033864

Due to changes in OpenSSL configuration options, the ruby package was not compatible with builds of OpenSSL that have enabled support for Elliptic Curve Cryptography (ECC) introduced in Red Hat Enterprise Linux 6. Consequently, ruby failed to build. This update enables ECC support in Ruby, thus fixing the build problem.

The ruby package has been upgraded to upstream version 1.8.7, which provides a number of bug fixes and enhancements over the previous version. (BZ#830098)

All ruby users are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

8.207. S390UTILS

8.207.1. RHBA-2014:1546 — 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 that should be used together with the zSeries (s390) Linux kernel and device drivers.

Bug Fixes

BZ#1009897

Due to incorrect order of initialization, Anaconda failed to detect the presence of the zSeries Linux fibre-channel adapter (zFCP) disks. To fix this bug, the cio_settle kernel interface has been implemented, which waits for the zFCP devices to become online. Now, Anaconda detects the zFCp devices as intended.

BZ#1016181

For each possible CPU, the zfcpdump kernel consumed all memory for the per-CPU data structures. Because only 32 MB are available for zfcpdump, zfcpdump could run out of memory. This update adds a new kernel parameter "possible_cpus=1", and the zfcpdump system no longer runs out of memory.

BZ#1020364

Previously, when the "fdasd -c" command was called with a configuration file that contained only one parameter for a partition, the fdasd daemon terminated unexpectedly with a segmentation fault during configuration file parsing. This update adds a new function to parse configuration file lines, and fdasd no longer crashes in the described situation.

BZ#1094376

Previously, removing a device that was currently offline resulted in an error. The znetconf protocol has been fixed to handle removal of an offline ccwgroup devices correctly, and the "znetconf -r" command now removes a currently offline device as intended.

BZ#1107779

The output of the lsqeth command depends on the presence of a file named "?". Due to a bug in the grep command regular expression (regex), the system qeth devices failed to be detected when a file named "?" was present in the current working directory. To fix this bug, the regex argument of grep

has been put in single quotes, and the system qeth devices are now detected successfully.

BZ#1109898

Due to incomplete dependencies specified in the s390utils packages, various command-line tools did not work when invoked or gathered incomplete data. This update adds the missing dependencies to the tools, which now work as expected.

In addition, this update adds the following

Enhancements

BZ#1017854, BZ#1031143, BZ#1032061, BZ#1088328

With this update, various information gathered by the dbginfo.sh utility has been expanded, along with the relevant manual page.

BZ#1053832

This update introduces a new interface that enables Linux applications such as Data Stage to access and process read-only data in physical sequential data sets owned by IBM System z without interfering with System z. By avoiding FTP or NFS transfer of data from System z, the turnaround time for batch processing is significantly reduced.

Users of s390utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

8.208. SAMBA

8.208.1. RHBA-2014:1372 — samba bug fix and enhancement update

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

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 samba packages have been upgraded to upstream version 3.6.23, which provides a number of bug fixes and enhancements over the previous version. The notable changes are:

- The format of the Trivial Database (TDB) files has been updated. The files are upgraded as soon as the new version of the **smbd** daemon is started. Note that it is not possible to downgrade to an older Samba version without backups of the old TDB files.

- Printing subsystem TDB files, such as **ntprinting.tdb**, **ntforms.tdb**, **ntdrivers.tdb**, for old versions of Samba may contain non-UTF-8 strings in Latin-1 or other 8-bit encodings. When updating to Samba 3.6 these files have to be migrated to the new registry-based printing management. The migration has to be done manually because there is no information about the charset encoding in the files. To do so, specify the correct code page for the conversion. Use the **iconv -l** command to list the available code pages. The mostly used one is Windows encoding corresponding to Latin-1, named CP1252.

- The **net printing dump** and **net printing migrate** commands were extended to define the new encoding of the TDB files. As a result, it is possible to view the files with the **net printing dump encoding=CP1252/path/to/ntprinters.tdb** command or migrate them with the **net printing migrate encoding=CP1252 /path/to/ntprinters.tdb** command. When migrating printers, Red Hat suggests to do so in the following order:

  1. **ntforms.tdb**
  2. **ntdrivers.tdb**
  3. **ntprinting.tdb**

  Note that the migration has to be done when the Samba processes are shut down and that after migration it is needed to rename, move, or delete the files in the **/var/lib/samba/** directory. (BZ#1003921)

Bug Fixes

BZ#1021706

The **%G** substitution character in certain variables did not resolve into a name. As a consequence, **%G** was replaced by the GID number and not by the group name. This update provides a patch to fix this bug and **%G** is now successfully substituted into a name.

BZ#1035332

When the user logs in as a **guest**, the guest boolean flag is attached to the user's token. When the user connected to a share with the **force user** option, this flag overrode the creation of the token for the specific share with the **force user** set, ensuring that the user had only the guest access. Consequently, files were created as the **nobody** user. With this update, the guest flag is set under a **force user** share only when the user name being mapped to was the same as the **guest** user. As a result, the files are created as the specified user.

BZ#1053886

The function that is used to authenticate the user did not provide all information about the user. When this function was used with another call to authenticate the user over a secure channel, the field for the path to the home directory was empty. Now, the correct **DCPRC()** function is called and all required fields are filled out as expected.

BZ#1087472

The **libsmbclient** library toolset did not initialize the default configuration parameters. As a consequence, applications using **libsmbclient** terminated unexpectedly when the ***$HOME*** parameter was not properly set. With this update, the default configuration values are loaded correctly and the applications no longer crashe in the described scenario.

BZ#1096522

Due to missing support for partial data and small size of certain buffers, clients were unable to cope with the buffer size returned by the server. The missing support has been added and Samba now works as expected.

BZ#1107777

With the SMB2 and SMB3 protocols, the **filenama_convert()** function was not called on the full path, which caused that the last component of the path was not normalized. Consequently, listing of large directories did not work correctly with SMB2 and SMB3. This bug has been fixed and large directories can be listed properly.

Enhancements

BZ#1081539, BZ#1099693

A timeout option has been added to the **smbclient** command-line utility. This allows users to customize the timeout value for Samba file operations.

BZ#1129006

It is now possible to set a different OS version for the Printing subsystem (**spoolss**) configuration. This allows users to work around situations where printing drivers do not interact with the printing server because they detect that its version is too old.

Users of samba are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. After installing this update, the **smb** service will be restarted automatically.

8.209. SAMBA4

8.209.1. RHBA-2014:1605 — samba4 bug fix update

Updated samba4 packages that fix one bug are now available for Red Hat Enterprise Linux 6.

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.

Users of samba4 are advised to upgrade to these updated packages, which fix this bug. After installing this update, the smb service will be restarted automatically.

8.210. SAPCONF

8.210.1. RHBA-2014:1424 — sapconf bug fix update

Updated sapconf package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The sapconf package contains a script that checks the basic installation of Red Hat Enterprise Linux and modifies it according to SAP requirements. The script ensures that all necessary packages are installed and that configuration parameters are set correctly to run SAP software.

Bug Fixes

BZ#1024356

In certain situations, the sapconf script created the /etc/hosts file in an incorrect format, thus the file did not return the fully qualified domain name (FQDN). As a consequence, SAP installation failed unexpectedly. With this update, the script has been edited to handle situations when the incorrect /etc/hosts file was created. In addition, when FQDN is not returned properly, the script exits with the error code 4.

BZ#1025187

Previously, the manual page for the sapconf script was missing. This update adds the missing manual page to the sapconf package.

BZ#1040617

Due to a bug in the underlying source code, the sapconf script was unable to verify if a virtual guest was a VMware guest. Consequently, an attempt to use sapconf on such a guest failed. With this update, sapconf recognizes the VMware guests as expected.

BZ#1051017

The order of reading limit files in Red Hat Enterprise Linux is as follows: First is read the /etc/security/limits.conf file and then the limit files located in the /etc/security/limits.d/ directory according to the C localization functions. When an entry is specified in two or more files, the entry that is read last takes effect. Previously, the sapconf script wrote entries to /etc/security/limits.conf, which could cause the sapconf entries to be overwritten by the same entries in files located in /etc/security/limits.d/. With this update, a separate sapconf limit file has been added to /etc/security/limits.d/ to anticipate this bug.

BZ#1083651

When the sapconf script updated the /etc/hosts file, permissions of that file were incorrectly modified. This update applies a patch to fix this bug, and sapconf no longer overwrites the file's permissions.

Users of sapconf are advised to upgrade to this updated package, which fixes these bugs.

8.211. SCRUB

8.211.1. RHBA-2014:1493 — scrub bug fix and enhancement update

Updated scrub packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 6.

Scrub writes patterns on files or disk devices to make retrieving the data more difficult. It is a program for erasing disks.

Bug Fix

BZ#903890

When the "scrub -X" command was executed, it rewrote free space on given disk partition but failed to remove files created during this process. As a consequence, the respective file system remained full after this process. With this update, the newly created files are removed, and the file system regains the free space.

In addition, this update adds the following

Enhancement

BZ#907173

With this update, the new "-E" option has been added to scrub, which has the ability to scrub only used blocks of a sparse file. This option is especially useful in combination with large sparse files, as it skips the holes in the sparse file. Nevertheless, use this option with caution, as the result may not be compliant with cited standards and information about the actual on-disk data allocation may leak since only the allocated parts will be scrubbed.

Users of scrub are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

8.212. SCSI-TARGET-UTILS

8.212.1. RHBA-2014:1599 — scsi-target-utils bug fix update

Updated scsi-target-utils packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The scsi-target-utils packages contain a daemon and utilities to setup Small Computer System Interface (SCSI) targets. Currently, software Internet SCSI (iSCSI) and iSCSI Extensions for RDMA (iSER) targets are supported.

Bug Fixes

BZ#848585

Previously, the tgtadm SCSI target administration utility did not correctly handle backing-store errors. As a consequence, calling tgtadm with an invalid backing-store parameter in some cases caused the tgtd service to become unresponsive. With this update, the bug in tgtadm has been fixed, and tgtd now recovers from an invalid request as intended.

BZ#854123

Prior to this update, tgtadm failed to handle setting a device to pass-through mode. As a consequence, calling tgtadm with the device-type option set to "passthrough" caused tgtd on the server side to terminate unexpectedly with a segmentation fault. A patch has been applied to fix this bug, and tgtadm no longer crashes in the described scenario.

BZ#865960

Prior to this update, running the "tgtadm --mode target --op show" command did not return the complete number of targets if many targets were present on the system. Consequently, tgtadm could show incorrect and also inconsistent results, because the displayed number of targets varied over repeated attempts. A patch has been applied to fix this bug. Running "tgtadm --mode target --op show" now shows all the targets correctly even on systems with a large amount of targets.

BZ#1094084

Previously, scsi-target-utils did not support the "WRITE and VERIFY (10)" SCSI command which is used by the AIX operating system. As a consequence, AIX failed to execute the mkvg command when the user tried to add iSCSI targets to the system. With this update, the support for "WRITE and VERIFY (10)" has been added, and scsi-target-utils now provide iSCSI targets to AIX as expected.

BZ#1123438

Previously, tgtd could experience a buffer overflow due to incorrect usage of the snprintf() function in the source code. As a consequence, tgtd terminated unexpectedly when trying to respond to a tgtadm query about a large number of connections. The source code has been updated to avoid the buffer overflow, and using tgtadm to display a large number of connections no longer causes tgtd to crash.

Users of scsi-target-utils are advised to upgrade to these updated packages, which fix these bugs. All running scsi-target-utils services must be restarted for the update to take effect.

8.213. SELINUX-POLICY

8.213.1. RHBA-2014:1568 — selinux-policy bug fix and enhancement update

Updated selinux-policy packages that fix multiple bugs and add various enhancements 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 Fixes

BZ#1062384

SELinux prevented the qemu-guest-agent process from executing the settimeofday() and hwclock() functions. Consequently, qemu-guest-agent was unable to set the system time. A new rule has been added to the SELinux policy and qemu-guest-agent can now set the time as expected.

BZ#1082640

Previously, SELinux did not allow the dhcpd daemon to change file ownership on the system. As a consequence, the ownership of files that dhcpd created was changed from the required dhcpd:dhcpd to root:root. The appropriate SELinux policy has been changed, and dhcpd is now able to change the file ownership on the system.

BZ#1097387

Due to the missing miscfiles_read_public_files Boolean, the user could not allow the sshd daemon to read public files used for file transfer services. The Boolean has been added to the SELinux policy, thus providing the user the ability to set sshd to read public files.

BZ#1111538

Due to a missing SELinux policy rule, the syslog daemon was unable to read the syslogd configuration files labeled with the syslog_conf_t SELinux context. With this update, the SELinux policy has been modified accordingly, and syslog now can read the syslog_conf_t files as expected.

BZ#1111581

Due to an insufficient SELinux policy rule, the thttpd daemon ran in the httpd_t domain. As a consequence, the daemon was unable to change file attributes of its log files. The SELinux policy has been modified to fix this bug, and SELinux no longer prevents thttpd from changing attributes of its log files.

BZ#1122866

Previously, SELinux did not allow the sssd daemon to write to the krb5 configuration file, thus the daemon was unable to make any changes in krb5. The SELinux policy has been changed with this update, and sssd can now write to krb5.

BZ#1127602

Due to a missing SELinux policy rule, the Samba daemons could not list the /tmp/ directory. The SELinux policy has been modified accordingly, and SELinux no longer prevents the Samba daemons from listing the /tmp/ directory.

In addition, this update adds the following

Enhancement

BZ#1069843

With this update, new SELinux policy rules have been added, and the following services now run in their own domains, not in the initrc_t domain:

thttpd

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

8.214. SERVICELOG

8.214.1. RHBA-2014:1443 — servicelog bug fix and enhancement update

Updated servicelog packages that fix several bugs and add various enhancements are now available.

The servicelog packages provide a relational database to help manage errors on IBM eServer System p machines. Firmware and device driver errors are logged and managed using this database, which provides advanced error management capabilities.

NOTE

The servicelog packages have been updated to upstream version 1.1.12, which includes several minor bug fixes and adds support for handling platform dependencies like the PowerVM guest or BE guest. (BZ#739119, BZ#1088404)

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

8.215. SG3_UTILS

8.215.1. RHBA-2014:1601 — sg3_utils bug fix update

Updated sg3_utils packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The sg3_utils packages contain a collection of tools for SCSI devices that use the Linux SCSI generic (sg) interface. This collection includes utilities for database copying based on "dd" syntax and semantics (the "sg_dd", "sgp_dd" and "sgm_dd" commands), INQUIRY data checking and associated pages ("sg_inq"), mode and log page checking ("sg_modes" and "sg_logs"), disk spinning ("sg_start") and self-tests ("sg_senddiag"), as well as other utilities. It also contains the rescan-scsi-bus.sh script.

Bug Fix

BZ#857200

When a Logical Unit Number (LUN) was resized on a target side, the rescan-scsi-bus.sh script failed to resize SCSI devices on the host side. This update applies a patch to fix this bug and when an LUN is resized on the target side, the change is propagated to the host side as expected.

Users of sg3_utils are advised to upgrade to these updated packages, which fix this bug.

8.216. SGML-COMMON

8.216.1. RHBA-2014:0540 — sgml-common bug fix update

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

The sgml-common packages contain a collection of entities and document type definitions (DTDs) that are useful for processing Standard Generalized Markup Language (SGML), but do not need to be included in multiple packages. The sgml-common packages also include an up-to-date Open Catalog file.

Bug Fix

BZ#613637

Prior to this update, the licensing COPYING file and documentation was missing from the xml-common subpackage. This update adds the missing basic documentation and COPYING file to xml-common.

Users of sgml-common are advised to upgrade to these updated packages, which fix this bug.

8.217. SHADOW-UTILS

8.217.1. RHBA-2014:1522 — shadow-utils bug fix update

Updated shadow-utils packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The shadow-utils packages include programs for converting UNIX password files to the shadow password format, as well as utilities for managing user and group accounts.

Bug Fixes

BZ#787742

Previously, pwconv and grpconv utilities improperly parsed respective shadow and gshadow files with errors. Consequently, when writing corrected shadow and gshadow files, only the first error on two consecutive erroneous lines was corrected. With this update, pwconv and grpconv parse the files with errors correctly, and all lines are corrected in the newly written files.

BZ#890222

Due to a bug in code parsing in the /etc/group file, the useradd command could terminate unexpectedly with a segmentation fault when merging group entries. The parsing code has been fixed, and useradd now correctly merges group entries.

BZ#955769

Previously, the useradd command assigned the SELinux user to the new user being created after creating and populating the home directory of the user. Consequently, the SELinux contexts of the home directory files were incorrect. With this update, the SELinux user is assigned to the newly created user before populating the home directory, and the SELinux contexts on the home directory files for newly created users are now correct.

BZ#956742

Due to improper detection of invalid date specification in the chage command, chage did not fail when used with invalid date specification. With this update, the code of chage properly detects invalid date specification, and fails if an invalid date is specified.

BZ#957782

Prior to this update, the chage command incorrectly handled date in the format of "[month] DD YYYY" as "[month] DD hhmm". As a consequence, if chage was used with such date specification, the date was set to an unexpected value. The updated chage code correctly handles date in the aforementioned format. As a result, if chage is used with such date specification, the date is set to an expected value.

BZ#993049

Previously, the newgrp command always tried to find a group with a matching group ID (GID) within all the groups on the system. If the groups were stored on the LDAP server, it caused large data to be pulled from the LDAP server on each invocation of newgrp. The underlying source code has been fixed, and newgrp no longer tries to find a matching group among all the groups on the system if the user is a member of the group specified on the command line. Thus no extra data is pulled from the LDAP server.

BZ#1016516

The usermod code handled improperly the creation of a new entry in the /etc/shadow file. As a consequence, the "usermod -p" command failed to set the new password if the entry in the /etc/shadow file was missing. The updated usermod code properly creates a new entry in /etc/shadow if it is missing, and the "usermod -p" command sets the new password correctly even if the user's entry in /etc/shadow is missing.

Users of shadow-utils are advised to upgrade to these updated packages, which fix these bugs.

8.218. SHARED-MIME-INFO

8.218.1. RHBA-2014:0555 — shared-mime-info bug fix update

Updated shared-mime-info packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The shared-mime-info packages contain the core database of common types. Programs and desktops consult the MIME database to determine the correct MIME type for a file.

Bug Fix

BZ#974505

Due to optimizations performed by the Anaconda installer, the glib2 packages, which the shared-mime-info packages depend on, were not yet installed when the shared-mime-info's post-installation script was run. As a consequence, a harmless error message was reported. This update adds an explicit dependency on glib2 for the post-installation script to only run after the glib2 packages have been installed, and the errors no longer occur in the described situation.

Users of shared-mime-info are advised to upgrade to these updated packages, which fix this bug.

8.219. SLAPI-NIS

8.219.1. RHBA-2014:1583 — slapi-nis bug fix update

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

The slapi-nis packages contain the NIS server plug-in and the Schema Compatibility plug-in for use with the 389 directory server.

Bug Fixes

BZ#1039942

Prior to this update, the NIS Server plug-in did not release memory that was used to hold a decoded client request. Consequently, the directory server used an excessive amount of memory as it processed more requests from NIS clients. The bug has been fixed and thus no longer causes memory leaks on the directory server.

BZ#1056648

Due to a bug in slapi-nis plug-in behavior, modifying a directory server entry, such as disabling sudo rules, did previously not correctly add or remove the corresponding NIS map entry or compatibility entry. As a consequence, the intended changes to configuration failed to take effect. With this update, slapi-nis plug-ins notice the configuration changes as expected and update their data accordingly.

Users of slapi-nis are advised to upgrade to these updated packages, which fix these bugs.

8.220. SOS

8.220.1. RHBA-2014:1528 — sos bug fix and enhancement update

An updated sos package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The sos package contains a set of utilities that gather information from system hardware, logs, and configuration files. The information can then be used for diagnostic purposes and debugging.

Bug Fixes

BZ#1001600

Depending on site-local configuration, large quantities of System Activity Reporter (SAR) data could be present on systems. Previous versions of the sos utility attempted to collect all data present, potentially leading to very large report sizes and slow data collection. This update applies a size limit to both binary and text data captured by the SAR module, and SAR data in the report are now limited to 20 MB by default. In addition, a new "all_sar" option has been added to the module to request the old behavior.

BZ#1041770

The sos utility makes use of the Red Hat Network Client Tools hardware module to obtain information on the hardware present in the system. However, due to the way in which the module was invoked by sos, a change in the Red Hat Network component caused errors when running the sosreport command. The sos hardware plug-in now imports the Red Hat Network module directly and stores the resulting output in the report, thus fixing the bug. Now, exceptions or other errors are no longer displayed during report processing.

BZ#1085042

Previous versions of the sos utility failed to correctly handle file system exceptions resulting from out-of-space conditions. As a consequence, running the sosreport utility with insufficient space could lead to thousands of logged errors and creation of an unusable report tarball. With this update, all I/O paths in sosreport correctly handle out-of-space and other fatal file system exceptions. Now, attempting to run sos with insufficient space results in an immediate descriptive error and the tool no longer attempts to create a report archive.

BZ#1101311

Previous versions of the sos utility did not omit passwords or password hashes in the grub.conf bootloader configuration file. Consequently, passwords or password hashes contained in these files could be disclosed to the recipient of an sos report archive. The sos utility now removes passwords and password hashes from grub.conf, and the generated report archive no longer contains password material.

In addition, this update adds the following

Enhancements

BZ#961041

With this update, the sos package includes support for the Samba Clustered Trivial Database (CTDB), clustered implementation of the TDB used by Samba. Users can now require information on the CTDB state and configuration to diagnose problems in clustered Samba deployments.

BZ#1005703

Depending on system configuration and fault state, some commands can become blocked indefinitely causing the sos utility to appear unresponsive. With this update, the sosreport utility applies a timeout when running all external commands, so that commands that become blocked for an excessive

period now terminate with a timeout and no longer cause the main sos process to hang.

BZ#1039755

Previous versions of the sos utility did not capture diagnostic data for OpenShift Node and Broker installations. With this update, configuration and state information is collected on applicable systems.

BZ#1052344

Previously, information related to failed upgrades was not collected by the sosreport command. With this update, attempted upgrades leave diagnostic data in the host file system that can assist in determining the cause of the upgrade problem.

Users of sos are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

8.221. SPICE-GTK

8.221.1. RHBA-2014:1487 — spice-gtk bug fix and enhancement update

Updated spice-gtk packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 6.

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.

This update also fixes the following bugs:

NOTE

The spice-gtk packages have been upgraded to upstream version 0.22, which provides a number of bug fixes over the previous version. (BZ#1097338)

This update also fixes the following bugs:

Bug Fixes

BZ#871034

Previously, for SSL connections, a connection was considered successful if the certificate subject matched the host name even if a non-matching user-specified host certificate subject was provided. Consequently, a remote-viewer client could connect to the remote host even if the certificate subject did not match. With this update, the certificate subject check has a priority over the host name check, and connections now fail if user-specified certificate subject does not match.

BZ#1017860

Prior to this update, protocol version fallback was broken. As a consequence, the user could not connect to spice guests on Red Hat Enterprise Linux 5 servers. The protocol fallback has been fixed, and the user is again able to connect to spice guests on Red Hat Enterprise Linux 5 servers.

BZ#1019797

Previously, the virt-viewer utility was unable to handle large copy and paste operations; if a very large amount of text was copied, the mingw-virt-viewer utility displayed a failure to allocate memory for extensive data. This bug has been fixed, and up to 100 MB of data can now be copied and pasted.

BZ#1022565

When migrating a VM with a client connected via mime connection file and Secure Socket Layer (SSL), the migration fell back to a non-seamless operation, because the Certification Authority (CA) was not correctly copied from memory. With this update, the CA is now correctly copied on the destination session, and the seamless migration can now be realized.

BZ#1028637

When migrating a guest repeatedly while connected to the guest with an i686 client, the client could terminate unexpectedly with a segmentation fault. The underlying source code has been patched, and the client no longer crashes during migration.

BZ#1029765

Previously, the virt-viewer utility was taking invalid screenshots on secondary displays. The screenshot memory region for secondary displays has been fixed, and virt-viewer now creates correct screenshots.

BZ#1054757

Virt-viewer and remote-viewer utilities always scaled displays, but also allowed the user to disable display resizing, changing the resolution on the guest to match the display window size. Consequently, users could become confused as they expected different behavior. The ability for the user to disable resizing thus has been removed.

BZ#1108642

Previously, various clipboard managers operating on the client or on the guest occasionally lost synchronization, which resulted in clipboard data loss and the SPICE console freezing. Now, the spice-gtk utility has been patched so that clipboard synchronization no longer freezes the SPICE console.

The spice-gtk packages have been upgraded to upstream version 0.22, which provides a number of bug fixes over the previous version. (BZ#1097338)

In addition, this update adds the following

Enhancement

BZ#1035728

The spice-gtk utility advertises TLS 1.0 as its maximum supported TLS version. With this update, spice-gtk supports more recent TLS version provided by the openssl utility.

Users of spice-gtk are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

8.222. SPICE-SERVER

8.222.1. RHBA-2014:1435 — spice-server bug fix update

Updated spice-server packages that fix several bugs 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.

Bug Fixes

BZ#994175

Previously, the SPICE server assumed that the SPICE client was connected until it became disconnected. However, when the client became unresponsive, or did not disconnect explicitly, the server kept trying to communicate with it. Consequently, queues, such as a driver commands ring, filled up, and the guest display driver hung. With this update, the SPICE server monitors if the client is responsive and disconnect if it is not.

BZ#1004443

Previously, pending data from the client were cleaned inappropriately. As a consequence, QEMU could terminate unexpectedly when a VM was rebooting while being migrated. This update ensures that the pending client data are cleaned appropriately, and QEMU crashes no longer occur.

BZ#1035695

Prior to this update, the SPICE server used exclusively Transport Layer Security (TLS) version 1.0 for encrypted connections no matter what version(s) the client advertised. Consequently, the SPICE client could not use newer versions of TLS. To fix this bug, the SPICE server code has been changed to allow for TLS 1.0 and above, and clients can now connect using TLS version 1.0 or newer.

BZ#1072700

Due to an integer overflow on a 32 bit timer value, infinite loop in the SPICE server on long running VMs longer than 46 days caused SPICE sessions to become unresponsive. Where appropriate, 64 bit timer values are now used, and SPICE sessions no longer crash.

BZ#1086820

Due to invalid assertion in the video streaming code, the SPICE hypervisor could terminate unexpectedly when the assert was triggered. The following error message was returned in the log file:

qemu sometimes crashes in spice-server with "rate_control->num_recent_enc_frames" assertion

The invalid assertion has been fixed, and the hypervisor no longer crashes.

Users of spice-server are advised to upgrade to these updated packages, which fix these bugs.

8.223. SPICE-VDAGENT

8.223.1. RHBA-2014:1578 — spice-vdagent bug fix update

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

The spice-vdagent packages provide a SPICE agent for Linux guests.

Bug Fix

BZ#1066094

When using Eclipse within a Red Hat Enterprise Linux 6 guest in Virtual Desktop Infrastructure, the digit displaying the number of hidden tabs or within was rendered incorrectly. This bug has been fixed, and the text is now rendered normally, keeping the physical screen size to a constant 96 DPI.

Users of spice-vdagent are advised to upgrade to these updated packages, which fix this bug.

8.224. SPICE-XPI

8.224.1. RHBA-2014:1560 — spice-xpi bug fix update

Updated spice-xpi packages that fix one bug 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.

This update fix the following update:

* Due to a bug in the Red Hat Enterprise Virtualization Manager web admin portal, it was possible to open a second SPICE console, which caused the SPICE plug-in to terminate unexpectedly. With this update, the underlying source code has been modified to address this bug and the console no longer crashes in the described scenario. (BZ#1073461)

Bug Fix

BZ#1073461

Due to a bug in the Red Hat Enterprise Virtualization Manager web admin portal, it was possible to open a second SPICE console, which caused the SPICE plug-in to terminate unexpectedly. With this update, the underlying source code has been modified to address this bug and the console no longer crashes in the described scenario.

This update fix the following update:

Users of spice-xpi are advised to upgrade to these updated packages, which fix this bug. After installing the update, the Mozilla Firefox browser must be restarted for the changes to take effect.

8.225. SQUID

8.225.1. RHBA-2014:1446 — squid bug fix update

Updated squid packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.

Bug Fixes

BZ#876980

Prior to this update, the /etc/init.d/squid initialization script did not describe the condrestart option, and therefore it did not appear in the Usage message. This bug has been fixed, and condrestart is now displayed correctly in the Usage message.

BZ#998809

Under certain circumstances, the comm_write() function of the squid utility attempted to write to file descriptors that were being closed. Consequently, the squid utility was aborted. With this update, a patch that handles the write attempt has been introduced. As a result, squid is no longer aborted in the aforementioned scenario.

BZ#1011952

Due to a bug in the default /etc/httpd/conf.d/squid.conf configuration file, the squid utility was not allowed to access the CacheManager tool at http://localhost/Squid/cgi-bin/cachemgr.cgi. The bug has been fixed, and squid can now access CacheManager without complications.

BZ#1034616

Under certain circumstances, the squid utility leaked Domain Name System (DNS) queries. Consequently, squid often reached the limit of maximum locks set to 65,535 and terminated unexpectedly. With this update, several changes have been made to prevent leaked queries. Also, the lock limit has been increased to the maximum value of the integer data type.

BZ#1047839

Previously, after receiving a malformed Domain Name System (DNS) response, the squid utility terminated unexpectedly and did not start again. The underlying source code has been modified, and as a result, squid now handles malformed DNS responses without complications.

BZ#1058207

Under certain circumstances, child processes of the squid utility terminated unexpectedly and generated a core file. This bug has been fixed, and squid processes no longer exit abnormally.

BZ#1066368, BZ#1089614

Previously, the AuthBasicUserRequest method of the squid utility overrode the default user() methods with its own data. Consequently, a memory leak occurred when using basic authentication, which led to high memory consumption of squid. With this update, the aforementioned override was removed and the memory leak no longer occurs.

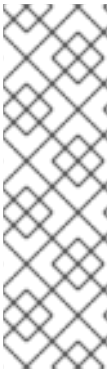
Users of squid are advised to upgrade to these updated packages, which fix these bugs. After installing this update, the squid service will be restarted automatically.

8.226. SSSD

8.226.1. RHBA-2014:1375 — sssd bug fix and enhancement update

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

The **System Security Services Daemon (SSSD)** provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides the Name Service Switch (NSS) and the Pluggable Authentication Modules (PAM) interfaces toward the system and a pluggable back-end system to connect to multiple different account sources.



NOTE

The sssd has been upgraded to upstream version 1.11, which provides a number of bug fixes and enhancements to the System Security Services Daemon (SSSD) over the previous version. These include improvements to interoperability of Red Hat Enterprise Linux clients with Active Directory, which makes identity management easier in Linux and Windows environments. The most notable enhancements also include resolving users and groups, as well as authenticating users from trusted domains in a single forest, DNS updates, site discovery, and using the NetBIOS name for user and group lookups. (BZ#1051164)

Bug Fixes

BZ#1065534

Previously, the SSSD Pluggable Authentication Module (PAM) accepted user names containing spaces before or after the name. As a consequence, users in some situations entered incorrect names at the Gnome Display Manager (GDM) login screen. With this update, the SSSD PAM ignores space characters before and after a user name, and entering them no longer complicates logging in by the GDM login screen.

BZ#1059423

Prior to this update, attempting to save a user group member who does not conform to the configured search bases caused the group to be saved with incomplete membership. Consequently, using the "id" command returned inconsistent results for user group memberships. With this update, a user group can be saved correctly even when it contains members outside of the configured search bases. As a result, "id" now returns consistent results in such a scenario.

BZ#1031807

SSSD was incorrectly able to access random data if the "ad_matching_rule" option was enabled. As a consequence, if the user configured SSSD to use the "ad_matching_rule" option with no available group members, SSSD accessed random data and terminated unexpectedly with a segmentation fault. This update prevents SSSD from accessing random data, and the described scenario no longer causes SSSD to crash.

BZ#1025813

Previously, when SSSD was configured with the "id_provider=proxy" and "auth_provider=ldap" options, the Lightweight Directory Access Protocol (LDAP) authentication code used a hard-coded filter when searching for the user. Consequently, if the LDAP server used a customized LDAP pattern for the user name, the SSSD authentication with "id_provider=proxy" and "auth_provider=ldap" failed. With this update, SSSD is able to adjust for custom LDAP user name pattern, and SSSD authentication with the mentioned options succeeds in such a situation.

BZ#1028422

Because the autofs responder did not correctly ignore the "default_domain_suffix" option, autofs maps could previously not be retrieved when "default_domain_suffix" was enabled in SSSD. With this update, "default_domain_suffix" is properly ignored in the autofs responder and autofs maps can be retrieved when this option is enabled.

BZ#1030135

Prior to this update, when two different providers, such as id_provider=ipa and sudo_provider=ldap, were configured and enumeration was enabled, SSSD incorrectly started two parallel enumeration tasks. This caused conflicts in the enumeration tasks and produced incomplete enumeration data.

With this update, SSSD only starts an enumeration task for the id_provider in the descibed scenario. As a result, enumeration data is now complete even for configurations with two different provider types.

BZ#1038098

Due to a bug in freeing used memory, running a persistent process that periodically requests a netgroup caused a memory leak. With this update, memory is freed correctly and the memory leak in the mentioned scenario no longer occurs.

BZ#1084532

Previously, SSSD could not process entries with more than 255 sudo rules. As a consequence, the sssd_sudo process under some circumstances terminated unexpectedly with a segmentation fault, which caused sudo to be unusable with SSSD for some users. This update changes the way sssd_sudo handles sending sudo rules. As a result, SSSD can now process LDAP entries with more than 255 rules and sssd_sudo no longer crashes.

BZ#1135855

Prior to this update, when using the getservent() call to retrieve information about all services, SSSD wrote the service count into an incorrect part of the output buffer. As a consequence, the "getent" command in some cases returned inaccurate information or became unresponsive. With this update, the sssd_nss code has been fixed to sort the ouput buffer properly, and "getent" now functions reliably.

BZ#1085412

Due to the asynchronous processing that SSSD uses, an LDAP connection handle was in some cases freed between obtaining the handle and using it. As a consequence, SSSD frequently terminated unexpectedly when the Storage Area Network (SAN) experienced high latency. With this update, additional NULL checks have been added for the LDAP handle and SSSD now aborts the current request instead of crashing when high latency occurs on SAN.

BZ#1092766

Previously, when using the id_provider=ad provider, the processing of user group membership was in some cases terminated prematurely for users with POSIX attributes and with disabled ID mapping. Consequently, the primary group of the user sometimes did not resolve properly, and the simple access provider sometimes failed. With this update, resolving user groups no longer ends prematurely, and the simple access provider now always obtains the primary group of users.

BZ#990143

Prior to this update, SSSD's dynamic DNS update feature did not filter out the multicast and subnet broadcast addresses when the "ipa_dyndns_iface" option was enabled. As a consequence, addresses that were not valid for DNS appeared in the Red Hat Identity Management DNS. With this update, multicast and subnet broadcast addresses are filtered out when performing a DNS update with "ipa_dyndns_iface", and only the appropriate adresses are used.

BZ#1082633

Previously, SSSD could not handle a zero value of the "ldap_group_nesting_level" option, and nested groups were thus not properly skipped. Consequently, SSSD retured more results than intended when identifying groups that a user is a member of. With this update, when "ldap_group_nesting_level" is set to 0, SSSD now correctly skips processing of nested groups and correct results are returned. In addition, the sssd-ldap(5) manual page has been updated with a detailed description for the behavior of "ldap_group_nesting_level".

BZ#1020945

When generating an enumeration of services with the "getent services" command, SSSD previously used incorrect pointer arithmetics, which caused its internal buffer to overflow. As a consequence, the sssd_nss process in some cases terminated unexpectedly when the user executed the "getent services" command. This update fixes the pointer arithmetics and "getent services" now works as expected.

BZ#1071823

Prior to this update, the HostID back end was incorrectly used when its target was not configured. As a consequence, SSSD terminated unexpectedly with a segmentation fault when connecting via SSH. This update adds a check whether the HostID back end is configured properly, and it no longer causes SSSD to crash.

BZ#1064581

The sss_cache tool previously lacked proper support for expiring user group membership, and did not reset the "syssdb_initgr_expire" attribute when expiring users. This update adds correct support for expiring user group membership to sss_cache and it now resets "syssdb_initgr_expire" when expiring users as expected.

BZ#1104145

Previously, the SSSD public key validator was excessively strict and could not handle the trailing newline character (\n) in a public key string obtained from LDAP. Consequently, the SSH key containing this character was marked as invalid and the user was not able to use it to connect to other machines. With this update, trailing newline in an SSH public key is ignored by the SSSD public key validator, and SSSD can now use an public key that contains this character.

BZ#1074014

Because of a redundant "success" or "fail" call of the Bash function daemon, an extra "[OK]" was printed during the restart of the SSSD service. This update removes the redundant call, and "[OK]" is correctly printed only two times when restarting SSSD.

BZ#1118541

Due to a race condition in the initialization of fast memory cache in SSSD client libraries, multi-threaded applications in some situations received the SIGSEGV or SIGFPE signals, and thus terminated unexpectedly. This update removes the race condition from the initialization, which prevents it from causing multi-threading application to crash.

BZ#1079783

Previously, SSSD could not handle the Enterprise Principal Names (EPN). As a consequence, certain users could not log in using the Active Directory (AD) provider. This problem has been fixed by the rebase, and SSSD now handles EPN correctly. As a result, users can now log in using the AD provider as expected.

BZ#1007381

Prior to this update, the proxy provider expected that every user had at least one supplementary group due to a bug in the proxy provider's group handling. Consequently, requesting a user that belonged only to their private group resulted in an error. With this update, the proxy provider has been fixed to handle the described situation correctly. As a result, requesting a user with no supplementary groups now works as expected.

BZ#995737

Previously, SSSD failed when the "entryUSN" attribute of sudo rules was empty. As a result, processing of sudo rules failed and the user was denied access when invoking sudo. With this update, SSSD can handle an empty "entryUSN" attribute of sudo rules and no longer causes denied access to sudo operations.

BZ#1127757

Previously, SSSD incorrectly used the "default_domain_suffix" option also for netgroups, rather than just for users and groups. As a consequence, sudo rules that rely on netgroup lookups did not work when "default_domain_suffix" was enabled. To fix this problem, SSSD has been updated to ignore "default_domain_suffix" for netgroup lookups. As a result, sudo rules now work correctly even when "default_domain_suffix" is enabled.

BZ#1122873

Prior to this update, when Service (SRV) record lookup status failed, port status was not marked as not working and SSSD did not try to resolve the SRV record again. As a consequence, the failover mechanism did not cycle through all the available servers, and SSSD therefore remained offline. A patch has been applied to fix this problem, and port status is now correctly marked as not working. As a result, failover continues with the next configured server.

BZ#1122158

Previously, when calling the initgroups() function, SSSD under some circumstances resolved Security Identifiers (SIDs) for groups but did not store the membership status. Consequently, group membership was not resolved correctly, as only the primary groups were acquired. A patch has been applied to fix this problem, and SSSD now updates the user's membership after SIDs are resolved. As a result, group membership is resolved correctly in the described situation.

Enhancements

BZ#1111317, BZ#1127278

The "override_space" option has been introduced to SSSD, which allows users to replace spaces in user names and group names with a specified character string. This makes it easier to use certain shell scripts or other applications that cannot properly handle user names and group names containing spaces. For further information on "override_space", refer to the sssd.conf(5) man page.

BZ#1042848

SSSD now supports obtaining users and user groups, as well as logging in as a user, not only from the AD domain that the user is currently connected to, but also from AD domains that are "trusted" by the current AD domain.

BZ#1111315

SSSD is now able to replace the "%H" string in the home directory obtained from the LDAP server with a value specified in the SSSD configuration file. This allows users to migrate Red Hat Enterprise Linux to SSSD while retaining the configuration of their existing environemnt.

BZ#1000061

A new option that disables the Kerberos locator plug-in has been added to SSSD. Thanks to this option, users can now choose not to inform the libkrb5 library about the Kerberos servers that SSSD uses, and to use only servers specified in the krb5.conf file.

BZ#1042922

With this update, SSSD now checks for and triggers the deprecated "sudoRunAs" attribute when the "sudoRunAsUser" attribute and the "ldap_sudorule_runasuser" mapping are not defined in the sssd.conf file. This ensures better retroactive compatibility with older SSSD settings.

BZ#1044729

SSSD is now able to locate the nearest Active Directory (AD) Domain Controller (DC) using the DNS Sites feature of AD. This allows SSSD to connect to DNS Sites more reliably and efficiently.

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

8.227. STRACE

8.227.1. RHBA-2014:1415 — strace bug fix update

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

The strace utility intercepts and records the system calls that are made and received by a running process and prints a record of each system call, its arguments, and its return value to standard error output or a file. It is often used for problem diagnoses, debugging, and for instructional purposes.

Bug Fixes

BZ#862321

Previously, the strace utility incorrectly assumed that the size of the integer data type and the size of the long data type was the same. As a consequence, strace incorrectly printed the options of a getsockopt call on targets with different sizes of integer and long. A patch has been applied to address this bug, and strace no longer returns incorrect values in the described situation.

BZ#1044605

Previously, invalid system calls were not required to have names in the system calls table. As a consequence, running the "strace -c -S name" command resulted in a segmentation fault under certain circumstances. With this update, invalid system calls are properly handled, and sorting calls by name now works as expected.

Users of strace are advised to upgrade to these updated packages, which fix these bugs.

8.228. SUBSCRIPTION-MANAGER

8.228.1. RHBA-2014:1384 — subscription-manager bug fix and enhancement update

Updated subscription-manager packages that fix numerous 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.

Bug Fixes

BZ#1096734

When python-rhsm made a request to the entitlement server for data in a JSON format, but got the response in a different format, such as HTML, the following attribute error was presented to the user:

```
AttributeError: 'exceptions.ValueError' object has no attribute 'msg'
error.
```

With this python-rhsm fix applied, the error message presented to the user is more accurate and informative concerning the problem:

```
Network error. Please check the connection details, or see
/var/log/rhsm/rhsm.log for more information.
```

BZ#1128658

Previously, the Subscription Manager tool made calls to Red Hat Network even when the system was not registered. As a consequence, some yum commands contacted Red Hat Network unexpectedly. With this update, Subscription Manager only makes contact if the server is registered for managing subscriptions, and Red Hat Network is contacted only when needed.

BZ#1118755

This update fixes typographical errors in the subscription-manager(8) manual page.

BZ#1062353

Previously, the rhn-migrate-classic-to-rhsm tool provided a confusing prompt, and it was unclear if the "Red Hat account:" prompt required the user the account number or the login. With this update, the user is prompted for Red Hat login.

BZ#1070388

Prior to this update, the Subscription Manager tool did not accept valid passwords that contained special characters for accounts on the Customer Portal. As a consequence, registration of some accounts failed. With this update, all valid passwords are accepted, and registration is no longer blocked for passwords with special characters.

BZ#1129480

Previously, the Subscription Manager tool inspected the environments URL when an activation key was provided. Consequently, Subscription Manager failed to provide authentication to environments. With this update, environments are not inspected when an activation key is given, and the activation key sequence is properly executed.

BZ#1107810

Previously, the help message for the "subscription-manager identity --force" command contained ambiguous information. With this update, the help message provides accurate information on how the "--force" option should be used.

BZ#1131213

Prior to this update, the "--serveurl" option was ignored. Consequently, a URL could not be migrated from a server without being specified in the rhsm.conf file. A patch has been applied to recognize the "--serveurl" option during migrations, and the user can now specify a server on the command line as expected.

BZ#1112326

This update fixes a typographical error in a path included in the rhsm.log file, which caused an error when loading facts from a file.

BZ#1126724

Previously, the help text contained hard-coded mention of port 443. As a consequence, help incorrectly displayed 443 port regardless of what was configured as the port. This update removes the 443 value, and appropriate values for both the host name and port are now displayed.

BZ#1135621

Previously, the GUI of the Subscription Manager tool showed both the default product certificates and the installed product certificates. As a consequence, duplicate certificates were displayed. The underlying source code has been modified to prefer the installed certificates over the default product certificates. As a result, duplicates are no longer shown in the GUI of Subscription Manager.

BZ#1122772

Previously, running the "yum repolist" command did not inform the user in the output if the system was not yet registered. With this update, the user is properly notified if the system is not registered after running "yum repolist".

Enhancements

BZ#1035115

This update adds support for updating the installed product ID certificates to the later versions.

BZ#1132071

With this update, the rhsm-debug tool collects more directories. A new directory that contains the default product certificates has been added, and rhsm-debug now collects the /etc/pki/product-default/ directory to help support personnel identify subscription problems.

BZ#1031755

With this update, subscription-manager and subscription-manager-plugin honor the http_proxy and https_proxy environment variables.

BZ#1115499

With this update, the user can enable X and disable on the same line, which reduces the number of necessary steps to perform the commands and makes disabling and enabling repositories more convenient.

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

8.229. SUDO

8.229.1. RHBA-2014:1484 — sudo bug fix update

Updated sudo packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The sudo packages contain the sudo utility which allows system administrators to provide certain users with the permission to execute privileged commands, which are used for system management purposes, without having to log in as root.

Bug Fixes

BZ#1006447

Previously, the sudo utility did not correctly handle the "sudo -ll" command when the System Security Service Daemon (SSSD) was used to get available sudo entries. Consequently, running "sudo -ll" returned incomplete results, as it did not list the rule names of sudo users. A patch has been applied to fix this bug, and "sudo -ll" now lists the rule names as expected when SSSD is used.

BZ#1006463

Prior to this update, sudo did not respond correctly to the root user's request to list the privileges for a specified user when SSSD was used. As a consequence, running the "sudo -l -U" command for a certain user as root returned incomplete results, while running the same command as the user worked as expected. The source code has been updated to fix this problem, and executing "sudo -l -U" as root now returns correct results.

BZ#1052940

Previously, sudo did not correctly handle the situation when the group specification in the /etc/sudoers file contained escape characters on systems integrated with the Active Directory (AD) service. As a consequence, specifying a custom password prompt for a group containing escape characters did not work, as sudo displayed the default password prompt instead when a member of that group used sudo. A patch has been applied to fix this bug, and setting a custom password prompt now works as expected even if the group specification contains escape characters.

BZ#1065415

Previously, the sesh process, when called as "-sesh" by sudo, executed the login shell with an incorrect path name, as it replaced the last slash character in the shell path with a dash while the rest of the path remained unchanged. As a consequence, the login shell was being called as "/bin-[shell]" instead of "-[shell]", which could result in unexpected system behavior. The source code has been updated to fix this bug, and sesh no longer causes this problem.

BZ#1070952

Previously, the pam_faillock module did not acknowledge the attempts to terminate sudo login with the Ctrl+C shortcut after the password prompt showed up. As a consequence, sudo continued to try to log in and eventually locked the user out. The problem has been fixed, and even though an attempt terminated with Ctrl+C still counts as one failed attempt to log in, sudo no longer locks the user out.

BZ#1078338

Previously, sudo did not correctly handle setting the NIS domain name value as "(none)", as it considered the "(none)" text string a valid domain name. Consequently, the getdomainname() function returned "(none)" as the NIS domain name instead of recognizing that no domain name was set. The source code has been updated to fix this problem, and sudo now handles the described situation correctly.

BZ#1083064

Prior to this update, when a sudo rule contained the +netgroup variable in the sudoUser attribute, the system ignored the rest of the sudo rule under certain circumstances. Consequently, executing the "sudo -l" command did not show the complete list of rules configured for the specified user. With this

update, the problem has been fixed, and running "sudo -l" now shows the complete list of rules even when a sudo rule contains the +netgroup variable.

Users of sudo are advised to upgrade to these updated packages, which fix these bugs.

8.230. SUITESPARSE

8.230.1. RHBA-2014:0296 — suitesparse bug fix update

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

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

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

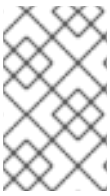
8.231. SYSLINUX

8.231.1. RHBA-2014:1461 — syslinux bug fix update

Updated syslinux packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The syslinux packages provide a suite of boot loaders, currently supporting DOS FAT file systems, Linux ext2 and ext3 file systems (EXTLINUX), PXE network boots (PXELINUX), or ISO 9660 CD-ROMs (ISOLINUX). It also includes a tool, MEMDISK, which loads legacy operating systems from these media.

This update also fixes the following bugs:



NOTE

The syslinux packages have been upgraded to upstream version 4.04, which provides a number of bug fixes over the previous version, including a patch that corrects the PXE chain functionality. (BZ#970946)

This update also fixes the following bugs:

Bug Fixes

BZ#980671, BZ#1085780

The pxelinux.0 file incorrectly used a BIOS interrupt call when booting up from a local hard drive through the Pre-Boot Execution Environment (PXE). As a consequence, the booting process became unresponsive. With this update, the behavior of pxelinux.0 has been fixed and PXE booting now functions as expected.

BZ#989867

The syslinux-tftpboot program incorrectly installed tftp files into the /tftpboot/ directory. Consequently, these files could not be located and used by the appropriate programs, such as tftp. With this update, tftp files are installed into the /var/lib/tftpboot/ directory as expected.

The syslinux packages have been upgraded to upstream version 4.04, which provides a number of bug fixes over the previous version, including a patch that corrects the PXE chain functionality. (BZ#970946)

Users of syslinux are advised to upgrade to these updated packages, which fix these bugs.

8.232. SYSSTAT

8.232.1. RHBA-2014:1468 — sysstat bug fix and enhancement update

Updated sysstat packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 6.

The sysstat packages provide a set of utilities which enable system monitoring of disks, network, and other I/O activity.

Bug Fixes

BZ#921612

When the sysstat utility appended new statistics to the "sa" daily data files, it did not check whether those files existed from the previous month. Under certain circumstances, for example when a month was short, sysstat appended new statistics to the old files. With this update, the utility has been modified to check whether the old files exist and remove them in case they does. As a result, new statistics are not appended to the old "sa" files.

BZ#1088998

Previously, the "sa2" script did not support the xz compression. As a consequence, old daily data files were not deleted. The support for the xz compression has been added to the script and the data is now deleted as expected.

BZ#1124180

The dynamic ticks kernel feature can currently make the /proc/stat file unreliable because a CPU cannot provide reliable statistics if it is stopped. Even though the kernel is trying to provide the best guess, the statistics are not always accurate. As a consequence, some sysstat commands could show overflowed values. This update detects values going backwards in sysstat, and sysstat commands no longer show overflowed values.

In addition, this update adds the following

Enhancements

BZ#1102603

With this update, the user is able to set a compress method in the /etc/sysconfig/sysstat configuration file using the ZIP variable. This enhancement provides an easier configuration of the data file compression method.

BZ#1110851

The sysstat(5) manual page now provides documentation of the /etc/sysconfig/sysstat configuration file as well as detailed description of the HISTORY configuration variable.

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

8.233. SYSTEM-CONFIG-FIREWALL

8.233.1. RHBA-2014:0837 — system-config-firewall bug fix update

Updated system-config-firewall packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The system-config-firewall packages contain a graphical user interface for basic firewall setup.

Bug Fixes

BZ#634857

Previously, the default iptables rules for IPv6 did not allow the DHCPv6 configuration. Consequently, the DHCPv6 responses were blocked. With this update, the rules enabling DHCPv6 have been added, so that network environments using DHCPv6 are now supported as expected.

BZ#682391

Recently, some arbitrary names for network devices have been changed. As a consequence, it was impossible to find such devices by name. This update provides a patch that reflects the name change, so that it is now easy to find the renamed devices.

BZ#711231

Under certain circumstances, an attempt to execute the system-config-firewall utility failed with the following error:

"shutil.py:50:copyfile:IOError: [Errno 13] Permission denied: '/etc/sysconfig/iptables-config'"

The underlying source code has been modified to fix this bug and system-config-firewall now works as expected in the described scenario.

BZ#720831

Previously, the "eth+" GUI option could not be expanded to show individual network interfaces. Consequently, the user was unable to specify a rule for a particular interface. With this update, the particular entries have been added to the list of interfaces, thus allowing to specify a rule for a single interface.

BZ#756048

Due to a missing dependency, an attempt to run the system-config-firewall-tui utility on a system with a minimal installation of Red Hat Enterprise Linux 6 failed. The missing dependency has been added to the system-config-firewall-tui dependency list and the utility now works correctly.

BZ#819809

Previously, the localization of the system-config-firewall utility was not complete. This update completes translations for all languages supported by Red Hat.

Users of system-config-firewall are advised to upgrade to these updated packages, which fix these bugs.

8.234. SYSTEM-CONFIG-KDUMP

8.234.1. RHBA-2014:1529 — system-config-kdump bug fix update

An updated system-config-kdump package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The system-config-kdump tool is a graphical utility used to configure kernel crash dumping via the kdump and kexec utilities.

Bug Fixes

BZ#962724

On the IBM System z architecture, the system-config-kdump utility updated bootloader settings only when the kdump service was already running. However, since system-config-kdump does not run when kdump is disabled, it was impossible to enable kdump on the IBM System z architecture. With this update, the bootloader configuration updates regardless of the status of the kdump service, and the kdump feature can now be enabled on this architecture using the system-config-kdump interface.

BZ#1017611

Prior to this update, the drop-down list of raw devices in the system-config-kdump interface incorrectly included partitions that were already in use. As a consequence, users could choose these partitions as the targets for copying the kdump file, which in turn corrupted the file system. With this update, the system-config-kdump interface only lists unused partitions in the list of raw devices, and it is therefore no longer possible for kdump to cause files system corruption in the described scenario.

BZ#987681

Previously, the kdump parser of kernel parameters did not properly handle entries that contain quoted strings. As a consequence, modifying boot options via system-config-kdump on a system that used quoted strings in the kernel parameters could lead to the system failing to boot. With this update, the parser correctly accounts for quoted strings and kernel parameters with quoted strings are now handled properly.

BZ#1030533

Prior to this update, the automatic kdump memory thresholds in system-config-kdump did not match their respective values in the kernel. Consequently, selecting the "Automated kdump memory setting" option in the system-config-kdump interface on some systems disabled kdump. The memory thresholds in system-config-kdump have been updated to reflect those in the kernel, and on systems with sufficient memory, "Automated kdump memory settings" no longer disables kdump. However, on systems with not enough memory, this option is disabled and the memory for kdump has to be configured manually.

BZ#977981

Previously, system-config-kdump used an incorrect path to bootloader configuration on EFI systems using the GRUB bootloader on AMD64 and Intel 64 architectures. Consequently, it was not possible to configure kdump memory on these systems. This update adds the correct path to the list of known bootloader configuration paths, and it is now possible to configure kdump memory in the described circumstances.

Users of system-config-kdump are advised to upgrade to this updated package, which fixes these bugs.

8.235. SYSTEM-CONFIG-KEYBOARD

8.235.1. RHBA-2014:1617 — system-config-keyboard bug fix update

Updated system-config-keyboard packages that fix one bug are now available for Red Hat Enterprise Linux 6.

The system-config-keyboard packages provide a graphical user interface that allows the user to change the default keyboard of the system.

Bug Fix

BZ#1136833

Previous versions of gtk2 used a horizontal separator between the dialog contents and the buttons in GUI windows. The system-config-keyboard program was configured to remove this separator from its GUI without additional checks. With the gtk2 update, this separator was no longer displayed and system-config-keyboard instead removed the "OK" button from its GUI. With this update, system-config-keyboard has been modified to check if the item to be deleted is actually a horizontal separator. As a result, the "OK" button remains and no horizontal separator is shown, regardless of the gtk2 package version currently installed.

Users of system-config-keyboard are advised to upgrade to these updated packages, which fix this bug.

8.236. SYSTEM-CONFIG-LVM

8.236.1. RHBA-2014:1403 — system-config-lvm bug fix update

Updated system-config-lvm package that fixes several bugs is now available for Red Hat Enterprise Linux 6.

The system-config-lvm utility enables users to configure logical volumes using a GUI.

Bug Fixes

BZ#878253

Previously, the system-config-lvm utility did not support thin logical volumes. As a consequence, previously supported volumes could not be managed. With this update, thin logical volumes are still not supported but do not block managing supported volumes.

BZ#953071

Prior to this update, the Logical Volume Management (LVM) GUI was not always displayed correctly when accessed over remote access. Consequently, the user could not initiate the GUI. A patch has been provided to fix this bug, and the LVM GUI is now displayed correctly as intended.

BZ#1029755

Previously, when the ext3 Logical Volume (LV) partition was mounted and the user attempted to extend it online, the system-config-lvm utility tried to unmount ext3 and only after that to extend it. The underlying source code has been patched, and ext3 file systems can now be extended online using the command line tools without system-config-lvm trying to unmount it first.

Users of system-config-lvm are advised to upgrade to this updated package, which fixes these bugs.

8.237. SYSTEMTAP

8.237.1. RHBA-2014:1449 — 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.

This update also fixes the following bugs:

NOTE

The systemtap packages have been upgraded to upstream version 2.5-5, which provides a number of bug fixes and enhancements over the previous version. (BZ#1038692, BZ#1074541)

This update also fixes the following bugs:

Bug Fixes

BZ#1020437

Previously, the kernel added some trace points in a way which failed to expose them to systemtap's search mechanisms. This update extends systemtap's search mechanism to include these extra trace points, thus allowing them to be probed from a systemtap script.

BZ#1027459

The SystemTap runtime could attempt to open a file named "trace1" in the current directory rather than the one that was created in the /sys/kernel/debug/systemtap/ directory. As a consequence, SystemTap terminated unexpectedly if such a file existed in the current directory. This update applies a patch to fix this bug and SystemTap now works as expected in the described scenario.

BZ#1109084

Previously, it was not entirely clear that names of scripts configured with the SystemTap init script service could contain only alphanumeric characters and the underscore character ("_"). Also, the first character in a name cannot be a number. This update adds this information to the systemtap(8) manual page to prevent any confusion.

The systemtap packages have been upgraded to upstream version 2.5-5, which provides a number of bug fixes and enhancements over the previous version. (BZ#1038692, BZ#1074541)

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

8.238. TBOOT

8.238.1. RHBA-2014:1495 — tboot bug fix and enhancement update

Updated tboot packages that fix several bugs and add various enhancements 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.

NOTE

The tboot packages have been upgraded to upstream version 1.8.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#1037469, BZ#1065320)

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

8.239. TELNET

8.239.1. RHBA-2014:0868 — telnet bug fix update

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

Telnet is a popular protocol for logging in to remote systems over the Internet. The telnet-server packages include a telnet service that supports remote logins into the host machine. The telnet service is disabled by default.

Bug Fixes

BZ#772912

Prior to this update, the telnet utility could enter an infinite loop when the user specified the "-b" parameter with a non-existing network interface. This update modifies the telnet command to print errors when users specify a non-existing network interface.

BZ#832059

Prior to this update, the in.telnetd service could fail to update information in the /var/run/utmp directory when a deadlock occurred in a telnet session. This update modifies telnetd to update /var/run/utmp correctly.

Users of telnet are advised to upgrade to these updated packages, which fix these bugs.

8.240. TIGERVNC

8.240.1. RHBA-2014:1412 — tigervnc bug fix update

Updated tigervnc packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

Virtual Network Computing (VNC) is a remote display system which allows users 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.

Bug Fixes

BZ#562669

When more than one display was configured in the /etc/sysconfig/vncservers file, the vncserver initscript could stop, preventing other displays from being started. The source code has been fixed, and vncserver now attempts to start each configured display as intended.

BZ#840972

The position of the mouse cursor in the VNC session was not correctly communicated to the VNC viewer, resulting in cursor misplacements. The method of displaying the remote cursor has been changed, and cursor movements on VNC server are now accurately reflected on VNC client.

BZ#917717, BZ#991285

Previously, incompatible versions of pixman, libX11, and tigervnc-server utilities could be installed on Xvnc. Nevertheless, Xvnc could not start due to symbol resolution failures or crashes. With this update, tigervnc-server has explicit version requirements for pixman and libX11, and Xvnc now starts successfully.

BZ#949522

The vncserver initscript made an assumption about the preferred shell for users of TigerVNC. As a consequence, configured displays started only for users using bash. The underlying source code has been fixed, and configured displays now start for any shell the user chooses.

BZ#958988

Previously, Xvnc created via the xinetd daemon a random connection that was not invoked by the user, consuming abundant CPU memory. A problem with running Xvnc from x/inetd in the "nowait" mode has been fixed, and user or non-user Xvnc connections no longer lead to high CPU usage.

BZ#975778

Drawing operations on window borders accessed the pixmap screen directly with Xvnc assuming that all drawing operations operated on a window. This could lead to artifacts on the screen. A fix has been back-ported from upstream, and anomalies no longer occur during visual representation.

BZ#1004093

Previously, the VNC Xorg extension could be initialized twice, leading to a busy loop on exit. An upstream patch has been back-ported to allow initialization only once.

BZ#1029923

When using TigerVNC with certain keyboard layouts, the AltGr key did not work, preventing users from producing symbols such as "@" (at-sign). A fix from a later version of tigervnc has been back-ported, and AltGr key combinations now work correctly.

BZ#1031506

Due to differences in keyboard mappings, keypresses over VNC sometimes needed to be sent using a fake shift keypress. When using keys on the numeric keypad with NumLock active, this approach did not work. With this update, a fix has been back-ported to avoid using fake shift keypresses for numeric keypad keys, and the numeric keypad now works correctly when using VNC.

BZ#1044244

When using TigerVNC as a loadable X module, initialization of the GLX extension was not performed correctly. This could lead to the X server unexpected termination. A fix from a later version of TigerVNC has been back-ported, and the GLX extension is now initialized correctly.

BZ#1116956

When the last X client disconnected, the X server regenerated and all input devices and extensions were reinitialized. Nevertheless, the VNC extension module left the VNC extension inactive. With this update, VNC is retained or re-loaded after server regeneration, and a remote system connects to X server over VNC successfully.

BZ#1121041

When negotiating which encoding to use, the vncviewer utility did not validate server-provided encoding values correctly. This caused a write to an array index outside the correct range, leading to a crash. With this update, the encoding values are now correctly validated, preventing such crashes.

Users of tigervnc are advised to upgrade to these updated packages, which fix these bugs.

8.241. TOMCAT6

8.241.1. RHBA-2014:1618 — tomcat6 bug fix update

Updated tomcat6 packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

Bug Fix

BZ#1140855

Due to a bug in the tomcat6 packages, an attempt to install the ipa-server package with Domain Name System (DNS) failed because it was not possible to configure the Certification Authority (CA) instance. This update provides a patch to fix this bug and ipa-server can now be installed as expected.

Users of tomcat6 are advised to upgrade to these updated packages, which fix this bug.

8.242. TOMCATJSS

8.242.1. RHBA-2014:1550 — tomcatjss bug fix update

An updated tomcatjss package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The tomcatjss package provides a Java Secure Socket Extension (JSSE) implementation using Java Security Services (JSS) for Tomcat 6.

Bug Fix

BZ#1084224

Previously, the tomcatjss package missed the strictCiphers implementation. Consequently, the user could not disable weaker ciphers and enable the stronger ciphers. With this update, strictCiphers has been implemented to tomcatjss.

Users of tomcatjss are advised to upgrade to this updated package, which fixes this bug.

8.243. TRACE-CMD

8.243.1. RHBA-2014:1559 — trace-cmd bug fix update

Updated trace-cmd packages that fix one bug 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 Fix

BZ#879814

Due to invalid pointers, executing the "trace-cmd split" or "trace-cmd report" commands after running latency tracers failed with a segmentation fault. With this update, additional checks have been added to ensure that the pointers are properly initialized before attempting to use them. As a result, the segmentation fault no longer occurs in the described scenario.

Users of trace-cmd are advised to upgrade to these updated packages, which fix this bug.

8.244. TRANSFIG

8.244.1. RHBA-2014:0483 — transfig bug fix update

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

The transfig utility creates portable documents that can be printed in a wide variety of environments. The utility converts the FIG files produced by the Xfig editor to other formats by creating a makefile that can translate the FIG files and the figures in the PIC format into a specified LaTeX graphics language, for example PostScript.

Bug Fix

BZ#858718

Prior to this update, the PostScript files generated by the transfig utility incorrectly were reported to conform to the PostScript document structuring conventions (DSC). As a consequence, printing from the Xfig editor and printing the PostScript files generated by transfig could result in blank pages. A patch that improves the DSC conformance has been applied to address this bug, and the Xfig drawings are printed as expected in the aforementioned cases.

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

8.245. TROUSERS

8.245.1. RHSA-2014:1507 — Low: trousers security, bug fix, and enhancement update

Updated trousers packages that fix one security issue, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 6.

Red Hat Product Security 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 from the CVE link in the References section.

TrouSerS is an implementation of the Trusted Computing Group's Software Stack (TSS) specification. You can use TrouSerS to write applications that make use of your TPM hardware. TPM 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.

Security Fix

CVE-2012-0698

A flaw was found in the way tcsd, the daemon that manages Trusted Computing resources, processed incoming TCP packets. A remote attacker could send a specially crafted TCP packet that, when processed by tcsd, could cause the daemon to crash. Note that by default tcsd accepts requests on localhost only.

Red Hat would like to thank Andrew Lutomirski for reporting this issue.

The trousers package has been upgraded to upstream version 0.3.13, which provides a number of bug fixes and enhancements over the previous version, including corrected internal symbol names to avoid collisions with other applications, fixed memory leaks, added IPv6 support, fixed buffer handling in tcsd, as well as changed the license to BSD. (BZ#633584, BZ#1074634)

All trousers users are advised to upgrade to these updated packages, which correct these issues and add these enhancements.

8.246. TSCLIENT

8.246.1. RHBA-2014:0524 — tsclient bug fix update

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

The Terminal Server Client (tsclient) is a GTK2 front end that makes it easy to use the Remote Desktop Protocol client (rdesktop) and vncviewer utilities.

Bug Fixes

BZ#798631

Previously, the tsclient user interface did not offer an option to set the 32-bit color depth in the "Advanced Options" menu for the "Windows Terminal Service" connection type. Consequently, the 32-bit color depth could not be selected even though it was supported on the system, and connection to Windows systems could not be established with more than 16-bit color depth. With this update, the error in the "Advanced Options" menu has been fixed, and the 32-bit color depth option now functions as intended.

BZ#848526

Prior to this update, tsclient was not fully compatible with the Remote Desktop Protocol (RDP). Consequently, tsclient could, under certain circumstances, terminate unexpectedly when the user was connected to a remote system over RDP. This update addresses the problems with RDP compatibility, and tsclient no longer crashes when using RDP for remote connection.

Users of tsclient are advised to upgrade to these updated packages, which fix these bugs.

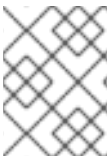
8.247. TUNA

8.247.1. RHBA-2014:1404 — tuna bug fix update

Updated tuna packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The tuna packages provide 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 update also fixes the following bugs:



NOTE

The tuna package has been upgraded to upstream version 0.10.4, which provides a number of bug fixes over the previous version. (BZ#1029591)

This update also fixes the following bugs:

Bug Fixes

BZ#1035795

Previously, if the scheduler priority was not specified, the "tuna -t $PID -p OTHER" command failed with the following error:

ValueError: invalid literal for int() with base 10: 'OTHER'

This error occurred also when different parameters, such as RR or FIFO, were passed to the -p option. This bug has been fixed and the value error no longer occurs.

BZ#1059685

Due to a bug in the tuna package, the "tuna -CP" command failed to list processes, returning the following message:

NameError: global name 'cgroups' is not defined

This bug has been fixed and the name error no longer occurs when executing "tuna -CP".

The tuna package has been upgraded to upstream version 0.10.4, which provides a number of bug fixes over the previous version. (BZ#1029591)

Users of tuna are advised to upgrade to these updated packages, which fix these bugs.

8.248. TZDATA

8.248.1. RHEA-2014:1621 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#1147318

This update contains the changes implemented in tzdata-2014h that are all related to historical transition times. In particular, transition to standard time in Asia/Novokuznetsk on Jan 5 1920 actually took place on Apr 30 1924, transition to saving time in Jamaica took place not on Apr 28 1974, but already on Jan 6. In addition, a number of African zones (Africa/Blantyre, Bujumbura, Gaborone,

Harare, Kigali, Lubumbashi, and Lusaka) have been merged with Africa/Maputo, because their transition times do not differ in post-1970 era. Africa/Maseru and Africa/Mbabane have now been merged to Africa/Johannesburg for the same reason.

Users of tzdata are advised to upgrade to these updated packages, which add this enhancement.

8.249. UDEV

8.249.1. RHBA-2014:1524 — udev bug fix and enhancement update

Updated udev packages that fix several bugs and add two enhancements 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 runs in user space, dynamically creates and removes devices, provides consistent naming, and a user-space API. The udev packages replace the devfs package and provides better hot plug functionality.

Bug Fixes

BZ#839172, BZ#1020856

Previously, hard disks connected to a Peripheral Component Interconnect Express SSD (PCIe SSD) did not have an entry with their IDs in the udev database, because device names did not trigger any persistent disk udev rule. As a consequence, no symbolic link was created in the /dev/disk/by-* file and the device vendor and product were shown as "Unknown" in the installer. This update adds a udev rule to supply information gathered via the ata_id utility. Now, a symbolic link in /dev/disk/by-id is created by udev and additional information is available in the udev database.

BZ#1008341

Prior to this update, a udev rule tried to write to a sysfs file without checking its existence. As a consequence, an error message was returned to syslog. With this update, the udev rule checks for the existence of the file before trying to write to it, and no inappropriate error messages appear in syslog.

BZ#028174

The udev version in Red Hat Enterprise Linux 6 serialized modprobe execution for network cards limiting the amount of worker processes. However, if a lot of modprobes were triggered, udev could reach the limit of worker processes and stopped reacting to firmware load requests. With this update, for every modprobe process in the queue, the amount of worker processes has been increased, and firmware load requests are now executed successfully.

BZ#077186

Previously, for a firmware loading request, the global timeout was 60 seconds by default. However, some firmware loading took longer than 60 seconds on systems with heavy I/O load during the boot process, and thus sometimes failed. The global timeout for firmware loading has been increased to 600 seconds, which is long enough for all systems to let all firmware load without a timeout.

BZ#091790

The sr_mod kernel module was loaded via a udev rule without honoring any blacklist options. As a consequence, sr_mod was loaded although the administrator could have blacklisted this kernel module. With this update, the udev rule calls modprobe with the "-b" option, which lets modprobe

check the blacklist. As a result, the sr_mod kernel module is no longer loaded automatically if the administrator chose to blacklist it.

BZ#1103278

For some data cards, a udev rule called the modem-modeswitch tool to switch the card from CDROM to modem mode. However, newer versions of the kernel did not require this call. Consequently, these data cards could not switch to modem mode. To fix this bug, the udev rule for the data cards have been removed, and switching to modem mode no longer causes problems.

In addition, this update adds the following

Enhancements

BZ#910168

This update adds descriptions of scsi_id short options to the scsi_id(8) manual page, and thus scsi_id(8) is now complete.

BZ#1054482

As the "iDRAC7" network interface needed to be distinguished from normal network interfaces, it has been renamed to "idrac".

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

8.250. UNIXODBC

8.250.1. RHBA-2014:0869 — unixODBC bug fix update

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

The unixODBC packages contain a framework that supports accessing databases through the ODBC protocol.

Bug Fixes

BZ#768986

Prior to this update, the desktop file for unixODBC, ODBCConfig.desktop, contained deprecated options and incorrect values. Consequently, the unixODBC application was not appropriately categorized. In this update, the options and values have been fixed and the application categorization works as intended.

BZ#1060225

Previously, file name values were hard-coded in the ODBC Driver Manager. As a consequence, the Driver Manager did not correctly interact with other applications after an update. The current update changes the hard-coded values to dynamically determined ones, and updating no longer causes Driver Manager incompatibilities with other applications.

Users of unixODBC are advised to upgrade to these updated packages, which fix these bugs.

8.251. UTIL-LINUX-NG

8.251.1. RHBA-2014:1545 — util-linux-ng bug fix and enhancement update

Updated util-linux-ng packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The util-linux-ng packages contain a large variety of low-level system utilities that are necessary for a Linux operating system to function.

Bug Fixes

BZ#999625

Previously, the behavior of the "acl" option was not correctly documented in the mount(8) manual page. The manual page now clarifies that the "acl" option is specific to the file system and not a default mount option.

BZ#1004021

The blkid(8) manual page now documents the behavior of the "-w" option correctly, mentioning that "blkid -w" always writes to the default cache file even if the output has been redirected elsewhere.

BZ#1011590

Previously, using the fdisk command on multipath mapped devices failed with a "floating point exception" error. This bug has been fixed and fdisk now successfully executes on multipath mapped devices.

BZ#1016470

The blockdev(8) manual page now clarifies the behavior of the "--setbsz" option, which sets the block size on file descriptors opening the block size.

BZ#1031641

Previously, the findmnt command did not handle correctly trailing forward slashes ("/") in the entries of the /proc/mounts file. As a consequence, findmnt sometimes failed to match the correct path. This bug has been fixed and the findmnt command now matches the correct path independently of the trailing slash.

BZ#1033309

The rename(1) manual page referred to the non-existing mmv(1) manual page. This reference has been removed.

BZ#1039187

The PERMISSIONS section of the taskset(1) manual page has been corrected to mention that a user is allowed to change the affinity of processes he owns, but a CAP_SYS_NICE flag is required to change the affinity of another user's process.

BZ#1072583

Previously, the "hwclock --systohc" command could enter an indefinite loop on busy or virtual machines. Consequently, the machine could not complete the shutdown or reboot a process. A patch with a different mechanism has been applied, and the "hwclock --systohc" command now completes successfully.

BZ#1049055

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#1097715

Previously, when attempting to use the flock command to lock a file in NFSv4 volumes, the command failed with the following error:

[nfs4] flock nfs file fail: Bad file descriptor

This bug has been fixed and now the flock command executes successfully on NFSv4 volumes.

BZ#1104575

Previously, the kill command which is used by the ntfs service did not check the "errno" value after calling the strtol() function. As a consequence, using the "service netfs stop" command could kill every process on the system if there were more than 100 000 processes running at the same time. This bug has been fixed, and using the "service netfs stop" command only stops ntfs as expected.

In addition, this update adds the following

Enhancements

BZ#619521

This update implements the lslogins(1) command which lists information about accounts on the system in a easy to read format.

BZ#957906

This update adds the nsenter utility to the util-linux-ng packages. It allows to run commands in kernel namespaces. If the namespace does not exist, nsenter creates a new one and then executes the command.

Users of util-linux-ng are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

8.252. VALGRIND

8.252.1. RHBA-2014:1464 — valgrind bug fix update

Updated valgrind packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The valgrind packages provide the Valgrind programming tool that helps detect memory-management problems in programs. Valgrind is used for debugging memory, detecting memory leaks, and profiling.

Bug Fixes

BZ#828341

Previously, the Valgrind tool did not recognize that certain older i386 AMD Athlon processors supported the PREFETCH instruction from the MmxExt instruction set. As a consequence, Valgrind displayed an error message about an unsupported instruction after running an application under

Valgrind on the i386 architecture that used PREFETCH. Valgrind has been updated to recognize which processors implement the MmxExt instruction set. As a result, applications now run as expected under Valgrind on i386 using PREFETCH.

BZ#881893

Prior to this update, on the IBM System z architecture, Valgrind could incorrectly report that it supported the KIMD Message-Security Assist (MSA) instruction extension even when it was the host machine that supported MSA, not Valgrind. Consequently, a program could use some instructions that Valgrind did not support, which caused the system to terminate that program. With this update, Valgrind no longer considers the instruction sets supported by the host machine. As a result, programs executed under Valgrind now run as expected in the described situation.

BZ#1007400

Previously, Valgrind did not support the [lf]setxattr system calls on Linux kernels for the 32-bit PowerPC and 64-bit PowerPC architectures. Consequently, programs using [lf]setxattr displayed warning and error messages. With this patch, Valgrind has been updated to recognize [lf]setxattr, and programs using [lf]setxattr now run under Valgrind on 32-bit PowerPC and 64-bit PowerPC without displaying warnings or errors.

BZ#1012932

Prior to this update, Valgrind did not correctly recognize the MOVNTDQA instruction from the Intel Streaming SIMD Extension 4 (Intel SSE4) instruction set. As a consequence, programs using MOVNTDQA terminated unexpectedly when executed under Valgrind. With this update, the problem has been fixed, and programs using MOVNTDQA now run as expected under Valgrind.

BZ#1024162

Prior to this update, Red Hat Enterprise Linux 6 signal handlers were executed on a misaligned stack when used on the AMD64 and Intel 64 architectures. Consequently, instructions that require 16-byte data alignment terminated unexpectedly. This update fixes the stack pointer alignment, and invoking a signal on the AMD64 and Intel 64 architectures is now executed properly.

BZ#1101422

Previously, Valgrind did not support the dup3 system calls on the PowerPC architecture kernels. As a consequence, programs using dup3 displayed warning and error messages when running under Valgrind. A patch has been applied to fix this problem, and Valgrind now handles dup3 properly. Programs using dup3 now run under Valgrind on PowerPC without displaying warnings or errors.

BZ#1120021

Previously, the Memcheck memory error detector on i386 did not correctly handle some address accesses used by the bcopy() function, a converted version of the memcpy() function, which is contained in the GNU C Library (glibc). Consequently, using glibc bcopy() in i386 binary files running under Valgrind could report an invalid address access. Memcheck has now been updated to handle this instance of bcopy() correctly. Programs using bcopy() or memcpy() no longer display warnings about an invalid access in the described situation.

BZ#1126483

Prior to this update, Valgrind did not support the prctl system calls on 64-bit PowerPC Linux kernels. As a consequence, programs using prctl displayed warning and error messages when running under Valgrind. Valgrind has now been updated to recognize prctl, and programs using prctl no longer display warnings or errors in the described situation.

Users of valgrind are advised to upgrade to these updated packages, which fix these bugs.

8.253. VIRT-MANAGER

8.253.1. RHBA-2014:1447 — virt-manager bug fix and enhancement update

Updated virt-manager packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

Updated virt-manager packages that fix several bugs 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.

This update fixes the following bugs:

Bug Fixes

BZ#870383, BZ#1094600

Due to a bug in the virt-manager package, the virt-manager application failed to connect to a remote host machine trough IPv6. Also, virt-manager failed to create virtual guests with remote connections through IPv6. This bug has been fixed and virt-manager now successfully opens IPv6 connections to remote hosts and creates guests with such connections as expected.

BZ#918451

When creating a virtual machine (VM), the virt-manager application incorrectly configured a custom added TCP net console device. The bug has been fixed and TCP consoles are now configured correctly when creating a VM.

BZ#1025706

When starting the virt-manager application over SSH without enabled x-forwarding, virt-manager terminated and returned a traceback instead of an informative error message. With this update, virt-manager has been modified to return a well-formed error message in the aforementioned scenario.

BZ#1091292

After executing the pm-suspend command on the guest virtual machine, the virt-manager application displayed the status of this guest as "Running" instead of "Suspended". The bug has been fixed and virt-manager now shows the correct status of suspended guests.

BZ#1091878

Previously, after clicking the 'refresh volume list' button in the virt-manager GUI, the virt-manager application became unresponsive. This bug has been fixed and virt-manager no longer hangs in the aforementioned scenario.

BZ#1124387

The virt-manager application has been modified to return an informative error message instead of a traceback when the LC_CTYPE variable is set incorrectly.

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.

In addition, this update adds the following

Enhancements

BZ#807277

This update adds support for USB redirection to the virt-manager package.

BZ#1049781

This update adds support for Virtio SCSI disk to the virt-manager package.

BZ#996517

The pvpanic device is now enabled by default when creating a virtual machine with the virt-manager application. The pvpanic is a simulated device that notifies virt-manager of panic events on guest machines.

BZ#1046583

This update adds an option for changing the default CPU model when creating a virtual machine (VM) with the virt-manager application. The VM CPU model can now be set to be as close as possible to the host CPU model.

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

8.254. VIRT-VIEWER

8.254.1. RHBA-2014:1379 — virt-viewer bug fix update

Updated virt-viewer packages that fix numerous bugs are now available for Red Hat Enterprise Linux 6.

The virt-viewer packages provide the 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. The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol designed for virtual environments.

Bug Fixes

BZ#1056041

Prior to this update, **`SPICE`** incorrectly determined the scaling of windows by using the original desktop size instead of the host screen size. As a consequence, when a guest window was open in **`SPICE`**, the screen could, under certain circumstances, become blurred. With this update, the guest window scaling has been fixed and this problem no longer occurs.

BZ#1083203

Prior to this update, when a **`virt-viewer`** console was launched from the Red Hat Enterprise Virtualization user portal with the **`Native Client`** invocation method and **`Open in Full Screen`** was selected, the displays of the guest virtual machine were not always configured to match the client

displays. With this update, **virt-viewer** correctly shows a full-screen guest display for each client monitor.

BZ#809546

Previously, when **virt-viewer** was opened in fullscreen mode on a client machine with two or more monitors, it opened a fullscreen guest display for each monitor, but sometimes placed more than one display on the same client monitor. With this update, the bug has been fixed and each fullscreen guest display is now placed on its own client monitor.

BZ#1002156, BZ#1018180

When configuring and aligning multiple guest displays, the display setting sometimes used outdated information about the position of the **virt-viewer** and **remote-viewer** windows. This caused overlapping in the guest displays, and different client windows showed some of the same content. In addition, the content of the guest displays in some cases swapped completely when a guest display window was resized. With this update, only the current window location is used to align and configure displays. As a result, the overlaps of content and the swapping no longer occur.

BZ#1099295

Under some circumstances, the system USB channels are created after the display channel. This sometimes caused redirecting a USB device to a guest machine to fail, which in turn caused the **USB device selection** menu in the **virt-viewer** client interface to be unusable. With this update, redirecting a USB device works regardless of the order in which the USB channels and the display channels are created. As a result, **USB device selection** no longer becomes unusable in the described scenario.

BZ#1096717

Due to a bug in the fullscreen configuration of virt-viewer, the guest resolution was set incorrectly after leaving and re-entering fullscreen mode when **virt-viewer** was launched with the **--full screen=auto-conf** option. This update fixes the bug and screen resolution is now always adjusted properly when leaving and re-entering fullscreen mode.

BZ#1029108

Assigning only modifier keys (such as **Ctrl** or **Alt**) as the key combination to the **--hotkeys** option in **virt-viewer** is not possible. When such a combination is set, **virt-viewer** automatically reverts the option to its default value. However, the **release-cursor** function previously did not revert correctly. As a consequence, when a modifier-only hotkey was set for **release-cursor**, the cursor did not release in the guest window. With this update, **release-cursor** reverts correctly when the user attempts to register a modifier-only hotkey, and releasing the cursor in the guest window works as expected.

BZ#1024199

Due to a bug in **remote-viewer**, typing a URI in the **remote-viewer** GUI tool with additional space characters before or after the address previously caused the guest connection to fail. This update fixes the bug and adding spaces before or after the URI no longer prevents **remote-viewer** from connecting to a guest.

BZ#1009513

Prior to this update, when connected to a server with the **--fullscreen=auto-conf** option, leaving fullscreen mode of a guest display and opening another guest display caused the second guest display to open in fullscreen mode rather than in the windowed mode. This update fixes the

problem and the second guest display will now correctly open in the windowed mode in the described circumstances.

BZ#1063238

Due to incorrect association of the **SPICE** client with the Multipurpose Internet Mail Extension (MIME) of the **console.vv** file, **console.vv** was previously opened in a text editor instead of launching a remote desktop session in **remote-viewer**. With this update, the erroneous MIME association has been fixed and the remote desktop session launches correctly.

BZ#1007649

Prior to this update, the **virt-veiwer** interface offered the **Automatically resize** option. However, the availability of the automatic resize function in **virt-viewer** is dependent on the protocol and guest used. Therefore, **Automatically resize** in some cases did not work. Now, automatic guest resizing will only be enabled when the required conditions are met.

BZ#1004051

Due to rounding errors in the client display size calculation, zooming in or out on a window in **virt-viewer** or **remote-viewer** sometimes incorrectly resized the guest display. With this update, the errors have been fixed and zooming now correctly causes the guest display to be scaled up or down rather than resized.

Users of virt-viewer are advised to upgrade to these updated packages, which fix these bugs.

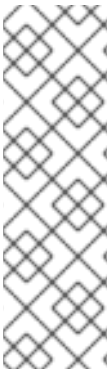
8.255. VIRT-WHO

8.255.1. RHBA-2014:1513 — virt-who bug fix and enhancement update

Updated virt-who package that fixes several bugs and adds various enhancements is now available for Red Hat Enterprise Linux 6.

The virt-who package provides an agent that collects information about virtual guests present in the system and reports them to the Red Hat Subscription Manager tool.

This update also fixes the following bugs:



NOTE

The virt-who package has been upgraded to upstream version 0.10, which provides a number of bug fixes and enhancements over the previous version. This update includes support for multiple vCenter servers, fixed querying by cluster in large ESX environments, corrected communication with Red Hat Satellite server when ESXi has no host, fixed unregistering from Subscription Asset Manager (SAM) server, fixed bug in Virtual Desktop and Server Management (VDSM) mode, support for encrypted credentials, and fixed error when creating new VMs. (BZ#1002640, BZ#994575, BZ#1002447, BZ#1009230, BZ#1011877, BZ#1017056, BZ#1081286, BZ#1082416)

This update also fixes the following bugs:

Bug Fixes

BZ#1098019

Previously, the virt-who daemon did not report guest attributes to the server, which disabled the virt_guest_limit feature. With this update, virt-who has been modified to correctly report guest attributes. As a result, virt_guest_limit is now supported by virt-who.

BZ#1113938

Prior to this update, every call to Libvirtd.listDomains() function from the /usr/share/virt-who/virt/libvirtd/libvirtd.py script opened a new connection to the libvirtd daemon but did not close it. Consequently, after several iterations, virt-who consumed all connections allowed for any client of libvirtd. With this update, Libvirtd.listDomains() has been modified to properly close the livirtd connections, thus fixing this bug.

The virt-who package has been upgraded to upstream version 0.10, which provides a number of bug fixes and enhancements over the previous version. This update includes support for multiple vCenter servers, fixed querying by cluster in large ESX environments, corrected communication with Red Hat Satellite server when ESXi has no host, fixed unregistering from Subscription Asset Manager (SAM) server, fixed bug in Virtual Desktop and Server Management (VDSM) mode, support for encrypted credentials, and fixed error when creating new VMs. (BZ#1002640, BZ#994575, BZ#1002447, BZ#1009230, BZ#1011877, BZ#1017056, BZ#1081286, BZ#1082416)

Users of virt-who are advised to upgrade to this updated package, which fixes these bugs and add these enhancements.

8.256. VTE

8.256.1. RHBA-2014:0638 — vte bug fix update

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

Virtual Terminal Emulator (VTE) is a terminal emulator widget for use in Gtk2 applications.

Bug Fix

BZ#1063741

Previously, Virtual Terminal Emulator (VTE) did not correctly determine how many bytes could be read before performing a UI update and proceeding further. As a consequence, running the cat command on a large text file resulted in the GNOME terminal responding slowly. A patch has been applied to address this bug, and the performance of the GNOME terminal is no longer slowed down in the described situation.

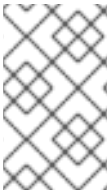
Users of vte are advised to upgrade to these updated packages, which fix this bug.

8.257. WEBKITGTK

8.257.1. RHBA-2014:1573 — webkitgtk bug fix and enhancement update

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

WebKitGTK+ is the port of the portable web rendering engine WebKit to the GTK+ platform.



NOTE

The webkitgtk package has been upgraded to upstream version 1.4.0, which provides a number of bug fixes and enhancements over the previous version. (BZ#1033151, BZ#1101400, BZ#1101401, BZ#1101403, BZ#1119647)

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

8.258. WGET

8.258.1. RHBA-2014:1408 — wget bug fix update

Updated wget packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

GNU Wget is a file retrieval utility which can use either the HTTP, HTTPS, or FTP protocol. 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#909604

Prior to this update, Wget was missing support for Server Name Indication (SNI). As a consequence, Wget was unable to successfully validate certificates from a server using SNI, even if the certificate was valid. The SNI support has been ported to the Wget distributed in Red Hat Enterprise Linux 6, and Wget is now able to successfully validate certificates from any server using SNI, provided the certificate is valid.

BZ#960137

An error in the Wget code prevented Wget from parsing all web links in retrieved pages correctly. Consequently, some links were not followed and pages not retrieved when doing recursive retrieving. The source code has been fixed to parse web links correctly, and all valid links found in the downloaded pages are now parsed and followed correctly in the aforementioned scenario.

BZ#873216

Due to potential resource leaks in the Wget source code, Wget could leak memory in some situations. With this update, the source code has been patched to free resources that could potentially leak, thus fixing this bug.

Users of wget are advised to upgrade to these updated packages, which fix these bugs.

8.259. X3270

8.259.1. RHBA-2014:1494 — x3270 bug fix update

Updated x3270 packages that fix two bugs are now available for Red Hat Enterprise Linux 6.

The x3270 packages contain files needed for emulating the IBM 3278 and 3279 terminals, commonly used with mainframe applications.

Bug Fixes

BZ#1070750

Prior to this update, the x3270 application entered a loop when it was executed with the "-script" option. As a consequence, x3270 terminated unexpectedly with a segmentation fault. With this update, x3270 no longer enters a loop in the above circumstances, and the crash thus no longer occurs.

BZ#961111

Due to an error in the underlying code, some Program Function (PF) keys did not work correctly in the X3270 interface. This error has been fixed and the affected PF keys now work as expected.

Users of x3270 are advised to upgrade to these updated packages, which fix these bugs.

8.260. XCB-UTIL

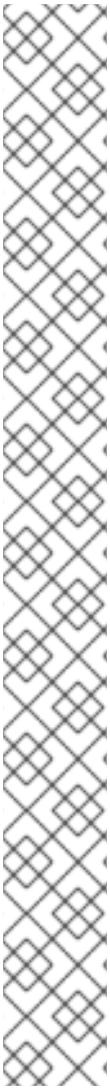
8.260.1. RHBA-2014:1376 xcb-util, xorg-x11-drivers, and mesa bug fix and enhancement update update

Updated xcb-util, xorg-x11-drivers, and mesa packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 6.

The xcb-util package provides a number of libraries that use the libxcb library, the core X protocol library, and some of the extension libraries. These experimental libraries provide convenience functions and interfaces which make the raw X protocol more usable. Some of the libraries also provide client-side code which is not strictly part of the X protocol but which have traditionally been provided by the Xlib library.

The individual X.Org drivers, previously provided by the xorg-x11-drivers package, are included to allow installation of all drivers at once, without having to track which individual drivers are present on each architecture.

This package also provides Mesa 3D graphics API that is compatible with Open Graphics Library (OpenGL), as well as hardware-accelerated drivers for many popular graphics chips.



NOTE

Utilities and drivers contained in the xcb-util package have been upgraded to newer upstream versions to provide a number of fixes and enhancements. The following components have been upgraded: xorg-x11-server, xorg-x11-server-utils, libwacom, xorg-x11-drv-aiptek, xorg-x11-drv-acecad, xorg-x11-drv-elographics, xorg-x11-drv-mutouch, xorg-x11-drv-keyboard, xorg-x11-drv-wacom, xorg-x11-drv-fpit, xorg-x11-drv-vmmouse, xorg-x11-drv-penmount, xorg-x11-drv-mouse, xorg-x11-drv-hyperpen, xorg-x11-drv-void, xorg-x11-drv-evdev, xorg-x11-drv-synaptics, xorg-x11-drv-, xorg-x11-drv-apm, xorg-x11-drv-ast, xorg-x11-drv-ati, xorg-x11-drv-cirrus, xorg-x11-drv-dummy, xorg-x11-drv-fbdev, xorg-x11-drv-geode, xorg-x11-drv-glint, xorg-x11-drv-i128, xorg-x11-drv-i740, xorg-x11-drv-intel, xorg-x11-drv-mach64, xorg-x11-drv-mga, xorg-x11-drv-modesetting, xorg-x11-drv-neomagic, xorg-x11-drv-nouveau, xorg-x11-drv-nv, xorg-x11-drv-openchrome, xorg-x11-drv-qxl, xorg-x11-drv-r128, xorg-x11-drv-rendition, xorg-x11-drv-s3virge, xorg-x11-drv-savage, xorg-x11-drv-siliconmotion, xorg-x11-drv-sis, xorg-x11-drv-sisusb, xorg-x11-drv-tdfx, xorg-x11-drv-trident, xorg-x11-drv-v4l, xorg-x11-drv-vesa, xorg-x11-drv-vmware, xorg-x11-drv-voodoo, xorg-x11-drv-xgi, xorg-x11-apps, xorg-x11-glamor, xorg-x11-proto-devel, xorg-x11-xtrans-devel, xcb-proto, xcb-util, libpciaccess, pixman, mesa, mesa-private-llvm, libdrm. (BZ#1077331, BZ#1088988, BZ#1077472, BZ#1077473, BZ#1077474, BZ#1077475, BZ#1077476, BZ#1077477, BZ#1077478, BZ#1077479, BZ#1077480, BZ#1077481, BZ#1077482, BZ#1077483, BZ#1077484, BZ#1077485, BZ#1077486, BZ#1078370, BZ#1078372, BZ#1078373, BZ#1078374, BZ#1078375, BZ#1078376, BZ#1078377, BZ#1078378, BZ#1078379, BZ#1078380, BZ#1078381, BZ#1078382, BZ#1078383, BZ#1078384, BZ#1078386, BZ#1078387, BZ#1078388, BZ#1078389, BZ#1078390, BZ#1078391, BZ#1078392, BZ#1078394, BZ#1078395, BZ#1078396, BZ#1078397, BZ#1078398, BZ#1078399, BZ#1078400, BZ#1078401, BZ#1078402, BZ#1078403, BZ#1078404, BZ#1078405, BZ#1078410, BZ#1078412, BZ#1078413, BZ#1078414, BZ#1078415, BZ#1078416, BZ#1078417, BZ#1078418, BZ#1078419, BZ#1078420, BZ#1078422, BZ#1061543, BZ#1071697, BZ#1026557, BZ#1022858, BZ#1084244, BZ#1103544)

Bug Fixes

BZ#858838

Under certain rare circumstances, due to a high default color depth setting in the xorg-x11-drv-mga driver, the mouse cursor flickered when moved. This bug has been fixed by setting the default color depth to 16 bpp.

BZ#921641

Previously, the Xephyr display server did not correctly parse the input provided with the -keybd option. Consequently, the -keybd settings were not fully applied. This bug has been fixed and the -keybd settings passed to Xephyr are now correctly parsed and accepted.

BZ#972647

Previously, the pixman library allocated insufficient amount of memory for the create_bits() function when processing PDF files. Consequently, the Evince document viewer terminated unexpectedly when opening PDF files. With this update, pixman has been modified to allocate a sufficient amount of memory when processing PDF files, thus fixing this bug.

BZ#978523

Previously, the "sessreg -a -w" command was not writing the lastlog entry into the log file specified on the command line. With this update, sessreg uses the utmp interface rather than utmpx. Now, when executing the "sessreg -a -w", lastlog entry is recorded to the correct file.

BZ#987701

Prior to this update, front buffer rendering with the software driver from the mesa package resulted in inverted rendering and incorrect readbacks. Consequently, some applications, such as examples in the /usr/lib/mesa/ directory, appeared inverted to the user. This bug has been fixed, and applications using the software driver now render correctly.

BZ#1001757

When using multiple QXL devices with the Xinerama extension, or multiple QXL devices while each being a separate screen, an attempt to set a resolution higher than 1024 x 768 pixels in the xorg.conf file failed with an error. With this update, the underlying source code has been modified and the screen resolution can now be set without complications.

BZ#1011959

Due to a missing dependency of the libGL library on the libX11 library, compiling libraries such as gl2ps failed with the "undefined reference _XgetRequest" message. The dependency has been added and compiling no longer fails with the aforementioned error.

BZ#1025714

Previously, the libGL library from the mesa package was unable to create connections to X servers running GLX 1.2 without fbconfig support. Consequently, all GL applications failed on those servers. This bug has been fixed, and GL applications are now connected to X servers as expected.

BZ#1025804

An attempt to lock a gnome-screensaver instance running within an remote Xnest session through VNC caused the Xnest session to terminate with the following message:

```
X Error of failed request: BadMatch (invalid parameter attributes)
```

This bug has been fixed, and the gnome-screensaver instance can now be locked successfully trough VNC.

BZ#1038082

Previously, the X server occasionally became unresponsive when using the Mozilla Firefox web browser. This bug has been fixed and X server no longer freezes in the aforementioned scenario.

BZ#1056011

The libglamoregl module from the xorg-x11-glamor package was loaded automatically, which caused conflicts if 3rd party drivers were installed. Consequently, Xorg terminated unexpectedly. With this update, libglamoregl is no longer loaded automatically, thus preventing the conflicts and the Xorg crash.

BZ#1057667

In certain cases, when using the Xephyr display server with 8-bit color depth, a color preview window was not automatically updated after modifying the color using sliders. This bug has been fixed and the color preview now correctly reacts to user's settings.

BZ#1076728

Previously, when switching to full screen mode with two monitors with higher resolution (for example, 1920x1200) without changing the resolution on the secondary monitor, the second screen became defected by two dark vertical stripes. The underlying source code has been updated, and automatic

scaling with higher resolution now works as expected.

BZ#1080941

Under certain circumstances, when running the gnome-system-monitor or glxgears utilities in full screen, Xorg used 100% of CPU. With this update, the xorg-x11-drv-mga driver has been fixed and the aforementioned problem no longer occurs.

BZ#1117574

Due to a bug in the xorg-x11-server package, a segmentation fault could occur when executing the "Xorg -configure" command. This bug has been fixed and the segmentation fault no longer occurs in the aforementioned scenario.

BZ#1129819

The xorg-x11-drv-vmware package has been updated to fix a command submission problem on systems that do not have the VMware kms driver installed.

Enhancements

BZ#795925

This update adds support for the AMD Chelsea XT GL M3000 GPU to the mesa package.

BZ#838739

This update adds support for the Lenovo X220 Tablet Touchscreen to the xorg-x11-drv-wacom driver.

BZ#1008692, BZ#1008693

This update adds support for new Wacom Intuos Pro Tablets to the xorg-x11-drv-wacom driver.

BZ#1078424

This update adds the xcb-util-image module to the xcb-utils package. This module provides a port of XImage and XShmImage functions from the Xlib library.

BZ#1078425

This update adds the xcb-util-keysyms module to the xcb-utils package. This module provides standard X key constants and conversion to and from keycodes.

BZ#1078426

This update adds the xcb-util-wm module to the xcb-utils package. This module provides client and window-manager helpers for the ewhm and icccm libraries.

BZ#1084172

This update adds support for AMD Radeon HD 7000 Series and AMD Radeon HD 8000 Series GPUs, excluding GPUs inside AMD Opteron X1150 and X2150 APUs.

Users of xcb-util, xorg-x11-drivers, and mesa are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

8.261. XFSDUMP

8.261.1. RHBA-2014:1565 — xfsdump bug fix update

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

The xfsdump packages provide several utilities for managing XFS file systems, including xfsrestore and xfsdump.

Users of xfsdump are advised to upgrade to these updated packages, which fix these bugs.

8.262. XFSPROGS

8.262.1. RHBA-2014:1564 — xfsprogs bug update

Updated xfsprogs packages that fix several 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#1018751

Due to a bug in the underlying source code, an attempt to use the xfs_io "pwrite" command to write to a block device residing on an XFS file system failed with the following error:

XFS_IOC_FSGEOMETRY: Inappropriate ioctl for device.

This update applies a patch to fix this bug and the command no longer fails in the described scenario.

BZ#1020438

Previously, the thread local data were used incorrectly. As a consequence, when the xfs_repair utility was executed with the ag_stride option, the utility could terminate unexpectedly with a segmentation fault. The underlying source code has been modified to fix this bug and xfs_repair no longer crashes in the described situation.

BZ#1024702

Under certain conditions, the xfs_fsr utility failed to reorganize files with SELinux attributes. With this update, a patch has been provided to address this bug and xfs_fsr can successfully defragment files with SELinux attributes.

BZ#1100107, BZ#1104956

When the sector size of the source file system was larger than 512 bytes, the xfs_copy utility could create a corrupted copy of that system. In addition, the utility exited with a non-zero return code in all cases, even if the operation was successful. This update applies a patch to fix these bugs and the utility now works as expected.

Users of xfsprogs are advised to upgrade to these updated packages, which fix these bugs.

8.263. XGUEST

8.263.1. RHBA-2014:0538 — xguest bug fix update

An updated xguest package that fixes two bugs is now available for Red Hat Enterprise Linux 6.

The xguest package sets up the xguest user which can be used as a temporary account to switch to or as a kiosk user account. These accounts are disabled unless SELinux is in enforcing mode.

Bug Fixes

BZ#877016

Due to a bug in the dependency requirements for the preinstall scriptlet, installing the xguest package failed because of a dependency problem. This update adds the selinux-policy-targeted package to the dependency list, and installing xguest now works as expected.

BZ#1081413

Previously, the xguest README file did not reflect the current state of the defined xguest SELinux booleans in the SELinux policy. This update modifies the README file to correctly document the current state of the aforementioned booleans.

Users of xguest are advised to upgrade to this updated package, which fixes these bugs.

8.264. XZ

8.264.1. RHBA-2014:0769 — xz bug fix update

Updated xz packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

XZ Utils is an integrated collection of user-space file compression utilities based on the Lempel-Ziv-Markov chain algorithm (LZMA), which performs lossless data compression. The algorithm provides a high compression ratio while keeping the decompression time short.

Bug Fixes

BZ#850898

Previously, the '-h' option of the xzgrep command was not included. As a consequence, the matching lines in the output were prefixed with the corresponding file names. This update adds the '-h' option, and running the 'xzgrep -h' command now suppresses the file name on output as expected.

BZ#863024

Prior to this update, running the 'xzgrep -l' command did not work correctly because the source code did not handle the '-q' option appropriately. As a consequence, an error message was displayed. A patch has been applied to handle the 'grep -q' command in the source code correctly. As a result, running the 'xzgrep -l' suppresses normal output and prints file names with a matching line as expected.

BZ#988703

The xzfgrep command is supposed to act as an alias for the 'xzgrep -F' command. Previously, this alias behavior was not set correctly, and the patterns were processed as regular expressions and not as fixed strings. As a consequence, running the xzfgrep command produced no output. With this update, xzfgrep command works as an alias of the 'xzgrep -F' command, and running the xzfgrep command returns correct output.

BZ#1108085

Previously, the xzgrep command returned exit status 1 when contents of one or more files did not match the requested pattern. With this update, xzgrep returns exit status 0 if there is at least one match of the pattern, which makes the xzgrep behavior consistent with the default grep command behavior.

Users of xz are advised to upgrade to these updated packages, which fix these bugs.

8.265. YUM

8.265.1. RHBA-2014:1410 — yum bug fix update

Updated yum packages that fix several bugs 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#875610

Previously, when the "yum history" command was executed and the /var/lib/yum/history file was missing or empty, the yum utility terminated unexpectedly. With this update, this situation is handled gracefully, and yum no longer crashes.

BZ#883463

If the /var/lib/yum/yumdb file was not writable for some reason, the yum utility terminated unexpectedly. With this update, this scenario is handled gracefully, and yum no longer crashes.

BZ#903634

Previously, if the http_proxy and https_proxy environment variables were set to an address and the "proxy=_none_" option was set in the repository configuration, the yum utility ignored the repository proxy option and used the proxy from the environment variables. A patch has been provided to fix this bug, and the proxy repository configuration option now always overrides the environment variables.

BZ#967121, BZ#1029359

Previously, "yum remove" and "yum grouplist" commands did not respect the "skip_if_unavailable=1" repository property, and failed when the repository was unavailable. As a consequence, the yum utility exited without completion. The underlying source codes have been fixed, the unavailable repository with the "skip_if_unavailabe=1" setting is now skipped, and "yum remove" and "yum grouplist" now work as expected.

BZ#1045415

When the "yum verify" command was executed, the yum utility reported changes to file permissions even though there were not any. A patch has been provided to fix this bug, and yum now provides only reliable reports.

BZ#1061583

When the yum command was executed on a non-C locale, yum terminated unexpectedly. This update adds support to locales, and the localized yum now runs without crashes.

BZ#1065122

Previously, if there was a broken symbolic link in the /etc/yum.repos.d/ directory and the "yum repolist" command was issued, the yum utility terminated unexpectedly. With this update, the unreadable repository files are skipped, and yum no longer crashes.

BZ#1073406

Prior to this update, the yum depsolver did not compare versions of virtual provides. As a consequence, when yum installed a package, the depsolver did not select the package with the highest version of virtual provides. The underlying source code has been patched, and the yum depsolver now respects versions of virtual provides as expected.

BZ#1099195

When the "yum check" command was issued on packages installed with missing pre- or post-dependencies, the yum utility reported RPM database problems, With this update, yum ignores missing pre- or post-dependencies, and "yum check" no longer reports such problems.

BZ#1102575

When environment variables $YUM0-$YUM9 were used in the yum.conf file, these variables were not substituted with their values. The underlying source code has been patched, and the variables are now correctly substituted with their values in yum.conf.

Users of yum are advised to upgrade to these updated packages, which fix these bugs.

8.266. YUM-RHN-PLUGIN

8.266.1. RHBA-2014:1536 — yum-rhn-plugin bug fix update

An updated yum-rhn-plugin package that fixes one bug is now available for Red Hat Enterprise Linux 6.

The yum-rhn-plugin package allows the Yum package manager to access content from Red Hat Network.

Bug Fix

BZ#1051972

An attempt to install a package that was not available or visible to YUM resulted in an empty transaction error. With this update, yum-rhn-plugin reports that the package is unavailable in this situation.

Users of yum-rhn-plugin are advised to upgrade to this updated package, which fixes this bug.

8.267. YUM-UTILS

8.267.1. RHBA-2014:1411 — yum-utils bug fix update

Updated yum-utils packages that fix several bugs are now available for Red Hat Enterprise Linux 6.

The yum-utils packages provide a collection of utilities and examples for the yum package manager to make yum easier and more powerful to use.

Bug Fixes

BZ#676193

Previously, the debuginfo-install utility considered only a certain naming scheme of debuginfo repositories, which Certificate-based Red Hat Network content delivery network (CDN) did not follow. As a consequence, debuginfo-install did not work with the debuginfo repositories created in CDN. With this update, support for the new naming scheme of debuginfo repositories has been added, and debuginfo-install now works with debuginfo CDN repositories as intended.

BZ#808347

Prior to this update, enabled source repositories without their respective binary repositories were automatically disabled. As a consequence, source packages could not be downloaded using the "yumdownloader --source" command. With this update, enabled source repositories are no longer disabled automatically, and the "yumdownloader --source" command now works as expected.

BZ#850612

Prior to this update, the fs-snapshot plugin did not work with the Device Mapper as the "dmsetup splitname" command line interface had changed and no longer supported the "-o" option. More specifically, fs-snapshot did not take snapshots of user's file systems before running a yum transaction. In addition, fs-snapshot did not work with Logical Volumes Management (LVM), failing to create new LVM snapshots. With this update, the plugin adjusts to the new command line interface, thus fixing both bugs.

BZ#981773

Previously, man pages for several utilities, such as repo-rss, repodiff, repoquery, or reposync, were missing. With this update, for each utility a man page has been created.

BZ#984119

When the yum-complete-transaction command was run, the /var/run/yum.pid file was left in the file system. A patch has been applied to yum-complete-transaction to clean the file system, and /var/run/yum.pid is now deleted after yum-complete-transaction finishes.

BZ#1004089

When the user tried to download an RPM using the yumdownloader utility when there had already been the same RPM of a bigger size in the destination directory, RPM was not redownloaded, and only a confusing error was displayed to the user. A patch for handling already downloaded RPMs has been applied, and if the checksum of RPMs does not match the intended, yumdownloader redownloads the RPM.

BZ#1013475

Previously, there was an insufficient check in the yum code. Consequently, under some circumstances, the yum-complete-transaction command removed the complete packages, nearly deleting the whole system, instead of updating them. With this update, yum-complete-transaction is more cautious with package removals, and when finding incomplete or aborted yum transactions on a system, it attempts to complete them.

BZ#1045494

Previously, when a package was removed and the yum post-transaction-action extension for a changed directory was enabled, the "yum remove" command terminated unexpectedly. A patch has been provided to fix the bug, "yum remove" no longer crashes, and post-transaction-action is fulfilled successfully without any exceptions.

BZ#1075705

Previously, executing the "yum-config-manager --setopt='debuglevel=9' --save" command caused the yum-utils utility to terminate unexpectedly. The underlying source code has been patched, and the "yum-config-manager --setopt='debuglevel=9' --save" command is now successfully executed.

BZ#1097560

Previously, running the repoquery command when the RPM database failed to open caused the repoquery utility to terminate unexpectedly. A patch has been applied to fix this bug, and repoquery no longer crashes.

Users of yum-utils are advised to upgrade to these updated packages, which fix these bugs.

APPENDIX A. REVISION HISTORY

Revision 0.1-12 **Tue May 10 2016** **Lenka Špačková**

Moved Btrfs and eCryptfs file systems from Technology Previews to Deprecated Functionality.

Revision 0.1-10 **Thu Apr 07 2016** **Lenka Špačková**

Removed a fixed known issue (in-place upgrade and **zipl**).

Revision 0.1-9 **Thu Jan 21 2016** **Lenka Špačková**

Added information about the removed systemtap-grapher package to the Deprecated Functionality Chapter.

Revision 0.1-8 **Thu June 11 2015** **Jana Švárová**

Update of the Red Hat Enterprise Linux 6.6 Technical Notes.

Revision 0.1-6 **Wed May 27 2015** **Milan Navrátil**

Update of the Red Hat Enterprise Linux 6.6 Technical Notes.

Revision 0.1-5 **Tue Oct 14 2014** **Milan Navrátil**

Release of the Red Hat Enterprise Linux 6.6 Technical Notes.