Red Hat Enterprise Linux 5
5.10 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 5.10
Edition 10

Red Hat Engineering Content Services

Red Hat Enterprise Linux 5 5.10 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 5.10
Edition 10

Red Hat Engineering Content Services

Legal Notice

Abstract

The Red Hat Enterprise Linux 5.10 Technical Notes list and document the changes made to the Red Hat Enterprise Linux 5 operating system and its accompanying applications between Red Hat Enterprise Linux 5.9 and minor release Red Hat Enterprise Linux 5.10.

Table of Contents

Preface

The *Red Hat Enterprise Linux 5.10 Technical Notes* list and document the changes made to the Red Hat Enterprise Linux 5 operating system and its accompanying applications between minor release Red Hat Enterprise Linux 5.8 and minor release Red Hat Enterprise Linux 5.10.

For system administrators and others planning Red Hat Enterprise Linux 5.10 upgrades and deployments, the *Red Hat Enterprise Linux 5.9 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 5.10 Technical Notes* provide a single, organized source for change tracking and compliance testing.

For every user, the *Red Hat Enterprise Linux 5.10 Technical Notes* provide details of what has changed in this new release.

Chapter 1. Technology Previews

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. Erratas 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 to fully support Technology Preview features in a future release.

DFS

Starting with Red Hat Enterprise Linux 5.3, CIFS supports Distributed File System (DFS) as a Technology Preview.

Package: *kernel-2.6.18-371*

LSI 12 Gb/s adapters with the MegaRAID SAS driver

LSI MegaRAID SAS 9360/9380 12Gb/s controllers are now supported as a Technology Preview.

Package: *kernel-2.6.18-371*

CDTB

CTDB is a clustered database based on Samba's Trivial Database (TDB). The *ctdb* package is a cluster implementation used to store temporary data. If an application is already using TBD for temporary data storage, it can be very easily converted to be cluster-aware and use CTDB.

Package: *ctdb-1.0.112-2*

Kerberos support for CIFS mounts

Starting with Red Hat Enterprise Linux 5.9, users can use their Kerberos credentials to perform a CIFS mount.

Package: *samba-client-3.0.33-3.39*

FreeIPMI

FreeIPMI is included in as a Technology Preview. FreeIPMI is a collection of Intelligent Platform Management IPMI system software. It provides in-band and out-of-band software, along with a development library conforming to the Intelligent Platform Management Interface (IPMI v1.5 and v2.0) standards.

For more information about FreeIPMI, refer to http://www.gnu.org/software/freeipmi/

Package: *freeipmi-0.5.1-7*

TrouSerS and tpm-tools

TrouSerS and **`tpm-tools`** are included in this release to enable use of *Trusted Platform Module* (TPM) hardware. TPM hardware features include (among others):

- Creation, storage, and use of RSA keys securely (without being exposed in memory)

- Verification of a platform's software state using cryptographic hashes

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 TPM hardware. **`tpm-tools`** is a suite of tools used to manage and utilize TPM hardware.

For more information about TrouSerS, refer to http://trousers.sourceforge.net/.

Packages: *tpm-tools-1.3.1-1*, *trousers-0.3.1-4*

eCryptfs

eCryptfs is a stacked cryptographic file system for Linux. It mounts on individual directories in existing mounted lower file systems such as EXT3; there is no need to change existing partitions or file systems in order to start using **eCryptfs**. **eCryptfs** is released as a Technology Preview for Red Hat Enterprise Linux 5.9.

For more information about **eCryptfs**, refer to http://ecryptfs.sf.net. You can also refer to https://launchpad.net/ecryptfs for basic setup information.

Package: *ecryptfs-utils-75-8*

Stateless Linux

Stateless Linux, included as a Technology Preview, is a new way of thinking about how a system should be run and managed, designed to simplify provisioning and management of large numbers of systems by making them easily replaceable. This is accomplished primarily by establishing prepared system images which get replicated and managed across a large number of stateless systems, running the operating system in a read-only manner (refer to **`/etc/sysconfig/readonly-root`** for more details).

In its current state of development, the Stateless features are subsets of the intended goals. As such, the capability remains as Technology Preview.

Red Hat recommends that those interested in testing stateless code join the stateless-list@redhat.com mailing list.

The enabling infrastructure pieces for Stateless Linux were originally introduced in Red Hat Enterprise Linux 5.

AIGLX

AIGLX is a Technology Preview feature of the otherwise fully supported X server. It aims to enable GL-accelerated effects on a standard desktop. The project consists of the following:

- A lightly modified X server.
- An updated Mesa package that adds new protocol support.

By installing these components, you can have GL-accelerated effects on your desktop with very few changes, as well as the ability to enable and disable them at will without replacing your X server. AIGLX also enables remote GLX applications to take advantage of hardware GLX acceleration.

Packages: X Window System group of packages.

FireWire

The **`firewire-sbp2`** module is included in this update as a Technology Preview. This module enables connectivity with FireWire storage devices and scanners.

At present, FireWire does not support the following:

- IPv4
- *pcilynx* host controllers
- multi-LUN storage devices
- non-exclusive access to storage devices

In addition, the following issues still exist in FireWire:

- a memory leak in the **SBP2** driver may cause the machine to become unresponsive.
- a code in this version does not work properly in big-endian machines. This could lead to unexpected behavior in PowerPC.

Package: *kernel-2.6.18-371*

Device Failure Monitoring of RAID sets

Device Failure Monitoring, using the **dmraid** and **dmevent_tool** tools, is included in Red Hat Enterprise Linux 5.9 as a Technology Preview. This Technology Preview provides the ability to watch and report device failures on component devices of RAID sets.

Packages: *dmraid-1.0.0.rc13-65*, *dmraid-events-1.0.0.rc13-65*

SGPIO Support for dmraid

Serial General Purpose Input Output (SGPIO) is an industry standard communication method used between a main board and a variety of internal and external hard disk drive bay enclosures. This method can be used to control LED lights on an enclosure through the AHCI driver interface.

In this release, SGPIO support in **dmraid** is included as a technology preview. This will allow **dmraid** to work properly with disk enclosures.

Package: *dmraid-1.0.0.rc13-65*

Kernel Tracepoint Facility

In this update, the kernel marker/tracepoint facility remains a Technology Preview. This interface adds static probe points into the kernel, for use with tools such as **SystemTap**.

Package: *kernel-2.6.18-371*

Software based Fibre Channel over Ethernet (FCoE)

The Fibre Channel over Ethernet (FCoE) driver (fcoe.ko), along with libfc, provides the ability to run FCoE over a standard Ethernet card. This capability is provided as a Technology Preview in Red Hat Enterprise Linux 5.9.

To enable this feature, you must login by writing the network interface name to the **/sys/module/fcoe/parameters/create** file, for example:

```
~]# echo eth6 > /sys/module/fcoe/parameters/create
```

To logout, write the network interface name to the **/sys/module/fcoe/parameters/destroy** file, for example:

```
~]# echo eth6 > /sys/module/fcoe/parameters/destroy
```

For further information on software based FCoE refer to: http://www.open-fcoe.org/open-fcoe/wiki/quickstart.

Red Hat Enterprise Linux 5.9 and later provides full support for FCoE on three specialized hardware implementations. These are: Cisco **fnic** driver, the Emulex **lpfc** driver, and the Qlogic **qla2xx** driver.

Package: *kernel-2.6.18-371*

iSER Support

iSER support, allowing for block storage transfer across a network and provided by the *scsi-target-utils* package, remains a Technology Preview in Red Hat Enterprise Linux 5.9. In this release, single portal and multiple portals on different subnets are supported. There are known issues related to using multiple portals on the same subnet.

To set up the iSER target component install the *scsi-target-utils* and *libibverbs-devel* packages. The library package for the InfiniBand hardware that is being used is also required. For example: host channel adapters that use the **cxgb3** driver the **libcxgb3** package is needed, and for host channel adapters using the **mthca** driver the **libmthca** package is needed.

There is also a known issue relating to connection timeouts in some situations. Refer to BZ#470627 for more information on this issue.

Package: *scsi-target-utils-1.0.14-2*

cman fence_virsh fence agent

The fence_virsh fence agent is provided in this release of Red Hat Enterprise Linux as a Technology Preview. fence_virsh provides the ability for one guest (running as a domU) to fence another using the libvirt protocol. However, as fence_virsh is not integrated with cluster-suite it is not supported as a fence agent in that environment.

Package: *cman-2.0.115-118*

glibc new MALLOC behavior

The upstream **glibc** has been changed to enable higher scalability across many sockets and cores. This is done by assigning threads their own memory pools and by avoiding locking in some situations. The amount of additional memory used for the memory pools (if any) can be controlled using the environment variables **MALLOC_ARENA_TEST** and **MALLOC_ARENA_MAX**.

MALLOC_ARENA_TEST specifies that a test for the number of cores is performed once the number of memory pools reaches this value. **MALLOC_ARENA_MAX** sets the maximum number of memory pools used, regardless of the number of cores.

The **glibc** in the Red Hat Enterprise Linux 5.9 release has this functionality integrated as a Technology Preview of the upstream malloc. To enable the per-thread memory pools the environment variable **MALLOC_PER_THREAD** needs to be set in the environment. This environment variable will become obsolete when this new malloc behavior becomes default in future releases. Users experiencing contention for the malloc resources could try enabling this option.

Package: *glibc-2.5-118*

Chapter 2. Known Issues

2.1. anaconda

The *anaconda* packages provide the installation program used by Red Hat Enterprise Linux to identify and configure the hardware, and to create the appropriate file systems for the system's architecture, as well as to install the operating system software.

- Installing Red Hat Enterprise Linux 5 from a hard drive is possible only if the source partition covers the whole disk. Otherwise, the following warning can appear:

  ```
  The kernel was unable to re-read the partition table on /dev/dasdb (Device
  or resource busy). This means Linux won't know anything about the
  modifications you made until you reboot. You should reboot your computer
  before doing anything with /dev/dasdb.
  ```

  (BZ#846231)

- If a read-only disk is present, installation of Red Hat Enterprise Linux 5 can be interrupted by an interactive warning dialog window, and thus blocking automated installations. (BZ#978250)

- When installing Red Hat Enterprise Linux 5.8 on a machine that had previously used a GPT partitioning table, Anaconda does not provide the option to remove the previous disk layout and is unable to remove the previously used GPT partitioning table. To work around this issue, switch to the tty2 terminal (using **CTRL**+**ALT**+**F2**), execute the following command, and restart the installation process:

  ```
  dd if=/dev/zero of=/dev/USED_DISK count=512
  ```

- Starting with Red Hat Enterprise Linux 5.2, to boot with **ibft**, the iSCSI boot firmware table support, use the **ip=ibft** option as the network install option:

  ```
  ip=<ip>
      IP to use for a network installation, use 'dhcp' for DHCP.
  ```

  By default, the installer waits 5 seconds for a network device with a link. If an iBFT network device is not detected in this time, you may need to specify the ***linksleep=SECONDS*** parameter in addition to the ***ip=ibft*** parameter by replacing ***SECONDS*** with an integer specifying the number of seconds the installer should wait, for example:

  ```
  linksleep=10
  ```

- Setting the ***dhcptimeout=0*** parameter does not mean that DHCP will disable timeouts. If the user requires the clients to wait indefinitely, the ***dhcptimeout*** parameter needs to be set to a large number.

- When starting an installation on IBM S/390 systems using SSH, re-sizing the terminal window running the SSH client may cause the installer to unexpectedly exit. Once the installer has started in the SSH session, do not resize the terminal window. If you want to use a different size terminal window during installation, re-size the window before connecting to the target system via SSH to begin installation.

- Installing on June with a RAID backplane on Red Hat Enterprise Linux 5.7 and later does not work properly. Consider the following example: a test system which had two disks with two redundant paths to each disk was set up:

```
mpath0: sdb, sdd
mpath1: sda, sdc
```

In the above setup, Anaconda created the PReP partition on mpath0 (sdb/sdd), but set the bootlist to boot from sda. To work around this issue, follow these steps:

- Add **mpath** to the append line in the **/etc/yaboot.conf** file.
- Use the **--ondisk=mapper/mpath0** in all **part** directives of the kickstart file.
- Add the following script to the **%post** section of the kickstart file.

```
%post
# Determine the boot device
device=;

# Set the bootlist in NVRAM
if [ "z$device" != "z" ]; then
bootlist -m normal $device;

# Print the resulting boot list in the log
bootlist -m normal -o;
bootlist -m normal -r;
else
echo "Could not determine boot device!";
exit 1;
fi
```

The above script simply ensures that the bootlist is set to boot from the disk with the PReP partition.

- Mounting an NFS volume in the rescue environment requires **portmap** to be running. To start **portmap**, run:

```
/usr/sbin/portmap
```

Failure to start **portmap** will return the following NFS mount errors:

```
sh-3.2# mount 192.168.11.5:/share /mnt/nfs
mount: Mounting 192.168.11.5:/share on /mnt/nfs failed: Input/output error
```

- 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, be sure to verify the storage device size, name, and type when configuring partitions and file systems.

- **anaconda** occasionally crashes while attempting to install on a disk containing partitions or file systems used by other operating systems. To workaround this issue, clear the existing partition table using the command:

```
clearpart --initlabel [disks]
```

(BZ#530465)

- Performing a System z installation, when the **install.img** is located on direct access storage device (DASD) disk, causes the installer to crash, returning a backtrace. **anaconda** is attempting to re-write (commit) all disk labels when partitioning is complete, but is failing because the partition is busy. To work around this issue, a non-DASD source should be used for **install.img**. (BZ#455929)

- When installing to an **ext3** or **ext4** file system, **anaconda** disables periodic file system checking. Unlike **ext2**, these file systems are journaled, removing the need for a periodic file system check. In the rare cases where there is an error detected at runtime or an error while recovering the file system journal, the file system check will be run at boot time. (BZ#513480)

- Red Hat Enterprise Linux 5 does not support having a separate **/var** on a network file system (**nfs**, **iSCSI** disk, **nbd**, etc.) This is because **/var** contains the utilities required to bring up the network, for example **/var/lib/dhcp**. However, you may have **/var/spool**, **/var/www** or the like on a separate network disk, just not the complete /var file system. (BZ#485478)

- When using rescue mode on an installation which uses iSCSI drives which were manually configured during installation, the automatic mounting of the root file system does not work. You must configure iSCSI and mount the file systems manually. This only applies to manually configured iSCSI drives; iSCSI drives which are automatically detected through iBFT are fully supported in rescue mode.

  To rescue a system which has **/** on a non-iBFT configured iSCSI drive, choose to skip the mounting of the root file system when asked, and then follow the steps below:

```
$TARGET_IP: IP address of the iSCSI target (drive)
$TARGET_IQN: name of the iSCSI target as printed by the discovery command
$ROOT_DEV: devicenode (/dev/.....) where your root fs lives
```

  - Define an initiator name:

```
$ mkdir /etc/iscsi
$ cat << EOF>> /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.1994-05.com.fedora:d62f2d7c09f
EOF
```

  - Start iscsid:

```
$ iscsid
```

  - Discover and login to target:

```
$ iscsiadm -m discovery -t st -p $TARGET_IP
$ iscsiadm -m node -T $TARGET_IQN -p $TARGET_IP --login
```

  - If the iSCSI LUN is part of a LVM Logical volume group:

```
$ lvm vgscan
$ lvm vgchange -ay
```

  - Mount your **/** partition:

```
$ mount /dev/path/to/root /mnt/sysimage
$ mount -t bind /dev /mnt/sysimage/dev
$ mount -t proc proc /mnt/sysimage/proc
$ mount -t sysfs sysfs /mnt/sysimage/sys
```

- Now you can **chroot** to the root file system of your installation if wanted

```
$ chroot /mnt/sysimage /bin/su -
```

- When installing KVM or Xen guests, always create a partition for the guest disk, or create an LVM volume. Guests should not be installed to block devices or raw disk devices. Anaconda includes disk label duplication avoidance code, but when installing within a VM, it has no visibility to the disk labels elsewhere on the host and cannot detect duplicates.

  If guest file systems, especially the root file system, are directly visible to the host, a host OS reboot may inadvertently parse the partition table and mount the guest file systems. This can lead to highly undesirable outcomes.

- The minimum memory requirement when installing all Red Hat Enterprise Linux packages (i.e. ***** or **@everything** is listed in the **%packages** section of the **kickstart** file) on a fully virtualized Itanium guest is 768MB. After installation, the memory allocated to the guest can be lowered to the desired amount.

- Upgrading a system using Anaconda is not possible if the system is installed on disks attached using zFCP or iSCSI (unless booted from the disk using a network adapter with iBFT). Such disks are activated after Anaconda scans for upgradable installations and are not found. To update please use the Red Hat Network with the hosted Web user interface, a Red Hat Network Satellite, the local graphical Updater, or the yum command line.

- Anaconda's graphical installer fails to start at the default 800x600 resolution on systems utilizing Intel Graphics Device Next Generation (IGDNG) devices. To work around this issue, ensure anaconda uses a higher resolution by passing the parameters **resolution=1024x768** or **resolution=1280x1024** to the installer using the boot command line.

- The NFS default for RHEL5 is **locking**. Therefore, to mount **nfs** shares from the **%post** section of anaconda, use the **mount -o nolock,udp** command to start the locking daemon before using **nfs** to mount shares. (BZ#426053)

- If you are using the Virtualized kernel when upgrading from Red Hat Enterprise Linux 5.0 to a later 5.x release, you must reboot after completing the upgrade. You should then boot the system using the updated Virtualized kernel.

  The hypervisor ABI changes in an incompatible way between Red Hat Enterprise Linux 5 and 5.1. If you do not boot the system after upgrading from Red Hat Enterprise Linux 5.0 using the updated Virtualized kernel, the upgraded Virtualization RPMs will not match the running kernel. (BZ#251669)

- When upgrading from Red Hat Enterprise Linux 4.6 to Red Hat Enterprise Linux 5.1 or later, **gcc4** may cause the upgrade to fail. As such, you should manually remove the *gcc4* package before upgrading. (BZ#432773)

- When provisioning guests during installation, the **RHN tools for guests** option will not be available. When this occurs, the system will require an additional entitlement, separate from the entitlement used by **dom0**.

  To prevent the consumption of additional entitlements for guests, install the **rhn-virtualization-common** package manually before attempting to register the system to Red Hat Network. (BZ#431648)

- When installing Red Hat Enterprise Linux 5 on a guest, the guest is configured to explicitly use a temporary installation kernel provided by **dom0**. Once installation finishes, it can then use its own bootloader. However, this can only be achieved by forcing the guest's first reboot to be a shutdown.

  As such, when the **Reboot** button appears at the end of the guest installation, clicking it shuts down the guest, but does not reboot it. This is an expected behavior.

Note that when you boot the guest after this it will then use its own bootloader.

- Using the **`swap --grow`** parameter in a **`kickstart`** file without setting the **`--maxsize`** parameter at the same time makes anaconda impose a restriction on the maximum size of the swap partition. It does not allow it to grow to fill the device.

  For systems with less than 2GB of physical memory, the imposed limit is twice the amount of physical memory. For systems with more than 2GB, the imposed limit is the size of physical memory plus 2GB. (BZ#462734)

- Existing encrypted block devices that contain **`vfat`** file systems will appear as type **`foreign`** in the partitioning interface; as such, these devices will not be mounted automatically during system boot. To ensure that such devices are mounted automatically, add an appropriate entry for them to **`/etc/fstab`**. For details on how to do so, refer to **`man fstab`**. (BZ#467202)

- When using anaconda's automatic partitioning on an IBM System p partition with multiple hard disks containing different Linux distributions, the anaconda installer may overwrite the bootloaders of the other Linux installations although their hard disks have been unchecked. To work around this, choose manual partitioning during the installation process.

The following known issue applies to the PowerPC architecture:

- The minimum RAM required to install Red Hat Enterprise Linux 5.8 is 1GB; the recommended RAM is 2GB. If a machine has less than 1GB RAM, the installation process may hang.

  Furthermore, PowerPC-based machines that have only 1GB of RAM experience significant performance issues under certain RAM-intensive workloads. For a Red Hat Enterprise Linux 5.8 system to perform RAM-intensive processes optimally, 4GB of RAM is recommended. This ensures the system has the same number of physical pages as was available on PowerPC machines with 512MB of RAM running Red Hat Enterprise Linux 4.5 or earlier.

The following known issue applies to the IBM System z architecture:

- Installation on a machine with existing Linux or non-Linux file systems on DASD block devices may cause the installer to halt. If this happens, it is necessary to clear out all existing partitions on the DASD devices you want to use and restart the installer.

The following known issue applies to the Itanium architecture:

- If your system only has 512MB of RAM, attempting to install Red Hat Enterprise Linux 5.4 may fail. To prevent this, perform a base installation first and install all other packages after the installation finishes. (BZ#435271)

2.2. autofs

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

- When using NFSv4 with a global root, **autofs** has no way to know which server export path corresponds to the global root. Consequently, the internal hosts map fails to mount server exports. For detailed information on this problem, refer the following Knowledge Base article:

  https://access.redhat.com/site/solutions/39397

- Starting with Red Hat Enterprise Linux 5.4, behavior of the **`umount -l`** autofs command has changed. For more information, refer to BZ#452122.

Previously, the **umount -l** would unmount all autofs-managed mounts and autofs internal mounts at start-up, and then mounted all autofs mounts again as a part of the start-up procedure. As a result, the execution of the external **umount -l** command was not needed.

The previous autofs behavior can be used via the following commands:

```
~]# service autofs forcerestart
```

or

```
~]# service autofs forcestart
```

2.3. cmirror

The *cmirror* packages provide user-level utilities for managing cluster mirroring.

- Due to limitations in the cluster infrastructure, cluster mirrors greater than 1.5TB cannot be created with the default region size. If larger mirrors are required, the region size should be increased from its default (512kB), for example:

  ```
  # -R <region_size_in_MiB>
  lvcreate -m1 -L 2T -R 2 -n mirror vol_group
  ```

  Failure to increase the region size will result in the LVM creation process hanging and may cause other LVM commands to hang. (BZ#514814)

2.4. cpio

The cpio packages provide the GNU cpio file archiver utility. GNU cpio can be used to copy and extract files into or from cpio and Tar archives.

- The cpio utility uses a default block size of 512 bytes for I/O operations. This may not be supported by certain types of tape devices. If a tape device does not support this block size, cpio fails with the following error message:

  ```
  cpio: read error: Cannot allocate memory
  ```

  To work around this issue, modify the default block size with the **--block-size long** option, or use the **-B** option to set the block size to 5120 bytes. When the block size supported by the tape device is provided, the cpio utility works as expected. (BZ#573943)

2.5. openswan

The *cpuspeed* packages provide a daemon to manage the CPU frequency scaling.

- When the frequency scaling is enabled, a kernel panic can occur on a HMV (Hardware Virtual Machine) guest, and the following message is logged:

  ```
  Kernel panic - not syncing: IO-APIC + timer doesn't work!
  ```

To work around this problem, change the default CPU governor to *performance* in the **/etc/sysconfig/cpuspeed** file as follows: **GOVERNOR=performance**.

2.6. compiz

Compiz is an OpenGL-based window and compositing manager.

- Running **rpmbuild** on the **compiz** source RPM will fail if any KDE or **qt** development packages (for example, **qt-devel**) are installed. This is caused by a bug in the **compiz** configuration script.

  To work around this, remove any KDE or **qt** development packages before attempting to build the **compiz** package from its source RPM. (BZ#444609)

2.7. device-mapper-multipath

The *device-mapper-multipath* packages provide tools to manage multipath devices using the device-mapper multipath kernel module.

- Note that under certain circumstances, the multipathd daemon can terminate unexpectedly during shutdown.
- It is possible to overwrite the default hardware table. However, regular expression matches are not allowed; the vendor and product strings need to be matched exactly. These strings can be found by running the following command:

  ```
  ~]# multipathd -k"show config"
  ```

- By default, the **multipathd** service starts up before the **iscsi** service. This provides multipathing support early in the bootup process and is necessary for multipathed iSCSI SAN boot setups. However, once started, the **multipathd** service adds paths as informed about them by udev. As soon as the **multipathd** service detects a path that belongs to a multipath device, it creates the device. If the first path that multipathd notices is a passive path, it attempts to make that path active. If it later adds a more optimal path, **multipathd** activates the more optimal path. In some cases, this can cause a significant overhead during a startup.

  If you are experiencing such performance problems, define the **multipathd** service to start after the **iscsi** service. This does not apply to systems where the root device is a multipathed iSCSI device, since it the system would become unbootable. To move the service start time run the following commands:

  ```
  ~]# mv /etc/rc5.d/S06multipathd /etc/rc5.d/S14multipathd
  ~]# mv /etc/rc3.d/S06multipathd /etc/rc3.d/S14multipathd
  ```

  To restore the original start time, run the following command:

  ```
  ~]# chkconfig multipathd resetpriorities
  ```

  (BZ#500998)

- Running the **multipath** command with the **-ll** option can cause the command to hang if one of the paths is on a blocking device. Note that the driver does not fail a request after some time if the device does not respond.

  This is caused by the cleanup code, which waits until the path checker request either completes or fails. To display the current **multipath** state without hanging the command, use **multipath -l** instead.

(BZ#214838)

2.8. dmraid

The *dmraid* packages contain the ATARAID/DDF1 activation tool that supports RAID device discovery, RAID set activation, and displays properties for ATARAID/DDF1 formatted RAID sets on Linux kernels using device-mapper.

- The installation procedure stores the name of RAID volume and partition in an initscript. When the system boots, dmraid enables the RAID partition (that are named implicitly in the init script. This action functions until the volume and partition names are changed. In these cases, the system may not boot, and the user is given an option to reboot system and start the rebuild procedure in OROM.

  OROM changes the name of RAID volume (as seen by dmraid) and dmraid cannot recognize the array identified by previous name stored in initscript. The system no longer boots from RAID partition, since it is not enabled by dmraid. In case of RAID 1 (mirror), the system may be booted from disk that is part of RAID volume. However, dmraid does not allow to active or rebuild the volume which component in mounted.

  To work around this issue, do not rebuild the RAID array in OROM. Start the rebuild procedure by dmraid in the operating system, which performs all the steps of rebuilding. dmraid does not change the RAID volume name, therefore the system can be booted from RAID array without the need of init script modification.

  To modify init script after OROM has started rebuild:

  - Start the system in rescue mode from the installation disk, skip finding and mounting previous installations.
  - At the command line, find and enable the raid volume that is to be booted from (the RAID volume and partitions will be activated)

    ```
    ~]# dmraid -ay isw_effjffhbi_Volume0
    ```

  - Mount the root partition:

    ```
    ~]# mkdir /tmp/raid
    ~]# mount /dev/mapper/isw_effjffhbi_Volume0p1 /tmp/raid
    ```

  - Decompress the boot image:

    ```
    ~]# mkdir /tmp/raid/tmp/image
    ~]# cd /tmp/raid/tmp/image
    ~]# gzip -cd /tmp/raid/boot/inird-2.6.18-155.el5.img | cpio -imd –
    quiet
    ```

  - Change the names of the RAID volumes in the initscript to use the new names of RAID:

    ```
    ~]# dmraid –ay –I –p –rm_partition
    “/dev/mapper/isw_effjffhbi_Volume0”
    ~]# kpartx –a –p p “/dev/mapper/isw_effjffhbi_Volume0”
    ~]# mkrtootdev –t ext3 –o defaults,ro
    /dev/mapper/isw_effjffhbi_Volume0p1
    ```

  - Compress and copy initrd image with the modified init script to the boot directory

```
~]# cd /tmp/raid/tmp/image
~]# find . –print | cpio –c –o | gzip -9 > /tmp/raid/boot/inird-
2.6.18-155.el5.img
```

- Unmount the raid volume and reboot the system:

```
~]# umount /dev/mapper/isw_effjffhbi_Volume0p1
~]# dmraid -an
```

2.9. dogtail

dogtail is a GUI test tool and automation framework that uses assistive technologies to communicate with desktop applications.

- Attempting to run **`sniff`** may result in an error. This is because some required packages are not installed with **`dogtail`**. (BZ#435702)

  To prevent this from occurring, install the following packages manually:

  - *librsvg2*
  - *ghostscript-fonts*
  - *pygtk2-libglade*

2.10. file

The File utility is used to identify a particular file according to the type of data contained in the file.

- The **file** utility can exit with the 0 exit code even if some input files have not been found. This behavior is correct; refer to the file(1) man page for more information.

2.11. firefox

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

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

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

2.12. firstboot

The **firstboot** utility runs after installation. It guides the user through a series of steps that allows for easier configuration of the machine.

The following known issue applies to the IBM System z architecture:

- When **firstboot** is running in text mode, the user can only register to Red Hat Netwrork legacy, not with **subscription-manager**. When **firstboot** is running in GUI mode, both options are available.
- The *IBM System z* does not provide a traditional Unix-style physical console. As such, Red Hat Enterprise Linux 5 for the *IBM System z* does not support the *firstboot* functionality during initial program load.

  To properly initialize setup for Red Hat Enterprise Linux 5 on the *IBM System z*, run the following commands after installation:

  - **/usr/bin/setup** — provided by the **setuptool** package.
  - **/usr/bin/rhn_register** — provided by the **rhn-setup** package.

  (BZ#217921)

2.13. gfs2-utils

The *gfs2-utils* packages provide the user-level tools necessary to mount, create, maintain and test **GFS2** file systems.

If gfs2 is used as the root file system, the first boot attempt will fail with the error message "**fsck.gfs2: invalid option -- a**". To work around this issue:

1. Enter the root password when prompted.
2. Mount the root file system manually:

   ```
   ~]# mount -o remount,rw /dev/VolGroup00/LogVol00 /
   ```

3. Edit the /etc/fstab file from:

   ```
   /dev/VolGroup00/LogVol00 / gfs2 defaults 1 1
   ```

   to

   ```
   /dev/VolGroup00/LogVol00 / gfs2 defaults 1 0
   ```

4. Reboot the system.

Important

Note, however that using **GFS2** as the root file system is unsupported.

2.14. gnome-volume-manager

The GNOME Volume Manager monitors volume-related events and responds with user-specified policy. The GNOME Volume Manager can automount hot-plugged drives, automount inserted removable media, autorun programs, automatically play audio CDs and video DVDs, and automatically import photos from a digital camera.

- Removable storage devices (such as CDs and DVDs) do not automatically mount when you are logged in as root. As such, you will need to manually mount the device through the graphical file manager.

  Alternatively, you can run the following command to mount a device to **/media**:

  ```
  mount /dev/[device name] /media
  ```

2.15. grub

The GRUB utility is responsible for booting the operating system kernel.

- Executing the **grub-install** command fails if the name of a volume group intended to be used for booting contains only non-digit characters. To prevent this problem, it is recommended to name the volume group with a combination of non-digit text followed by a digit; for example, *system0*.

2.16. initscripts

The *initscripts* package contains system scripts to boot your system, change runlevels, activate and deactivate most network interfaces, and shut the system down cleanly.

- On systems with more than two encrypted block devices, anaconda has a option to provide a global passphrase. The init scripts, however, do not support this feature. When booting the system, entering each individual passphrase for all encrypted devices will be required. (BZ#464895)
- Boot-time logging to **/var/log/boot.log** is not available in Red Hat Enterprise Linux 5. (BZ#223446, BZ#210136)

2.17. ipa-client

The ipa-client package provides a tool to enroll a machine to an IPA version 2 server. IPA (Identity, Policy and Audit) is an integrated solution to provide centrally managed identity, that is, machine, user, virtual machines, groups, and authentication credentials.

- Sometimes, the **krb5.conf** file contains incorrect SELinux context, namely, when the krb5.conf is not created by default, or the IPA client is installed, un-installed, or re-installed. AVC denials can therefore occur in such scenarios.
- Attempting to run the **ipa-client-install** command with the **--no-sssd** option fails with the following error message:

  ```
  authconfig: error: no such option: --enableforcelegacy
  ```

  (BZ#852746)

2.18. iscsi-initiator-utils

The *iscsi* package provides the server daemon for the 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 networks.

- Broadcom L2 iSCSI (Internet Small Computer System Interface) boot is not supported in Red Hat Enterprise Linux 5. (BZ#831681)

2.19. kernel-xen

Xen is a high-performance and secure open-source virtualization framework. The virtualization allows users to run guest operating systems in virtual machines on top of a host operating system.

- The Xen hypervisor will not start when booting from an iSCSI disk. To work around this issue, disable the Xen hypervisor's EDD feature with the "edd=off" kernel parameter. For example:

  ```
  kernel /xen.gz edd=off
  ```

  (BZ#568336)

- With certain hardware, **blktap** may not function as expected, resulting in slow disk I/O causing the guest to operate slowly also. To work around this issue, guests should be installed using a physical disk (i.e. a real partition or a logical volume). (BZ#545692)

- When booting paravirtualized guests that support gigabyte page tables (i.e. a Fedora 11 guest) on Red Hat Enterprise Linux 5.7 Xen, the domain may fail to start if more than 2047MB of memory is configured for the domain. To work around this issue, pass the "**nogbpages**" parameter on the guest kernel command-line. (BZ#502826)

- Boot parameters are required to enable SR/IOV Virtual Function devices. SR/IOV Virtual Function devices can only be accessed if the parameter pci_pt_e820_access=on is added to the boot stanza in the /boot/grub/grub.conf file. For example:

  ```
  title Red Hat Enterprise Linux Server (2.6.18-152.el5xen)
  root (hd0,1)
  kernel /xen.gz-2.6.18-152.el5 com1=115200,8n1 console=com1 iommu=1
  module /vmlinuz-2.6.18-152.el5xen ro root=LABEL=/ console=ttyS0,115200
  pci_pt_e820_access=on
  ```

  This enables the MMCONF access method for the PCI configuration space, a requirement for VF device support

- Diskette drive media will not be accessible when using the virtualized kernel. To work around this, use a USB-attached diskette drive instead.

  Note that diskette drive media works well with other non-virtualized kernels. (BZ#401081)

- Fully virtualized guests cannot correct for time lost due to the domain being paused and unpaused. Being able to correctly track the time across pause and unpause events is one of the advantages of paravirtualized kernels. This issue is being addressed upstream with replaceable timers, so fully virtualized guests will have paravirtualized timers. Currently, this code is under development upstream and should be available in later versions of Red Hat Enterprise Linux. (BZ#422531)

The following known issue applies to the Intel 64 and AMD64 architectures:

- Upgrading a host (**dom0**) system to Red Hat Enterprise Linux 5.7 may render existing Red Hat Enterprise Linux 5.4 SMP paravirtualized guests unbootable. This is more likely to occur when the host system has more than 4GB of RAM.

  To work around this, boot each Red Hat Enterprise Linux 5.4 guest in single CPU mode and upgrade its kernel to the latest version (for Red Hat Enterprise Linux 5.4.z). (BZ#253087, BZ#251013)

The following known issues apply to the Itanium architecture:

- On some *Itanium* systems configured for console output to VGA, the **dom0** virtualized kernel may fail to boot. This is because the virtualized kernel failed to properly detect the default console device from the *Extensible Firmware Interface* (EFI) settings.

  When this occurs, add the boot parameter **console=tty** to the kernel boot options in **/boot/efi/elilo.conf**. (BZ#249076)

- On some *Itanium* systems (such as the *Hitachi Cold Fusion 3e*), the serial port cannot be detected in **dom0** when VGA is enabled by the EFI Maintenance Manager. As such, you need to supply the following serial port information to the **dom0** kernel:

  - Speed in bits/second
  - Number of data bits
  - Parity
  - **io_base** address

  These details must be specified in the **append=** line of the **dom0** kernel in **/boot/efi/elilo.conf**. For example:

  ```
  append="com1=19200,8n1,0x3f8 -- quiet rhgb console=tty0
  console=ttyS0,19200n8"
  ```

  In this example, **com1** is the serial port, **19200** is the speed (in bits/second), **8n1** specifies the number of data bits/parity settings, and **0x3f8** is the **io_base** address. (BZ#433771)

- Virtualization does not work on some architectures that use Non-Uniform Memory Access (NUMA). As such, installing the virtualized kernel on systems that use NUMA will result in a boot failure.

  Some installation numbers install the virtualized kernel by default. If you have such an installation number and your system uses NUMA and does not work with kernel-xen, deselect the Virtualization option during installation.

2.20. kernel

The *kernel* packages contain the Linux kernel, the core of any Linux operating system.

- On Microsoft Hyper-V, a Red Hat Enterprise Linux 5 guest can start with more memory than the host's NUMA node memory, which results in a kernel panic on the guest. To prevent the crash in this scenario, set the **numa=off** boot parameter on the kernel command line.

- 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
```

- The **sar** and **sadf** commands can terminate unexpectedly with a segmentation fault when run on 64-bit PowerPC architecture. (BZ#BZ#984866)
- Hardware support for Intel/QLogix QLE7300 series InfiniBand adapters, which was included in Red Hat Enterprise Linux 5.9, has been removed at Red Hat Enterprise Linux 5.10. Please refer to Red Hat Knowledge Solution 426383 for more information.
- Earlier versions of the Broadcom MFW firmware on bnx2x devices have known bugs. A specific link problem is known to affect BCM57810 based devices with 10GBASE-KR connections. Consequently, depending on the exact timing, the network interface can fail to establish the link. To establish a more reliable link, update the MFW firmware on the bnx2x device's EEPROM (Electrically Erasable Programmable Read-Only Memory) to version 7.4.19 or later. The current version can be checked running **ethtool -i $NET_DEVICE | grep firmware-version**. Please consult your hardware vendor or manufacturer for instructions on how to update the MFW firmware on bnx2x devices.
- The Emulex **lpfc** driver is missing functionality required to support 16 Gb point-to-point configurations for all adapters in Red Hat Enterprise Linux 5. All other currently available 16 Gb **lpfc** configurations are supported on most adapters available. Specifically, the LPe16000B adapter is not supported for any configuration, and the LPe16000A adapter is supported for all configurations besides a point-to-point configuration.
- Red Hat Enterprise Linux 5 can become unresponsive or even terminate due to the lack of ticketed spinlocks in the **shrink_active_list()** function.
- When USB hardware uses the ACM interface, there is a race condition that can lead to a system deadlock due to the spinlocks not disabling interrupts. This has been noticed through various types of softlockups. To workaround this problem, reboot the machine.
- If **kdump** is configured on an i686 system using a non-PAE kernel and memory larger than 4 GB, it creates an elf core header which includes extra unavailable memory range. This causes **kdump** to become unresponsive.
- A large number of kernel log messages may flood **netconsole** while under heavy RX traffic, causing the **netconsole** kernel module to stop working. To work around this issue, avoid the use of **netconsole**, or remove the netconsole module using the **rmmod netconsole** command and re-configure it again using the **insmod netconsole** command.
- To update firmware on Mellanox cards, use **mstflint** which replaces the outdated **tvflash** utility.
- The kernel in Red Hat Enterprise Linux 5 does not support Data Center Bridging (DCB). Software-based Fibre Channel over Etherner (FCoE) is a Technology Preview and it is therefore recommended to use Red Hat Enterprise Linux 6 for fully supported software-based FCoE. The following hardware-accelerated FCoE cards are fully supported in Red Hat Enterprise Linux 5: Emulex LPFC, QLogic qla2xxx, Brocade BFA. (BZ#860112)
- The following problems can occur when using Brocade 1010 and 1020 Converged Network Adapters (CNAs):
  - BIOS firmware may not be able to log in the Fibre Channel over Ethernet (FCoE) session when loading a Brocade optional BIOS, which causes the server to be unable to boot and the following error message to appear:

    ```
    Adapter 1/0/0 Link initialization failed. Disabling BIOS
    ```

- Configuration cannot be saved via serial port of the server. Use a physical console or Brocade HSM software.

Contact Brocade for additional information on these problems.

- 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 error messages to continuously appear 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 problem, unload the Brocade BFA driver.

- Master Boot Record (MBR) or the /boot partition can be installed on an incorrect disk if the server boots from storage area network (SAN) with many Logical Unit Numbers (LUNs) assigned. To work around this problem, partition the space manually so that the operating system uses only the boot LUN as the root (/) and /boot partitions. (BZ#852305)

- Qemu-kvm does not check if a given CPU flag is really supported by the KVM kernel module. Attempting to enable the "acpi" flag can lead to a kernel panic on guest machines. To work around this problem, do not enable the "acpi" CPU flag in the configuration of a virtual machine. (BZ#838921)

- Running the **`ethtool --identify`** command in a production environment blocks network traffic and certain network configuration operations until **ethtool** is aborted. To prevent this problem, do not run **`ethtool --identify`** in a production environment; this command is supposed for debugging purposes only.

- Starting with Red Hat Enterprise Linux 5.8, the size of I/O operations allowed by the NFS server has been increased by default. The new default max block size varies depending on RAM size, with a maximum of 1M (1048576 bytes).

  This may cause problems for 32-bit servers configured to use large numbers of **`nfsd`** threads. For such servers, we recommend decreasing the number of threads, or decreasing the I/O size by writing to the **`/proc/fs/nfsd/max_block_size`** file before starting **`nfsd`**. For example, the following command restores the previous default ***`iosize`*** of 32k:

```
~]# echo 32767 >/proc/fs/nfsd/max_block_size
```

  (BZ#765751)

- If the **`qla4xxx`** driver fails to discover all iSCSI targets, make sure to **`Clear Persistent Targets`** and set up iSCSI again via **`CTRL`**+**`Q`** in the Qlogic iSCSI option ROM BIOS.

- The OProfile infrastructure in Red Hat Enterprise Linux 5 does not support the hardware performance counters of the AMD family 0x15 processor family; profiling is only available in timer interrupt mode. When profiling on bare metal, OProfile automatically selects the timer interrupt mode. When running under kernel-xen, due to different CPU family reporting, OProfile must be explicitly configured to use timer interrupt mode. This is possible by adding **`options oprofile timer=1`** to the **`/etc/modprobe.conf`** file. (BZ#720587)

- Red Hat Enterprise Linux 5 may become unresponsive due to the lack of ticketed spinlocks in the **`shrink_active_list()`** function. As a result, the **`spin_lock_irq(&zone->lru_lock)`** operation disables interrupts, and the following error message is returned when the system hangs:

```
NMI Watchdog detected LOCKUP
```

- Booting a Red Hat Enterprise Linux 5 system with a connected DVD drive and the **smartd**service running hangs with the following error messages:

```
Starting smartd: hdc: drive_cmd: status=0x58 { DriveReady SeekComplete
DataRequest }
ide: failed opcode was: 0xa1
hdc: status error: status=0x58 { DriveReady SeekComplete DataRequest }
ide: failed opcode was: unknown
hdc: drive not ready for command
hdc: status timeout: status=0xd8 { Busy }
ide: failed opcode was: unknown
hdc: drive not ready for command
hdc: ATAPI reset complete
hdc: status error: status=0x58 { DriveReady SeekComplete DataRequest }
⋮
```

  To work around this issue, disconnect the DVD drive or turn the **smartd** service off with the following command:

```
~]# chkconfig smartd off
```

- The **modify SRQ** verb is not supported by the **eHCA** adapter and will fail with an error code when called from an application context.

- In RHEL 5.8, machine check (MCE) support for Intel Nehalem or newer CPUs (family 6, model >= 26) is disabled. This is a change from RHEL5.6 and earlier where basic MCE support was provided for these CPUs. Uncorrected CPU and memory errors will cause an immediate CPU shut down and system panic.

- On a Red Hat Enterprise Linux 5.8 system and later, while hand-loading the i386 (32-bit) kernel on z210/z210 SFF with BIOS 1.08, the system may fail to boot. To workaround this issue, please add the following parameter to the boot command line option:

```
pci=nosort
```

  (BZ#703538)

- Red Hat Enterprise Linux 5.7 has introduced a new multicast snooping feature for the bridge driver used for virtualization (virt-bridge). This feature is disabled by default in order to not break any existing configurations. To enable this feature, please set the following tunnable parameter to **1**:

```
/sys/class/net/breth0/bridge/multicast_snooping
```

  Please note that when multicast snooping is enabled, it may cause a regression with certain switches where it causes a break in the multicast forwarding for some peers.

- By default, **libsas** defines a wideport based on the attached SAS address, rather than the specification compliant “strict” definition of also considering the local SAS address. In Red Hat Enterprise Linux 5.8 and later, only the default “loose” definition is available. The implication is that if an OEM configures an SCU controller to advertise different SAS addresses per PHY, but hooks up a wide target or an expander to those PHYs, libsas will only create one port. The expectation, in the “strict” case, is that this would result in a single controller multipath configuration.

  It is not possible to use a single controller multipath without the **strict_wide_port** functionality. Multi-controller multipath should behave as a expected.

  A x8 multipath configuration through a single expander can still be obtained under the following

conditions:

- Start with an SCU SKU that exposes (2) x4 controllers (total of 8 PHYs)
- Assign ***sas_address1*** to all the PHYs on **controller1**
- Assign ***sas_address2*** to all the PHYs on **controller2**
- Hook up the expander across all 8 PHYs
- Configure multipath across the two controller instances

It is critical for **controller1** to have a distinct address from **controller2**, otherwise the expander will be unable to correctly route connection requests to the proper initiator. (BZ#651837)

- On a Red Hat Enterprise Linux 5 system, it is advisable to update the firmware of the HP ProLiant Generation 6 (G6) controller's firmware to version 5.02 or later. Once the firmware is successfully updated reboot the system and Kdump will work as expected.

  HP G6 controllers include: P410i, P411, P212, P712, and P812

  In addition, kdump may fail when using the HP Smart Array 5i Controller on a Red Hat Enterprise Linux 5 system. (BZ#695493)

- On Red Hat Enterprise Linux 5.5 and later, suspending the system with the **lpfc** driver loaded may crash the system during the resume operation. Therefore, systems using the **lpfc** driver, either unload the **lpfc** driver before the system is suspended, or ,if that is not possible, do not suspend the system. (BZ#703631)

- NUMA class systems should not be booted with a single memory node configuration. Configuration of single node NUMA systems will result in contention for the memory resources on all of the non-local memory nodes. As only one node will have local memory the CPUs on that single node will starve the remaining CPUs for memory allocations, locks, and any kernel data structure access. This contention will lead to the "CPU#n stuck for 10s!" error messages. This configuration can also result in NMI watchdog timeout panics if a spinlock is acquired via **spinlock_irq()** and held for more than 60 seconds. The system can also hang for indeterminate lengths of time.

  To minimize this problem, NUMA class systems need to have their memory evenly distributed between nodes. NUMA information can be obtained from dmesg output as well as from the **numastat** command. (BZ#529428)

- When upgrading from Red Hat Enterprise Linux 5.0, 5.1 or 5.2 to more recent releases, the gfs2-kmod may still be installed on the system. This package must be manually removed or it will override the (newer) version of GFS2 which is built into the kernel. Do not install the **gfs2-kmod** package on later versions of Red Hat Enterprise Linux. **gfs2-kmod** is not required since GFS2 is built into the kernel from 5.3 onwards. The content of the gfs2-kmod package is considered a Technology Preview of GFS2, and has not received any updates since Red Hat Enterprise Linux 5.3 was released.

  Note that this note only applies to GFS2 and not to GFS, for which the gfs-kmod package continues to be the only method of obtaining the required kernel module.

- Issues might be encountered on a system with 8Gb/s LPe1200x HBAs and firmware version 2.00a3 when the Red Hat Enterprise Linux 5.8 kernel is used with the in-box LPFC driver. Such issues include loss of LUNs and/or fiber channel host hangs during fabric faults with multipathing.

  To work around these issues, it is recommended to either:

  - Downgrade the firmware revision of the 8Gb/s LPe1200x HBA to revision 1.11a5, or

- Modify the LPFC driver's **lpfc_enable_npiv** module parameter to zero.

  When loading the LPFC driver from the initrd image (i.e. at system boot time), add the line

  ```
  options lpfc_enable_npiv=0
  ```

  to **/etc/modprobe.conf** and re-build the initrd image.

  When loading the LPFC driver dynamically, include the **lpfc_enable_npiv=0** option in the insmod or modprobe command line.

For additional information on how to set the LPFC driver module parameters, refer to the Emulex Drivers for Linux User Manual.

- If AMD IOMMU is enabled in BIOS on ProLiant DL165 G7 systems, the system will reboot automatically when IOMMU attempts to initialize. To work around this issue, either disable IOMMU, or update the BIOS to version **2010.09.06** or later. (BZ#628534)

- As of Red Hat Enterprise Linux 5.6, the **ext4** file system is fully supported. However, provisioning ext4 file systems with the anaconda installer is not supported, and ext4 file systems need to be provisioned manually after the installation. (BZ#563943)

- In some cases the NFS server fails to notify NFSv4 clients about renames and unlinks done by other clients, or by non-NFS users of the server. An application on a client may then be able to open the file at its old pathname (and read old cached data from it, and perform read locks on it), long after the file no longer exists at that pathname on the server.

  To work around this issue, use NFSv3 instead of NFSv4. Alternatively, turn off support for leases by writing ***0*** to **/proc/sys/fs/leases-enable** (ideally on boot, before the nfs server is started). This change prevents NFSv4 delegations from being given out, restore correctness at the expense of some performance.

- Some laptops may generate continuous events in response to the lid being shut. Consequently, the gnome-power-manager utility will consume CPU resources as it responds to each event. (BZ#660644)

- A kernel panic may be triggered by the lpfc driver when multiple Emulex OneConnect Universal Converged Network Adapter initiators are included in the same Storage Area Network (SAN) zone. Typically, this kernel panic will present after a cable is pulled or one of the systems is rebooted. To work around this issue, configure the SAN to use single initiator zoning. (BZ#574858)

- If a Huawei USB modem is unplugged from a system, the device may not be detected when it is attached again. To work around this issue, the usbserial and usb-storage driver modules need to be reloaded, allowing the system to detect the device. Alternatively, the if the system is rebooted, the modem will be detected also. (BZ#517454)

- Memory on-line is not currently supported with the Boxboro-EX platform. (BZ#515299)

- Unloading a PF (SR-IOV Physical function) driver from a host when a guest is using a VF (virtual function) from that device can cause a host crash. A PF driver for an SR-IOV device should not be unloaded until after all guest virtual machines with assigned VFs from that SR-IOV device have terminated. (BZ#514360)

- Data corruption on NFS file systems might be encountered on network adapters without support for error-correcting code (ECC) memory that also have TCP segmentation offloading (TSO) enabled in the driver. Note: data that might be corrupted by the sender still passes the checksum performed by the IP stack of the receiving machine A possible work around to this issue is to disable TSO on network adapters that do not support ECC memory. (BZ#504811)

- After installation, a System z machine with a large number of memory and CPUs (e.g. 16 CPU's and 200GB of memory) might may fail to IPL. To work around this issue, change the line

  ```
  ramdisk=/boot/initrd-2.6.18-<kernel-version-number>.el5.img
  ```

  to

  ```
  ramdisk=/boot/initrd-2.6.18-<kernel-version-number>.el5.img,0x02000000
  ```

  The command **zipl -V** should now show **0x02000000** as the starting address for the initial RAM disk (initrd). Stop the logical partition (LPAR), and then manually increase the storage size of the LPAR.

- On certain hardware configurations the kernel may panic when the Broadcom iSCSI offload driver (**bnx2i.ko** and **cnic.ko**) is loaded. To work around this do not manually load the bnx2i or cnic modules, and temporarily disable the **iscsi** service from starting. To disable the iscsi service, run:

  ```
  ~]# chkconfig --del iscsi
  ~]# chkconfig --del iscsid
  ```

  On the first boot of your system, the **iscsi** service may start automatically. To bypass this, during bootup, enter interactive start up and stop the iscsi service from starting.

- In Red Hat Enterprise Linux 5, invoking the kernel system call "setpriority()" with a "which" parameter of type "PRIO_PROCESS" does not set the priority of child threads. (BZ#472251)

- A change to the cciss driver in Red Hat Enterprise Linux 5.4 made it incompatible with the **echo disk < /sys/power/state** suspend-to-disk operation. Consequently, the system will not suspend properly, returning messages such as:

  ```
  Stopping tasks:
  ======================================================================
  stopping tasks timed out after 20 seconds (1 tasks remaining):
  cciss_scan00
  Restarting tasks...<6> Strange, cciss_scan00 not stopped
  done
  ```

  (BZ#513472)

- The kernel is unable to properly detect whether there is media present in a CD-ROM drive during kickstart installs. The function to check the presence of media incorrectly interprets the "logical unit is becoming ready" sense, returning that the drive is ready when it is not. To work around this issue, wait several seconds between inserting a CD and asking the installer (anaconda) to refresh the CD. (BZ#510632)

- When a cciss device is under high I/O load, the kdump kernel may panic and the vmcore dump may not be saved successfully. (BZ#509790)

- Configuring IRQ SMP affinity has no effect on some devices that use message signaled interrupts (MSI) with no MSI per-vector masking capability. Examples of such devices include *Broadcom NetXtreme* Ethernet devices that use the **bnx2** driver.

  If you need to configure IRQ affinity for such a device, disable MSI by creating a file in **/etc/modprobe.d/** containing the following line:

  ```
  options bnx2 disable_msi=1
  ```

Alternatively, you can disable MSI completely using the kernel boot parameter **pci=nomsi**. (BZ#432451)

- The **smartctl** tool cannot properly read SMART parameters from SATA devices. (BZ#429606)
- *IBM T60* laptops will power off completely when suspended and plugged into a docking station. To avoid this, boot the system with the argument **acpi_sleep=s3_bios**. (BZ#439006)
- The *QLogic iSCSI Expansion Card* for the *IBM Bladecenter* provides both ethernet and iSCSI functions. Some parts on the card are shared by both functions. However, the current **qla3xxx** and **qla4xxx** drivers support ethernet and iSCSI functions individually. Both drivers do not support the use of ethernet and iSCSI functions simultaneously.

  Because of this limitation, successive resets (via consecutive **ifdown**/**ifup** commands) may hang the device. To avoid this, allow a 10-second interval after an **ifup** before issuing an **ifdown**. Also, allow the same 10-second interval after an **ifdown** before issuing an **ifup**. This interval allows ample time to stabilize and re-initialize all functions when an **ifup** is issued. (BZ#276891)
- Laptops equipped with the *Cisco Aironet MPI-350* wireless may hang trying to get a DHCP address during any network-based installation using the wired ethernet port.

  To work around this, use local media for your installation. Alternatively, you can disable the wireless card in the laptop BIOS prior to installation (you can re-enable the wireless card after completing the installation). (BZ#213262)
- Hardware testing for the *Mellanox MT25204* has revealed that an internal error occurs under certain high-load conditions. When the **ib_mthca** driver reports a catastrophic error on this hardware, it is usually related to an insufficient completion queue depth relative to the number of outstanding work requests generated by the user application.

  Although the driver will reset the hardware and recover from such an event, all existing connections at the time of the error will be lost. This generally results in a segmentation fault in the user application. Further, if **opensm** is running at the time the error occurs, then you need to manually restart it in order to resume proper operation. (BZ#251934)
- The *IBM T41* laptop model does not enter **Suspend Mode** properly; as such, **Suspend Mode** will still consume battery life as normal. This is because Red Hat Enterprise Linux 5 does not yet include the **radeonfb** module.

  To work around this, add a script named **hal-system-power-suspend** to **/usr/share/hal/scripts/** containing the following lines:

  ```
  chvt 1
  radeontool light off
  radeontool dac off
  ```

  This script will ensure that the *IBM T41* laptop enters **Suspend Mode** properly. To ensure that the system resumes normal operations properly, add the script **restore-after-standby** to the same directory as well, containing the following lines:

  ```
  radeontool dac on
  radeontool light on
  chvt 7
  ```

  (BZ#227496)
- If the **edac** module is loaded, BIOS memory reporting will not work. This is because the **edac** module clears the register that the BIOS uses for reporting memory errors.

The current Red Hat Enterprise Linux Driver Update Model instructs the kernel to load all available modules (including the **edac** module) by default. If you wish to ensure BIOS memory reporting on your system, you need to manually blacklist the **edac** modules. To do so, add the following lines to **/etc/modprobe.conf**:

```
blacklist edac_mc
blacklist i5000_edac
blacklist i3000_edac
blacklist e752x_edac
```

(BZ#441329)

- Due to outstanding driver issues with hardware encryption acceleration, users of Intel WiFi Link 4965, 5100, 5150, 5300, and 5350 wireless cards are advised to disable hardware accelerated encryption using module parameters. Failure to do so may result in the inability to connect to Wired Equivalent Privacy (WEP) protected wireless networks after connecting to WiFi Protected Access (WPA) protected wireless networks.

  To do so, add the following options to **/etc/modprobe.conf**:

  ```
  alias wlan0 iwlagn
  options iwlagn swcrypto50=1 swcrypto=1
  ```

  where wlan0 is the default interface name of the first Intel WiFi Link device.

  (BZ#468967)

- A kernel security fix released between Red Hat Enterprise Linux 5.7 and 5.8 may prevent PCI passthrough working and guests starting. Refer to Red Hat Knowledgebase article 66747 for further details.

The following note applies to the PowerPC architecture:

- The size of the PowerPC kernel image is too large for OpenFirmware to support. Consequently, network booting will fail, resulting in the following error message:

  ```
  Please wait, loading kernel...
  /pci@8000000f8000000/ide@4,1/disk@0:2,vmlinux-anaconda: No such file or
  directory
  boot:
  ```

  To work around this:

  - Boot to the OpenFirmware prompt, by pressing the '8' key when the IBM splash screen is displayed.
  - Run the following command:

    ```
    ~]# setenv real-base 2000000
    ```

  - Boot into System Management Services (SMS) with the command:

    ```
    ~]# 0> dev /packages/gui obe
    ```

  (BZ#462663)

2.21. kexec-tools

The *kexec-tools* package provides the **/sbin/kexec** binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot.

- Executing **kdump** on an *IBM Bladecenter QS21* or *QS22* configured with NFS root will fail. To avoid this, specify an NFS dump target in **/etc/kdump.conf**. (BZ#368981)

- Some **forcedeth** based devices may encounter difficulty accessing memory above 4GB during operation in a **kdump** kernel. To work around this issue, add the following line to the **/etc/sysconfig/kdump** file:

  ```
  KDUMP_COMMANDLINE_APPEND="dma_64bit=0"
  ```

  This work around prevents the **forcedeth** network driver from using high memory resources in the kdump kernel, allowing the network to function properly.

- The system may not successfully reboot into a **kexec**/**kdump** kernel if X is running and using a driver other than *vesa*. This problem only exists with *ATI Rage XL* graphics chipsets.

  If X is running on a system equipped with *ATI Rage XL*, ensure that it is using the *vesa* driver in order to successfully reboot into a **kexec**/**kdump** kernel. (BZ#221656)

- **kdump** now serializes drive creation registration with the rest of the **kdump** process. Consequently, **kdump** may hang waiting for IDE drives to be initialized. In these cases, it is recommended that IDE disks not be used with **kdump**. (BZ#473852)

- It is possible in rare circumstances, for **makedumpfile** to produce erroneous results but not have them reported. This is due to the fact that **makedumpfile** processes its output data through a pipeline consisting of several stages. If **makedumpfile** fails, the other stages will still succeed, effectively masking the failure. Should a vmcore appear corrupt, and makedumpfile is in use, it is recommended that the core be recorded without makedumpfile and a bug be reported. (BZ#475487)

- kdump now restarts when CPUs or DIMMs are hot-added to a system. If multiple items are added at the same time, several sequential restarts may be encountered. This behavior is intentional, as it minimizes the time-frame where a crash may occur while memory or processors are not being tracked by kdump. (BZ#474409)

The following known issue applies to the Itanium architecture:

- Some *Itanium* systems cannot properly produce console output from the **kexec purgatory** code. This code contains instructions for backing up the first 640k of memory after a crash.

  While **purgatory** console output can be useful in diagnosing problems, it is not needed for **kdump** to properly function. As such, if your *Itanium* system resets during a **kdump** operation, disable console output in **purgatory** by adding **--noio** to the **KEXEC_ARGS** variable in **/etc/sysconfig/kdump**. (BZ#436426)

2.22. krb5

Kerberos 5 is a network authentication system which authenticates clients and servers to each other using symmetric key encryption and a trusted third party, the KDC.

- In case the SSSD client authenticates against a Kerberos server (KDC) using a keytab, and the first encryption type the KDC offers is not present in the keytab, the authentication fails. Note that this problem was fixed in a later release of MIT Kerberos.

2.23. kvm

Kernel-based Virtual Machine (KVM) is a full virtualization solution for Linux on x86 hardware.

KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel. KVM can run multiple unmodified, virtualized guest Windows and Linux operating systems. KVM is a hypervisor which uses the libvirt virtualization tools (virt-manager and virsh).

- A Microsoft Windows 2008 guest can become unresponsive during boot if huge page memory is enabled on the Red Hat Enterprise Linux 5.9 host. To work around this problem, disable huge page memory on the Red Hat Enterprise Linux 5.9 host. (BZ#845489)
- A CD-ROM device can be assigned to a guest by configuring the guest to back a virtual CD-ROM device with a physical device's special file, for example, /dev/sr0. When a physical CD-ROM device is assigned to a guest, the guest assumes it has full control of the device. However, it is still possible to access the device from the host. In such a case, the guest can become confused about the CD-ROM state; for instance, running eject commands in the host to change media can cause the guest to attempt to read beyond the size of the new medium, resulting in I/O errors. To work around this problem, do not access a CD-ROM device from the host while it is assigned to a guest. (BZ#847259)
- VNC password authentication is disabled when the host system is operating in FIPS mode. QEMU exits if it is configured to run as a password-authenticated VNC server; if QEMU is configured to run as an unauthenticated VNC server, it will continue to run as expected.
- Erroneous boot-index of a guest with mixed virtio/IDE disks causes the guest to boot from the wrong disk after the OS installation and hang with the error message **`boot from HD`**.
- When using PCI device assignment with a 32-bit Microsoft Windows 2008 guest on an AMD-based host system, the assigned device may fail to work properly if it relies on MSI or MSI-X based interrupts. The reason for this is that the 32-bit version of Microsoft Windows 2008 does not enable MSI based interrupts for the family of processor exposed to the guest. To work around this problem, the user may wish to move to a RHEL6 host, use a 64-bit version of the guest operating system, or employ a wrapper script to modify the processor family exposed to the guest as follows (Note that this is only for 32-bit Windows guests):
  - Create the following wrapper script:

```
~]$ cat /usr/libexec/qemu-kvm.family16
#!/bin/sh

ARGS=$@

echo $ARGS | grep -q ' -cpu '
if [ $? -eq 0 ]; then
    for model in $(/usr/libexec/qemu-kvm -cpu ? \
                    | sed 's|^x86||g' | tr -d [:blank:]); do
        ARGS=$(echo $ARGS | \
               sed "s|-cpu $model|-cpu $model,family=16|g")
    done
else
    ARGS="$ARGS -cpu qemu64,family=16"
fi

echo "$0: exec /usr/libexec/qemu-kvm $ARGS" >&2

exec /usr/libexec/qemu-kvm $ARGS
```

- Make the script executable:

```
~]$ chmod 755 /usr/libexec/qemu-kvm.family16
```

- Set proper SELinux permissions:

```
~]$ restorecon /usr/libexec/qemu-kvm.family16
```

- Update the guest XML to use the new wrapper:

```
~]# virsh edit $GUEST
```

and replace:

```
<emulator>/usr/libexec/qemu-kvm</emulator>
```

with:

```
<emulator>/usr/libexec/qemu-kvm.family16</emulator>
```

(BZ#654208)

- Booting a Linux guest causes 1.5 to 2 second time drift from the host time when the default **hwclock** service starts. It is recommended to disable the hwclock service. Alternatively, enable the **ntp** service so that it can correct the time once the service is started. (BZ#523478)

- By default, KVM virtual machines created in Red Hat Enterprise Linux 5.6 have a virtual Realtek 8139 (rtl8139) network interface controller (NIC). The rtl8139 virtual NIC works fine in most environments, but may suffer from performance degradation issues on some networks for example, a 10 GigE (10 Gigabit Ethernet) network.

  One workaround for this issue is switch to a different type of virtual NIC, for example, Intel PRO/1000 (e1000) or virtio (a virtual I/O driver for Linux that can talk to the hypervisor).

  To switch to e1000:

  - Shutdown the guest OS
  - Edit the guest OS definition with the command-line tool virsh:

```
virsh edit GUEST
```

  - Locate the network interface section and add a model line as shown:

```
<interface type='network'>
...
<model type='e1000' />
</interface>
```

  - Save the changes and exit the text editor
  - Restart the guest OS

Alternatively, if you're having trouble installing the OS on the virtual machine because of the rtl8139 NIC (for example, because you're installing the OS over the network), you can create a virtual machine from scratch with an e1000 NIC. This method requires you to have at least one virtual machine already created (possibly installed from CD or DVD) to use as a template.

- Create an XML template from an existing virtual machine:

```
virsh dumpxml GUEST > /tmp/guest.xml
```

- Copy and edit the XML file and update the unique fields: virtual machine name, UUID, disk image, MAC address, etc. Note that you can delete the UUID and MAC address lines and virsh will generate a UUID and MAC address.

```
cp /tmp/guest.xml /tmp/new-guest.xml
vi /tmp/new-guest.xml
```

- Locate the network interface section and add a model line as shown:

```
<interface type='network'>
...
<model type='e1000' />
</interface>
```

- Create the new virtual machine:

```
virsh define /tmp/new-guest.xml
virsh start new-guest
```

- The mute button in the audio control panel on a Windows virtual machine does not mute the sound.
- When migrating KVM guests between hosts, the NX CPU feature setting on both source and destination must match. Migrating a guest between a host with the NX feature disabled (i.e. disabled in the BIOS settings) and a host with the NX feature enabled may cause the guest to crash. (BZ#516029)
- The use of the qcow2 disk image format with KVM is considered a Technology Preview. (BZ#517880)
- 64-bit versions of Windows 7 do not have support for the AC'97 Audio Codec. Consequently, the virtualized sound device Windows 7 kvm guests will not function. (BZ#563122)
- Hot plugging emulated devices after migration may result in the virtual machine crashing after a reboot or the devices no longer being visible. (BZ#507191)
- The KVM modules from the **kmod-kvm** package do not support kernels prior to version 2.6.18-203.el5. If kmod-kvm is updated and an older kernel is kept installed, error messages similar to the following will be returned if attempting to install these modules on older kernels:

```
WARNING: /lib/modules/2.6.18-194.el5/weak-updates/kmod-kvm/ksm.ko needs
unknown symbol kvm_ksm_spte_count
```

(BZ#509361)

- The KVM modules available in the **kmod-kvm** package are loaded automatically at boot time if the kmod-kvm package is installed. To make these KVM modules available after installing the **kmod-kvm** package the system either needs to be rebooted or the modules can be loaded manually by running the **/etc/sysconfig/modules/kvm.modules** script. (BZ#501543)

- The Preboot eXecution Environment (PXE) boot ROMs included with KVM are from the Etherboot project. Consequently, some bug fixes or features that are present on the newer gPXE project are not available on Etherboot. For example, Virtual Machines (VMs) cannot boot using Microsoft based PXE (that is, Remote Installation Services (RIS) or Windows Deployment Services (WDS)).
- The following QEMU / KVM features are currently disabled and not supported: (BZ#512837)
  - smb user directories
  - scsi emulation
  - "isapc" machine type
  - nested KVM guests
  - usb mass storage device emulation
  - usb wacom tablet emulation
  - usb serial emulation
  - usb network emulation
  - usb bluetooth emulation
  - device emulation for vmware drivers
  - sb16 and es1370 sound card emulations
  - bluetooth emulation
  - qemu CPU models other than qemu32/64 and pentium3
  - qemu block device drivers other than raw, qcow2, and host_device

2.24. lftp

LFTP is a sophisticated file transfer program for the FTP and HTTP protocols. Like bash, it has job control and uses the readline library for input. It has bookmarks, built-in mirroring, and can transfer several files in parallel. It is designed with reliability in mind.

- As a side effect of changing the underlying cryptographic library from OpenSSL to GnuTLS in the past, starting with *lftp-3.7.11-4.el5_5.3*, some previously offered TLS ciphers were dropped. In handshake, **lftp** does not offer these previously available ciphers:

```
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
```

  lftp still offers variety of other TLS ciphers:

```
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_RC4_128_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
```

For servers without support for any of these ciphers, it is now possible to force SSLv3 connection instead of TLS using the **`set ftp:ssl-auth SSL`** configuration directive. This works both for implicit and explicit FTPS. (BZ#532099)

2.25. lvm2

The lvm2 package contains support for Logical Volume Management (LVM).

- LVM no longer scans multipath member devices (underlying paths for active multipath devices) and prefers top level devices. This behavior can be switched off using the **`multipath_component_detection`** option in the **`/etc/lvm/lvm.conf`**.

2.26. mesa

Mesa provides a 3D graphics API that is compatible with OpenGL. It also provides hardware-accelerated drivers for many popular graphics chips.

The following known issue applies to the Intel 64 and AMD64 architectures:

- On an *IBM T61* laptop, Red Hat recommends that you refrain from clicking the **`glxgears`** window (when **`glxgears`** is run). Doing so can lock the system.

  To prevent this from occurring, disable the tiling feature. To do so, add the following line in the **`Device`** section of **`/etc/X11/xorg.conf`**:

  ```
  Option "Tiling" "0"
  ```

  (BZ#444508)

2.27. mkinitrd

The mkinitrd utility creates file system images for use as initial RAM disk (initrd) images.

- When running Red Hat Enterprise Linux 5 with an older kernel in a Microsoft Hyper-V virtualization guest, mkinitrd does not include the Microsoft Hyper-V drivers when asked to generate the initial RAM disk for a Red Hat Enterprise Linux 5.9 kernel or later. This causes a kernel panic when the guest is rebooted with such a kernel as there is no driver available for the storage hosting the guest's root file system. To work around this problem, run the mkinitrd utility with either the **`--preload`** option that loads the module before any SCSI modules are loaded, or with the **`--with`** option that loads the module after SCSI modules are loaded. For more information, refer to the following Knowledge Base article:

  https://access.redhat.com/site/solutions/27421

- When using an encrypted device, the following error message may be reported during bootup:

```
insmod: error inserting '/lib/aes_generic.ko': -1 File exists
```

  This message can safely be ignored. (BZ#466296)

- Installation using a Multiple Device (MD) RAID on top of multipath will result in a machine that cannot boot. Multipath to Storage Area Network (SAN) devices which provide RAID internally are not affected. (BZ#467469)

The following known issue applies to the IBM System z architecture:

- When installing Red Hat Enterprise Linux 5, the following errors may be returned in **`install.log`**:

```
Installing kernel-2.6.18-158.el5.s390x
cp: cannot stat `/sbin/dmraid.static': No such file or directory
```

  This message can be safely ignored.

- iSCSI root devices do not function correctly if used over an IPv6 network connection. While the installation will appear to succeed, the system will fail to find the root file system during the first boot. (BZ#529636)

2.28. mod_revocator

The mod_revocator module retrieves and installs remote Certificate Revocation Lists (CRLs) into an Apache web server.

- In order to run **mod_revocator** successfully, the following command must be executed in order to allow **`httpd`** to connect to a remote port which SELinux would otherwise deny:

```
~]# setsebool -P httpd_can_network_connect=1
```

  This is due to the fact that by default, Apache is not allowed to also be used as an HTTP client (that is, send HTTP messages to an external host).

2.29. nfs-utils

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 also contain the mount.nfs, umount.nfs, and showmount programs.

- In the previous version of the nfs-utils package, the mount utility incorrectly reported the rpc.idmapd mapping daemon as not running when the daemon was executed. This bug has been fixed; however the problem can occur after upgrading nfs-utils to a later version. Note that the mount operation is successful and the warning can be safely ignored. To avoid this problem, perform a clean installation of the package.

- Currently, the rpc.gssd daemon looks only for the "nfs/*" keys in the keytab file. Other keys are not supported.

2.30. openib

The OpenFabrics Alliance Enterprise Distribution (OFED) is a collection of Infiniband and iWARP hardware

diagnostic utilities, the Infiniband fabric management daemon, Infiniband/iWARP kernel module loader, and libraries and development packages for writing applications that use Remote Direct Memory Access (RDMA) technology. Red Hat Enterprise Linux uses the OFED software stack as its complete stack for Infiniband/iWARP/RDMA hardware support.

The following known issue applies to the Itanium architecture:

- Running **perftest** will fail if different CPU speeds are detected. As such, you should disable CPU speed scaling before running **perftest**. (BZ#433659)

2.31. openmpi

Open MPI, MVAPICH, and MVAPICH2 are all competing implementations of the Message Passing Interface (MPI) standard. MVAPICH implements version 1 of the MPI standard, while Open MPI and MVAPICH2 both implement the later, version 2 of the MPI standard.

- **mvapich** and **mvapich2** in Red Hat Enterprise Linux 5 are compiled to support only *InfiniBand/iWARP* interconnects. Consequently, they will not run over ethernet or other network interconnects. (BZ#466390)
- When upgrading openmpi using yum, the following warning may be returned:

  ```
  cannot open `/tmp/openmpi-upgrade-version.*' for reading: No such file or
  directory
  ```

  The message is harmless and can be safely ignored. (BZ#463919)
- A bug in previous versions of **openmpi** and **lam** may prevent you from upgrading these packages. This bug manifests in the following error (when attempting to upgrade **openmpi** or **lam**:

  ```
  error: %preun(openmpi-[version]) scriptlet failed, exit status 2
  ```

  As such, you need to manually remove older versions of **openmpi** and **lam** in order to install their latest versions. To do so, use the following **rpm** command:

  ```
  rpm -qa | grep '^openmpi-\|^lam-' | xargs rpm -e --noscripts --allmatches
  ```

  (BZ#433841)

2.32. openswan

Openswan is a free implementation of IPsec (Internet Protocol Security) and IKE (Internet Key Exchange) for Linux. The openswan package contains the daemons and user space tools for setting up Openswan. It supports the NETKEY/XFRM IPsec kernel stack that exists in the default Linux kernel. Openswan 2.6 and later also supports IKEv2 (Internet Key Exchange Protocol Version 2), which is defined in RFC5996

- Openswan generates a Diffie-Hellman (DH) shared key that is 1 byte short because nss does not add leading zero bytes when needed. Also, openswan does not support setting of the sha2_truncbug parameter starting with Red Hat Enterprise Linux 5.9, because the kernel does not support it.

2.33. perl-libxml-enno

The perl-libxml-enno modules were used for XML parsing and validation.

- Note: the perl-libxml-enno library did not ship in any Red Hat Enterprise Linux 5 release. (BZ#612589)

2.34. pm-utils

The *pm-utils* package contains utilities and scripts for power management.

- nVidia video devices on laptops can not be correctly re-initialized using VESA in Red Hat Enterprise Linux 5. Attempting to do so results in a black laptop screen after resume from suspend.

2.35. rpm

The RPM Package Manager (RPM) is a command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

- Users of a freshly-installed PowerPC Red Hat Enterprise Linux 5 system may encounter package-related operation failures with the following errors:

```
rpmdb: PANIC: fatal region error detected; run recovery
error: db4 error(-30977) from db->sync: DB_RUNRECOVERY: Fatal error, run
database recovery
```

2.36. redhat-release-notes

The *redhat-release-notes* package contains the Release Notes for Red Hat Enterprise Linux 5.10.

- The Release Notes shipped in Red Hat Enterprise Linux 5.10 through the *redhat-release-notes* package contain an year and minor Red Hat Enterprise Linux version in the **README** files. Additionally, two paragraphs in the **gu-IN** version of Release Notes are untranslated and display in the English language.
- The **/usr/share/doc/redhat-release-notes-5Server/README-*architecture*-en** file, provided by the *redhat-release-notes* package, contains no content. As a workaround, please refer to the **README-*architecture*-en.html** file in the same directory.

2.37. rhn-client-tools

Red Hat Network Client Tools provide programs and libraries that allow your system to receive software updates from Red Hat Network (RHN).

- Attempting to subscribe a system during firstboot can fail with a traceback. To work around this problem, register the system from the command line.

2.38. qspice

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display system built for virtual environments 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.

- Occasionally, the video compression algorithm starts when the guest is accessing text instead of video. This caused the text to be blurred. The SPICE server now has an improved heuristic for distinguishing between videos and textual streams.

2.39. samba3x

Samba is a suite of programs used by machines to share files, printers, and other utilities.

- In a large Active Directory environment with multiple trusted domains, attempting to list the users on all domains by running the **`wbinfo -u`** command can fail with the following message:

  ```
  Error looking up domain users
  ```

  To work around this problem, use the **`wbinfo --domain='*' -u`** command to list the users on all domains.

- The updated samba3x packages change the way ID mapping is configured. Users are advised to modify their existing Samba configuration files. Also, due to the ID mapping changes, authconfig does not create a working smb.conf file for the latest samba3x package, it only produces a valid configuration for the samba package.

  Note that several tdb files have been updated and the printing support has been rewritten to use the actua registry implementation. This means that all tdb files are upgraded as soon as you start the new version of smbd. You cannot downgrade to an older samba3x version unless you have backups of the tdb files.

  For more information about these changes, refer to the Release Notes for Samba 3.6.0.

- In Samba 3.0, the privilege **`SeSecurityPrivilege`** was granted to a user by default. To make Samba more secure, this privilege is no longer granted to a user by default. If you use an application that requires this privilege, like the IBM Tivoli Storage Manager, you need to grant it to the user running the Storage Manager with the following command:

  `net sam rights grant <username> SeSecurityPrivilege`

  See **`net sam rights list`** for a list of available privileges.

2.40. shadow-utils

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 also contain the mount.nfs, umount.nfs, and showmount programs.

- Previously, under certain circumstances, the **faillog** utility created huge files. This problem has been fixed; however, the **useradd** utility can still create large files. To avoid such a situation, use the **`-l`** option when creating a user with a very high user or group ID (UID or GID). (BZ#670364)

2.41. sos

The sos packages contain a set of tools that gather information from system hardware, logs and configuration files. The information can then be used for diagnostic purposes and debugging.

- If the **sosresport** utility becomes unresponsive, a keyboard interrupt (CTRL+C) can fail to terminate it. In such a case, to terminate the process:
  - press *Ctrl+Z* and execute **`kill %N`** (N represents the number of the sosreport job; usually 1) or
  - execute **`kill -9 %N`** (N represents the number of the sosreport job; usually 1). (BZ#708346)

2.42. subscription-manager

The new Subscription Management tooling allows users to understand the specific products which have been installed on their machines, and the specific subscriptions which their machines are consuming.

- Usually in non-English locales, processing the output of the **`subscription-manager list --installed`** command through the **grep** subshell can fail with the following message:

  ```
  ascii' codec can't encode character u'___' in position ___: ordinal not in
  range(128)
  ```

  (BZ#977535)

- For virtual guests, the Subscription Manager daemons use **dmidecode** to read the System Management BIOS (SMBIOS), which is used to retrieve the guest UUID. On 64-bit Intel architecture, the SMBIOS information is controlled by the Intel firmware and stored in a read-only binary entry. Therefore, it is not possible to retrieve the UUID or set a new and readable UUID. Because the guest UUID is unreadable, running the **`facts`** command on the guest system shows a value of **`Unknown`** in the **`virt.facts`** file for the system (**`virt.uuid: Unknown`**). This means that the guest does not have any association with the host machine and, therefore, does not inherit some subscriptions. The facts used by Subscription Manager can be edited manually to add the UUID:

  - Obtain the guest name or guest ID.
  - On the virtual host, use virsh to retrieve the guest UUID. For example, for a guest named 'rhel5server_virt1':

    ```
    virsh domuuid rhel5server_virt1
    ```

  - On the guest, manually create a facts file:

    ```
    vim /etc/rhsm/facts/virt.facts
    ```

  - Add a line which contains the given UUID.

    ```
    {
      "virt.uuid": "$VIRSH_UUID"
    }
    ```

  Creating the **`facts`** file and inserting the proper UUID means that Subscription Manager properly identifies the guest rather than using an **`Unknown`** value.

- Japanese SCIM input-method editor cannot be activated and cannot input locale string in the data field for non-root users. To work around this problem, follow these steps:

  - Log in to the system as a non-root user.
  - As root, run the following commands:

    ```
    ~]# export GTK_IM_MODULE=scim-bridge
    ~]# subscription-manager-gui
    ```

- Using Subscription Manager in the following use case fails: a user installs Red Hat Enterprise Linux Desktop from a Red Hat Enterprise Linux 5.7 Client CD/DVD without an installation number. A user uses Subscription Manager, which finds one Red Hat Enterprise Linux Desktop product ID to subscribe to a Red Hat Enterprise Linux Workstation subscription. A user downloads content from a Workstation repository.

The use case scenario described above fails because the rhel-workstation repositories require the rhel-5-workstation product tag in the product certification beforehand in order to view them.

To work around this issue, follow these steps:

- Install a rhel-5-client system.
- Mount the ISO to your file system.
- Copy **<*path_to_ISO*>/Workstation/repodata/productid** to the **/etc/pki/product/** directory, making sure that the file copied ends with **.pem** (for example, **/etc/pki/product/productid.pem**)
- Subscribe to a Workstation subscription.
- Install a package from a Workstation repository.

2.43. systemtap

SystemTap provides an instrumentation infrastructure for systems running the Linux 2.6 kernel. It allows users to write scripts that probe and trace system events for monitoring and profiling purposes. SystemTap's framework allows users to investigate and monitor a wide variety of wide variety of kernel functions, system calls, and other evens that occur in both kernel-space and user-space.

- The *systemap-testsuite* subpackage is designed for installation on development Workstation machines, not limited Client variants. More complete RPM dependencies now mandate the presence of several non-Client RPM packages, so it is no longer installable on the Client variant. Attempting to update can fail if the update includes the *system-testsuite* subpackage. To work around this problem remove the *systemtap-testsuite* subpackage from a Client machine before upgrading the systemtap package.
- Running some user-space probe test cases provided by the **systemtap-testsuite** package fail with an **Unknown symbol in module** error on some architectures. These test cases include (but are not limited to):
  - **systemtap.base/uprobes.exp**
  - **systemtap.base/bz10078.exp**
  - **systemtap.base/bz6850.exp**
  - **systemtap.base/bz5274.exp**

  Because of a known bug in the latest SystemTap update, new SystemTap installations do not unload old versions of the **uprobes.ko** module. Some updated user-space probe tests provided by the systemtap-testsuite package use symbols available only in the latest **uprobes.ko** module (also provided by the latest SystemTap update). As such, running these user-space probe tests result in the error mentioned earlier.

  If you encounter this error, simply run **rmmod uprobes** to manually remove the older **uprobes.ko** module before running the user-space probe test again. (BZ#499677)
- SystemTap currently uses GCC to probe user-space events. GCC is, however, unable to provide debuggers with precise location list information for parameters. In some cases, GCC also fails to provide visibility on some parameters. As a consequence, SystemTap scripts that probe user-space may return inaccurate readings. (BZ#239065)

2.44. vdsm22

VDSM is a management module that servers as the Red Hat Enterprise Virtualization Manager agent on Red Hat Enterprise Virtualization Hypervisor and Red Hat Enterprise Linux hosts.

- Adding Red Hat Enterprise Virtualization Hypervisor as a Red Hat Enterprise Linux host is not supported in Red Hat Enterprise Linux 5, and will therefore fail.

2.45. virt-v2v

The virt-v2v package provides a tool for converting virtual machines to use the KVM hypervisor or Red Hat Enterprise Virtualization. The tool can import a variety of guest operating systems from libvirt-managed hosts and VMware ESX.

- **VMware Tools** on Microsoft Windows is unable to disable itself when it detects that it is no longer running on a VMware platform. As a consequence, converting a Microsoft Windows guest from VMware ESX, which has **VMware Tools** installed, resulted in multiple error messages being displayed on startup. In addition, a **`Stop Error`** (also known as Blue Screen of Death, or BSOD) was displayed every time when shutting down the guest. To work around this issue, users are advised to uninstall VMware Tools from Microsoft Windows guests before conversion. (BZ#711972)

2.46. virtio-win

VirtIO para-virtualized Windows(R) drivers for 32-bit and 64-bit Windows (R) guests.

- The virtio-win network driver of Red Hat Enterprise Linux 5 can stop working when a Microsoft Windows XP guest is transferred to a Red Hat Enterprise Linux 6 host. To work around this problem, replace the Red Hat Enterprise Linux 5 drivers with the latest Red Hat Enterprise Linux 6 drivers before or after migrating the guest to the new host. (BZ#913094)

- Low performance with UDP messages larger than 1024 is a known Microsoft issue: http://support.microsoft.com/default.aspx/kb/235257. For the message larger than 1024 bytes follow the workaround procedure detailed in the above Microsoft knowledgebase article.

- Installation of Windows XP with the floppy containing guest drivers (in order to get the virtio-net drivers installed as part of the installation), will return messages stating that the viostor.sys file could not be found. viostor.sys is not part of the network drivers, but is on the same floppy as portions of the virtio-blk drivers. These messages can be safely ignored, simply accept the installation's offer to reboot, and the installation will continue normally.

2.47. xen

Xen is a high-performance and secure open-source virtualization framework. The virtualization allows users to run guest operating systems in virtual machines on top of a host operating system.

- 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 some 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 **`clocksource=acpi_pm`** or **`clocksource=jiffies`** to the kernel command line for the guest. Alternatively, if running under Red Hat Enterprise Linux 5.7 or newer, locate the guest configuration file for the guest and add the **`hpet=0`** option in it.

- There are only 2 virtual slots (00:06.0 and 00:07.0) that are available for hot plug support in a virtual guest. (BZ#564261)

- As of Red Hat Enterprise Linux 5.4, PCI devices connected to a single PCI-PCI bridge can no longer be assigned to different PV guests. If the old, unsafe behavior is required, disable pci-dev-assign-strict-check in /etc/xen/xend-config.sxp. (BZ#508310)
- When running x86_64 Xen, it is recommended to set dom0-min-mem in /etc/xen/xend-config.sxp to a value of 1024 or higher. Lower values may cause the dom0 to run out of memory, resulting in poor performance or out-of-memory situations. (BZ#519492)
- The Red Hat Enterprise Linux 3 kernel does not include SWIOTLB support. SWIOTLB support is required for Red Hat Enterprise Linux 3 guests to support more than 4GB of memory on AMD Opteron and Athlon-64 processors. Consequently, Red Hat Enterprise Linux 3 guests are limited to 4GB of memory on AMD processors. (BZ#504187)
- The Hypervisor outputs messages regarding attempts by any guest to write to an MSR. Such messages contain the statement **`Domain attempted WRMSR`**. These messages can be safely ignored; furthermore, they are rate limited and should pose no performance risk. (BZ#477647)

The following known issues applies to the Intel 64 and AMD64 architectures:

- Installing Red Hat Enterprise Linux 3.9 on a fully virtualized guest may be extremely slow. In addition, booting up the guest after installation may result in **`hda: lost interrupt`** errors.

  To avoid this bootup error, configure the guest to use the SMP kernel. (BZ#249521)

2.48. xorg-x11-drv-i810

xorg-x11-drv-i810 is an Intel integrated graphics video driver for the X.Org implementation of the X Window System.

- When switching from the X server to a virtual terminal (VT) on a Lenovo ThinkPad T510 laptop, the screen can remain blank. Switching back to the X server will restore the screen.
- Running a screensaver or resuming a suspended laptop with an external monitor attached may result in a blank screen or a brief flash followed by a blank screen. If this occurs with the screensaver, the prompt for your password is being obscured, the password can still be entered blindly to get back to the desktop. To work around this issue, physically disconnect the external monitor and then press the video hotkey (usually Fn-F7) to rescan the available outputs, before suspending the laptop.

The following known issues apply to the Intel 64 and AMD64 architectures:

- If your system uses an *Intel 945GM* graphics card, do not use the **`i810`** driver. You should use the default **`intel`** driver instead. (BZ#468218)
- On dual-GPU laptops, if one of the graphics chips is Intel-based, the Intel graphics mode cannot drive any external digital connections (including HDMI, DVI, and DisplayPort). This is a hardware limitation of the Intel GPU. If you require external digital connections, configure the system to use the discrete graphics chip (in the BIOS). (BZ#468259)

2.49. xorg-x11-drv-nv

xorg-x11-drv-nv provides a driver for NVIDIA cards for the X.org implementation of the X Window System.

- Improvements have been made to the 'nv' driver, enhancing suspend and resume support on some systems equipped with nVidia GeForce 8000 and 9000 series devices. Due to technical limitations, this will not enable suspend/resume on all hardware. (BZ#414971)

The following known issue applies to the Intel 64 and AMD64 architectures:

- Some machines that use *NVIDIA* graphics cards may display corrupted graphics or fonts when using the graphical installer or during a graphical login. To work around this, switch to a virtual console and back to the original X host. (BZ#222737, BZ#221789)

2.50. xorg-x11-drv-vesa

xorg-x11-drv-vesa is a video driver for the X.Org implementation of the X Window System. It is used as a fallback driver for cards with no native driver, or when the native driver does not work.

The following known issue applies to the x86 architecture:

- When running the bare-metal (non-Virtualized) kernel, the X server may not be able to retrieve **`EDID`** information from the monitor. When this occurs, the graphics driver will be unable to display resolutions highers than 800x600.

  To work around this, add the following line to the **`ServerLayout`** section of **`/etc/X11/xorg.conf`**:

  ```
  Option "Int10Backend" "x86emu"
  ```

  (BZ#236416)

2.51. xorg-x11-server

X.Org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

- On HP Z1 AIO workstations using Intel embedded graphics, the Anaconda installer uses graphical install mode, but displays it only in one quarter of the screen. Although the installation completes successfully, navigation can be difficult in this mode. To work around this problem, use the text-based installation instead of graphical mode, which correctly uses the entire screen on the mentioned workstations.

2.52. yaboot

The *yaboot* package is a boot loader for Open Firmware based PowerPC systems. It can be used to boot IBM eServer System p machines.

- If the string that represents the path to kernel (or ramdisk) is greater than 63 characters, network booting an IBM POWER5 series system may result in the following error:

  ```
  FINAL File Size = 8948021 bytes.
  load-base=0x4000
  real-base=0xc00000
  DEFAULT CATCH!, exception-handler=fff00300
  ```

  The firmware for IBM POWER6 and IBM POWER7 systems contains a fix for this issue. (BZ#550086)

2.53. yum

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.

- In Red Hat Enterprise Linux 5.10, users are allowed to install 32-bit and 64-bit packages in parallel. For

example, when a 32-bit package is installed on the system and the user runs the **`yum install`** ***`package`*** command, the 64-bit version will be installed in parallel with the 32-bit version.

Chapter 3. New Packages

3.1. RHBA-2013:1091 — new packages: sqlite

New sqlite packages are now available for Red Hat Enterprise Linux 5.

SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete database is stored in a single disk file.

* This enhancement update adds a missing package, sqlite.i386, for the Itanium architecture that is required by the nss.i386 package to Red Hat Enterprise Linux 5. (BZ#982260)

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

3.2. RHEA-2013:1130 — new packages: kmod-cciss

New kmod-cciss packages are now available for Red Hat Enterprise Linux 5.

The kmod-cciss packages provide kernel modules for controlling HP Smart Array Controllers.

The kmod-cciss packages provide temporary drivers for the following hardware beyond what was delivered in Red Hat Enterprise Linux 5.9:

- ML350p Gen8 Plus, DL360p Gen8 Plus
- DL380p Gen8 Plus, BL460 Gen8 Plus
- SL230 Gen8 Plus, SL250 Gen8 Plus
- SL270 Gen8 Plus, DL160 Gen8 Plus
- 1928103C | HP Smart Array P230i SAS Controller 1i x4 mini SAS for BladeSystem
- 1920103C | HP Smart Array P430i SAS Controller 1i x8 mini SAS
- 1922103C | HP Smart Array P430 2/4GB SAS Controller 1i x8 mini SAS
- 1923103C | HP Smart Array P431 2/4GB SAS Controller 2e x4 HD SAS
- 1926103C | HP Smart Array P731m 512MB/2GB SAS Controller for BladeSystem c-Class
- 1921103C | HP Smart Array P830i SAS Controller 2i x8 mini SAS Snap 6 (DL580)
- 1924103C | HP Smart Array P830 4GB SAS Controller 2i x8 ,mini SAS
- 1925103C | HP Smart Array P831 4GB SAS Controller 4e x4 HDSAS

This enhancement update adds the kmod-cciss packages to Red Hat Enterprise Linux 5 as part of the Red Hat Enterprise Linux Driver Update Program (DUP). (BZ#975150)

Only users requiring temporary driver support for the specific hardware noted above should install these packages. Unless a system includes the exact hardware explicitly supported by the kmod-cciss packages, these packages must not be installed.

3.3. RHEA-2013:1313 — new packages: mysql51

New mysql51 packages are now available for Red Hat Enterprise Linux 5.

MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) and many client programs and libraries.

The mysql51 package, provided as a Software Collection, is a metapackage that installs all necessary packages in order to use MySQL version 5.1. Software Collections allow users to install and use multiple versions of the same package in one system. Software Collection packages are installed into an alternate directory. Note that the MySQL 5.1 packages are provided only for the purposes of migrating to MySQL 5.5. You should not use the mysql51* packages on any of your production systems.

For more information about the changes included in MySQL 5.1, refer to the release notes.

This enhancement update adds the mysql51 packages to Red Hat Enterprise Linux 5. Install the mysql51 package in order to use the MySQL 5.1 server on your system, or as an intermediate step in the migration process to MySQL 5.5. (BZ#924769)

Note: for more information on the migration from MySQL 5.0 to MySQL 5.5, refer to chapter "Migrating from MySQL 5.0 to MySQL 5.5" in the "Red Hat Enterprise Linux 5 Deployment Guide" at https://access.redhat.com/site/documentation/Red_Hat_Enterprise_Linux/.

Note: Red Hat will not issue any more security advisories for the MySQL 5.0 packages (mysql-5.0.* and related packages). Security advisories will be provided only for MySQL 5.5.

All users who require mysql51 are advised to install these new packages.

3.4. RHEA-2013:1322 — new packages: gcc-libraries

New gcc-libraries packages are now available for Red Hat Enterprise Linux 5.

The new gcc-libraries packages contain various GCC runtime libraries, such as libatomic and libitm. In Red Hat Enterprise Linux 5.9, libitm was a separate package that included the libitm library. The libitm package is now deprecated and replaced by the gcc-libraries packages.

>This enhancement update adds the gcc-libraries packages to Red Hat Enterprise Linux 5. (BZ#906239)

All users who require gcc-libraries are advised to install these new packages.

3.5. RHEA-2013:1325 — new packages: mysql55

New mysql55 packages are now available for Red Hat Enterprise Linux 5.

MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) and many client programs and libraries.

The mysql55 package, provided as a Software Collection, is a metapackage that installs all necessary packages in order to use MySQL version 5.5. Software Collections allow users to install and use multiple versions of the same package in one system. Software Collection packages are installed into an alternate directory.

For more information about the changes included in MySQL 5.5, refer to the release notes.

This enhancement update adds the mysql55 packages to Red Hat Enterprise Linux 5. Install the mysql55 package in order to use the MySQL 5.5 server on your system. (BZ#924770)

Note: for more information on the migration from MySQL 5.0 to MySQL 5.5, refer to chapter "Migrating from MySQL 5.0 to MySQL 5.5" in the "Red Hat Enterprise Linux 5 Deployment Guide" at https://access.redhat.com/site/documentation/Red_Hat_Enterprise_Linux/.

Note: Red Hat will not issue any more security advisories for the MySQL 5.0 packages (mysql-5.0.* and

related packages). Security advisories will be provided only for MySQL 5.5.

All users who require mysql55 are advised to install these new packages.

3.6. RHEA-2013:1329 — new packages: mysql51-mysql

New mysql51-mysql packages are now available for Red Hat Enterprise Linux 5.

MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) and many client programs and libraries.

The mysql51-mysql package, provided as a Software Collection, contains MySQL version 5.1. Software Collections allow users to install and use multiple versions of the same package in one system. Software Collection packages are installed into an alternate directory. Note that the MySQL 5.1 packages are provided only for the purposes of migrating to MySQL 5.5. You should not use the mysql51* packages on any of your production systems.

For more information about the changes included in MySQL 5.1, refer to the release notes.

This enhancement update adds the mysql51-mysql packages to Red Hat Enterprise Linux 5. These packages include only the server part of MySQL 5.1; they do not include a client C library. A client C library that is a part of the core Red Hat Enterprise Linux 5 system is expected to be used to connect to the MySQL 5.1 server. (BZ#924771)

Note: for more information on the migration from MySQL 5.0 to MySQL 5.5, refer to chapter "Migrating from MySQL 5.0 to MySQL 5.5" in the "Red Hat Enterprise Linux 5 Deployment Guide" at https://access.redhat.com/site/documentation/Red_Hat_Enterprise_Linux/.

Note: Red Hat will not issue any more security advisories for the MySQL 5.0 packages (mysql-5.0.* and related packages). Security advisories will be provided only for MySQL 5.5.

All users who require mysql51-mysql are advised to install these new packages.

3.7. RHEA-2013:1330 — new packages: mysql55-mysql

New mysql55-mysql packages are now available for Red Hat Enterprise Linux 5.

MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) and many client programs and libraries.

The mysql55-mysql package, provided as a Software Collection, contains MySQL version 5.5. Software Collections allow users to install and use multiple versions of the same package in one system. Software Collection packages are installed into an alternate directory.

For more information about the changes included in MySQL 5.5, refer to the release notes.

This enhancement update adds the mysql55-mysql packages to Red Hat Enterprise Linux 5. These packages include only the server part of MySQL 5.5; they do not include a client C library. A client C library that is a part of the core Red Hat Enterprise Linux 5 system is expected to be used to connect to the MySQL 5.5 server. (BZ#924772)

Note: for more information on the migration from MySQL 5.0 to MySQL 5.5, refer to chapter "Migrating from MySQL 5.0 to MySQL 5.5" in the "Red Hat Enterprise Linux 5 Deployment Guide" at https://access.redhat.com/site/documentation/Red_Hat_Enterprise_Linux/.

Note: Red Hat will not issue any more security advisories for the MySQL 5.0 packages (mysql-5.0.* and related packages). Security advisories will be provided only for MySQL 5.5.

All users who require mysql55-mysql are advised to install these new packages.

3.8. RHEA-2013:1345 — new packages: python-lxml

New python-lxml packages are now available for Red Hat Enterprise Linux 5.

The python-lxml package provides bindings against libxml2 and libxslt, following, where possible, the ElementTree API, while also handling Unicode strings and memory management.

This enhancement update adds the python-lxml packages to Red Hat Enterprise Linux 5. (BZ#920884)

All users who require python-lxml are advised to install these new packages.

3.9. RHEA-2013:1346 — new package: python-dateutil

New python-dateutil package is now available for Red Hat Enterprise Linux 5.

The python-dateutil package includes bindings to provide powerful extensions to the standard datetime library provided by the system versions of Python.

This enhancement update adds the python-dateutil package to Red Hat Enterprise Linux 5. (BZ#920883)

Note: this package is being added as a dependency of the redhat-support-tool package.

All users who require python-dateutil are advised to install this new package.

3.10. RHEA-2013:1363 — new packages: redhat-support-lib-python and redhat-support-tool

New redhat-support-lib-python and redhat-support-tool packages are now available for Red Hat Enterprise Linux 5.

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 both the content and services available to them as Red Hat customers. Further, it enables our customers to integrate and automate their helpdesk services with our subscription services. The capabilities of this package include:

- Red Hat Access Knowledge Base article and solution viewing from the console (formatted as man pages). - Viewing, creating, modifying, and commenting on customer support cases from the console. - Attachment uploading directly to a customer support case or to ftp://dropbox.redhat.com/ from the console. - Full proxy support (that is, FTP and HTTP proxies). - Easy listing and downloading of attachments in customer support cases from the console. - Red Hat Access Knowledge Base searching on query terms, log messages, and other parameters, and viewing search results in a selectable list. - Easy uploading of log files, text files, and other sources to the Red Hat Access automatic problem determination engine for diagnosis. - Various other support-related commands.

Detailed usage information for the tool can be found in the Red Hat Customer Portal at https://access.redhat.com/site/articles/445443

This enhancement update adds the redhat-support-lib-python and redhat-support-tool packages to Red Hat Enterprise Linux 5. (BZ#869406, BZ#880766, BZ#987168, BZ#987170, BZ#987172, BZ#987160, BZ#967496, BZ#983085)

All users who require redhat-support-lib-python and redhat-support-tool are advised to install these new packages.

3.11. RHEA-2013:1364 — new packages: python-kerberos

New python-kerberos packages are now available for Red Hat Enterprise Linux 5.

This new python-kerberos package contains a high-level wrapper for Kerberos (GSSAPI) operations.

This enhancement update adds the python-kerberos packages to Red Hat Enterprise Linux 5. (BZ#975447)

All users who require python-kerberos are advised to install these new packages.

Chapter 4. Updated Packages

4.1. acroread

4.1.1. RHSA-2013:0150 — Critical: acroread security update

Updated acroread packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

Adobe Reader allows users to view and print documents in Portable Document Format (PDF).

Security Fix

CVE-2012-1530, CVE-2013-0601, CVE-2013-0602, CVE-2013-0603, CVE-2013-0604, CVE-2013-0605, CVE-2013-0606, CVE-2013-0607, CVE-2013-0608, CVE-2013-0609, CVE-2013-0610, CVE-2013-0611, CVE-2013-0612, CVE-2013-0613, CVE-2013-0614, CVE-2013-0615, CVE-2013-0616, CVE-2013-0617, CVE-2013-0618, CVE-2013-0619, CVE-2013-0620, CVE-2013-0621, CVE-2013-0623, CVE-2013-0626

This update fixes several security flaws in Adobe Reader. These flaws are detailed in the Adobe Security bulletin APSB13-02. A specially-crafted PDF file could cause Adobe Reader to crash or, potentially, execute arbitrary code as the user running Adobe Reader when opened.

All Adobe Reader users should install these updated packages. They contain Adobe Reader version 9.5.3, which is not vulnerable to these issues. All running instances of Adobe Reader must be restarted for the update to take effect.

4.1.2. RHSA-2013:0551 — Critical: acroread security update

Updated acroread packages that fix two security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

Adobe Reader allows users to view and print documents in Portable Document Format (PDF).

Security Fix

CVE-2013-0640, CVE-2013-0641

This update fixes two security flaws in Adobe Reader. These flaws are detailed in the Adobe Security bulletin APSB13-07. A specially-crafted PDF file could cause Adobe Reader to crash or, potentially, execute arbitrary code as the user running Adobe Reader when opened.

All Adobe Reader users should install these updated packages. They contain Adobe Reader version 9.5.4, which is not vulnerable to these issues. All running instances of Adobe Reader must be restarted for the update to take effect

4.1.3. RHSA-2013:0826 — Critical: acroread security update

Updated acroread packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

Adobe Reader allows users to view and print documents in Portable Document Format (PDF).

Security Fixes

CVE-2013-2549, CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2724, CVE-2013-2725, CVE-2013-2726, CVE-2013-2727, CVE-2013-2729, CVE-2013-2730, CVE-2013-2731, CVE-2013-2732, CVE-2013-2733, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, CVE-2013-3341

This update fixes multiple security flaws in Adobe Reader. These flaws are detailed in the Adobe Security bulletin APSB13-15. A specially-crafted PDF file could cause Adobe Reader to crash or, potentially, execute arbitrary code as the user running Adobe Reader when opened.

CVE-2013-2737

This update also fixes an information leak flaw in Adobe Reader.

All Adobe Reader users should install these updated packages. They contain Adobe Reader version 9.5.5, which is not vulnerable to these issues. All running instances of Adobe Reader must be restarted for the update to take effect.

4.2. am-utils

4.2.1. RHBA-2013:0864 — am-utils bug fix update

Updated am-utils packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The am-utils packages provide the BSD automounter, Amd, which maintains a cache of mounted file systems. File systems are mounted when they are first referenced by a user, and unmounted after a period of inactivity.

Bug Fix

BZ#964133

Previously, the BSD automounter ignored the NFS "noacl" mount option, which disables ACL (Access Control List) support on NFS shares. Local file systems such as ext3 do not have ACLs enabled unless the "acl" mount option is supplied. An attempt to use the setfacl utility or another ACL operation on a share that had "noacl" specified was supposed to result in an "Operation not supported" error, but it did not. With this update, a backported patch has been provided and the "noacl" option is supported as expected.

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

4.2.2. RHBA-2013:1349 — am-utils bug fix update

Updated am-utils packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The am-utils packages provide the BSD automounter, Amd, which maintains a cache of mounted file systems. File systems are mounted when they are first referenced by a user, and unmounted after a period of inactivity.

Bug Fixes

BZ#836359

Previously, the BSD automounter ignored the NFS "noacl" mount option, which disables ACL (Access Control List) support on NFS shares. Local file systems such as ext3 do not have ACLs enabled unless the "acl" mount option is supplied. An attempt to use the setfacl utility or another ACL operation on a share that had "noacl" specified was supposed to result in an "Operation not supported" error, but it did not. With this update, a backported patch has been provided and the "noacl" option is supported as expected.

BZ#862283

When using an autofs multi-level mount map amd failed to umount NFS leaf mounts causing shutdown to terminate unexpectedly. This was caused by the background umount of NFS mounts at the leaf of the tree not finishing before the autofs file system mounts above were attempted. As a consequence, the system became unresponsive during shutdown. With this update, a patch has been provided to fix this bug and the system no longer becomes unresponsive in this scenario.

Users of am-utils are advised to upgrade to these updated packages, which fix these bugs.

4.3. anaconda

4.3.1. RHBA-2013:1354 — anaconda bug fix update

Updated anaconda packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

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#751351

Previously, the lvm tool on cciss devices returned the list of PV (Physical Volume) paths delimited by exclamation marks while Anaconda expects the list to use the slash signs as the delimiter. Consequently, in some cases, lvm installation failed on cciss devices. The PV path list now uses the slash sign as the delimiter. As a result, lvm installation on cciss devices succeeds.

BZ#767260

The previous code function relied on the user having interface available in a corner case, that is more than 15 partitions on a disk. When a system was installed to a machine with a disk of more than 15 partitions, Anaconda terminated unexpectedly with a traceback. The method has been edited to first check whether the user interface is available and then log the message. As a result, installation on a machine with a disk of more than 15 partitions now works as expected.

BZ#873644

Previously, Anaconda completely ignored the lines in the /etc/fstab file that had the "noauto" mount option specified. Consequently, such lines were removed when upgrading the system. This update ensures that lines containing "noauto" are stored when parsing the /etc/fstab file and are written out to the new /etc/fstab file on upgrade.

BZ#907574

Previously, some translations, for example for NFS repository setup dialog window, were incomplete. Consequently, NFS repository setup dialog window in Russian locale contained incorrect translations. Incorrect translations have been fixed by updating the list of strings for translations and by adding missing Russian translations for the updated list. The NFS repository setup is now translated correctly for Russian.

BZ#908959

When Red Hat Enterprise Linux with the authconfig package specified in the packages lists was installed, authconfig, including the /etc/shadow file, was not installed. The authconfig package has been added to the packages list and is now successfully installed.

BZ#908959

Due to a regression, Anaconda detected the incorrect architecture value when checking for packages required for installation. Consequently, packages mandatory for installation were not installed. To fix this bug, the arch.getBaseArch() function is now used instead of arch.canonArch(), which returns the correct architecture value to Anaconda. As a result, packages required for installation are now installed, even if they are marked for exclusion in kickstart.

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

4.4. aspell

4.4.1. RHBA-2013:1309 — aspell bug fix update

Updated aspell packages that fix one bug are now available for Red Hat Enterprise Linux 5.

Aspell is a spelling checker that features compile-time and run-time support for English as well as non-English languages and can spell check TeX, LaTeX, and HTML files.

Bug Fix

BZ#862000

Using the "aspell dump master" command to create a dump of the master word list caused all of the words in the output to be truncated incorrectly. Specifically, the last letter of every word was cut off. This update fixes the string handling logic of the word lists, and output of the aforementioned command no longer contains incorrectly truncated words.

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

4.5. autofs

4.5.1. RHBA-2013:1350 — autofs bug fix update

Updated autofs packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The autofs utility controls the operation of the automount daemon. The automount daemon automatically mounts file systems when you use them and unmounts them when they are not busy. Autofs maps describe how file systems below the mount point of the map are to be mounted.

Bug Fixes

BZ#714766

Previously, autofs maps did not refresh the list of shares exported on the NFS server. As a consequence, ESTALE error messages were returned in the NFS client. A patch has been provided to fix this bug and autofs now refreshes the list of shares as expected. Moreover, within this bug, the ability to update hosts made on receiving a HUP signal has been added to autofs.

BZ#865309

Prior to this update, the description of MOUNT_WAIT setting in the configuration file was incorrect. Wrong timeout setting could cause problems as the mount utility would wait for a server that is temporarily unavailable. The description in the configuration file has been edited, thus fixing this bug.

BZ#866337

Previously, autofs manual pages described the "nobind" autofs option incorrectly, thus it was not possible to specify different options for individual direct mount maps. The manual pages have been updated to describe the current behavior of "nobind", which fixes the bug.

BZ#909263

A change that removed code to add the current map entry caused wildcard indirect multi-mount map entries to fail to mount. A patch to fix wildcard multi-map regression has been provided and map entries now mount successfully.

BZ#918843

Previously, the autofs RPC function, used to receive the exports list from a host, did not try all potentially available mountd versions. Consequently, when certain mountd protocol versions were disabled, autofs RPC function failed to receive the exports list. A patch has been provided to fix this bug and autofs RPC function now receives the exports list successfully.

BZ#947604

When the automount utility was sent a shutdown signal, the "autofs reload" command was causing automount to stop running when multiple maps were being removed from the auto.master map. A patch has been provided to fix this bug and automount no longer stops running in the described scenario.

BZ#976592

When using autofs with LDAP (Lightweight Directory Access Protocol), the code used to perform a base DN (distinguished name) search allowed a race between two threads executing the same function simultaneously to occur. As a consequence, autofs could attempt to access already freed memory and terminate unexpectedly due to a segmentation fault. With this update, the code used to perform base DN searches has been moved to the function protected by a mutex, which prevents the race from occurring. The base DN searches are now performed only when the map lookup modules settings are being refreshed.

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

4.6. axis

4.6.1. RHSA-2013:0683 — Moderate: axis security update

Updated axis packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

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

Apache Axis is an implementation of SOAP (Simple Object Access Protocol). It can be used to build both web service clients and servers.

Security Fix

CVE-2012-5784

Apache Axis did not verify that the server hostname matched the domain name in the subject's Common Name (CN) or subjectAltName field in X.509 certificates. This could allow a man-in-the-middle attacker to spoof an SSL server if they had a certificate that was valid for any domain name.

All users of axis are advised to upgrade to these updated packages, which correct this issue. Applications using Apache Axis must be restarted for this update to take effect.

4.7. bash

4.7.1. RHBA-2013:1040 — bash bug fix update

Updated bash packages that fix one bug are now available for Red Hat Enterprise Linux 5.

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

Bug Fix

BZ#978840

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

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

4.8. bind97

4.8.1. RHSA-2013:0690 — Important: bind97 security update

Updated bind97 packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

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

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

Security Fix

CVE-2013-2266

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

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

All bind97 users are advised to upgrade to these updated packages, which contain a patch to correct this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

4.8.2. RHSA-2013:1115 — Important: bind97 security update

Updated bind97 packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

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

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

Security Fix

CVE-2013-4854

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

All bind97 users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

4.9. binutils

4.9.1. RHBA-2013:1306 — binutils bug fix update

Updated binutils packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The binutils packages are a collection of programming tools for the manipulation of object code in various object file formats.

Bug Fixes

BZ#817056

Due to instability in calculating the program header size, the GNU linker could terminate unexpectedly with a "looping in map_segments" error message. With this update, the linker has been modified to properly handle changes in the size of the segment map, which prevents the instability, and the linker no longer crashes in this scenario.

BZ#855163

Previously, the PowerPC linker made assumptions about the order of instructions and relocations. Those assumptions were not correct for code compiled with GNU Compiler Collection version 4.1 (GCC-4.1). As a result, the linker could trigger an internal error during optimization of TLS sequences. Now, the linker code to optimize TLS has been modified to not attempt to optimize TLS

sequences which do not meet its assumptions about code and relocation ordering. Therefore, the linker no longer triggers an internal error when optimizing TLS sequences.

BZ#924354

The PowerPC linker did not verify whether certain pointers were validly non-NULL prior to dereferencing those pointers. As a result, under certain circumstances, the PowerPC linker could encounter a segmentation fault or a bus error. With this update, the PowerPC linker code has been changed to properly check for NULL pointers and take appropriate action, and links no longer experience segmentation faults or bus errors.

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

4.10. boost

4.10.1. RHSA-2013:0668 — Moderate: boost security update

Updated boost packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

The boost packages provide free, peer-reviewed, portable C++ source libraries with emphasis on libraries which work well with the C++ Standard Library.

Security Fix

CVE-2012-2677

A flaw was found in the way the ordered_malloc() routine in Boost sanitized the 'next_size' and 'max_size' parameters when allocating memory. If an application used the Boost C++ libraries for memory allocation, and performed memory allocation based on user-supplied input, an attacker could use this flaw to crash the application or, potentially, execute arbitrary code with the privileges of the user running the application.

All users of boost are advised to upgrade to these updated packages, which contain a backported patch to fix this issue.

4.11. ccid

4.11.1. RHSA-2013:1323 — Low: ccid security and bug fix update

An updated ccid package that fixes one security issue and one bug is now available for Red Hat Enterprise Linux 5.

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

Chip/Smart Card Interface Devices (CCID) is a USB smart card reader standard followed by most modern smart card readers. The ccid package provides a Generic, USB-based CCID driver for readers, which follow this standard.

Security Fix

CVE-2010-4530

An integer overflow, leading to an array index error, was found in the way the CCID driver processed a smart card's serial number. A local attacker could use this flaw to execute arbitrary code with the privileges of the user running the PC/SC Lite pcscd daemon (root, by default), by inserting a specially-crafted smart card.

Bug Fix

BZ#907821

The pcscd service failed to read from the SafeNet Smart Card 650 v1 when it was inserted into a smart card reader. The operation failed with a "IFDHPowerICC() PowerUp failed" error message. This was due to the card taking a long time to respond with a full Answer To Reset (ATR) request, which lead to a timeout, causing the card to fail to power up. This update increases the timeout value so that the aforementioned request is processed properly, and the card is powered on as expected.

All ccid users are advised to upgrade to this updated package, which contains backported patches to correct these issues.

4.12. clustermon

4.12.1. RHBA-2013:0787 — clustermon bug fix update

Updated clustermon packages that fix one bug are now available for Red Hat Enterprise Linux 5.

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

Bug Fix

BZ#958026

Prior to this update, the dynamic library that represents the CIM provider of a cluster status was not built with all the required dependencies, and certain symbols could not be resolved. As a consequence, the cluster status could not be accessed by CIM. This update adds the missing dependencies to the dynamic library, and the cluster status is now accessible as expected.

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

4.12.2. RHBA-2013:1305 — clustermon bug fix update

Updated clustermon packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

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

Bug Fixes

BZ#847289

Previously, the SNMP agent exposing the cluster status and shipped as cluster-snmp caused the SNMP server (snmpd) to terminate unexpectedly with a segmentation fault when this module was

loaded, and the containing server was told to reload. This was caused by an improper disposal of the resources facilitated by this server, alarms in particular. Now, the module will properly clean up such resources when being unloaded, preventing the crash on reload.

BZ#882277

Prior to this update, the dynamic library that represents the CIM provider of a cluster status was not built with all the required dependencies, and certain symbols could not be resolved. As a consequence, the cluster status could not be accessed by CIM. This update adds the missing dependencies to the dynamic library, and the cluster status is now accessible as expected.

BZ#957798

When modclusterd was about to associate the local machine with a particular cluster node entry from the cluster configuration, it first tried CMAN API in an improper way, yielding no expected results. This process occurred every five seconds. As a consequence, it had to periodically resort to iterative detection through local interface addresses. Also when logging for CMAN enabled, and including membership messages, it would cause messages arising from the CMAN API misuse to be emitted. Now, the API is used as expected, which corrects the aforementioned consequences.

BZ#965792

Previously, a segmentation fault occurred in the modclusterd daemon and/or modcluster, ricci cluster-dedicated module, when processing large cluster.conf files (or peer-delivered counterparts). This was caused by the allocation of large amounts of memory not available on the stack. With this update, a patch has been introduced to allocate memory on the heap, and provide an error if not enough memory is available. As a result, crashes no longer occur in the described scenario.

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

4.13. cman

4.13.1. RHBA-2013:1131 — cman bug fix update

Updated cman packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

Bug Fix

BZ#986981

Due to incorrect detection of newline characters during an SSH connection, the fence_drac5 agent could terminate the connection with a traceback error when fencing a Red Hat Enterprise Linux cluster node. Only the first fencing action completed successfully but the status of the node was not checked correctly. Consequently, the fence agent failed to report successful fencing. When the "reboot" operation was called, the node was only powered off. With this update, the newline characters are correctly detected and fencing works as expected.

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

4.13.2. RHBA-2013:0761 — cman bug fix update

Updated cman packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

Bug Fix

BZ#951049

Under some circumstances cman can return the fence daemon for the /dev/zero file, which is always active, and if the client application stores this instead of the one it expects then it will loop forever. This update addresses the problem by making sure that the fence daemon refreshes the file descriptor on each operation.

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

4.13.3. RHBA-2013:1304 — cman bug fix update

Updated cman packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

Bug Fixes

BZ#714042

Prior to this update, ccs_tool could fail due to a segmentation fault in two specific events. First, the input file was the same as the output file and options were specified with a subcommand. Second, the update command was used without an input file. With this update, ccs_tool has been fixed to report the appropriate error message without a segmentation fault.

BZ#854183

Previously, fence_xvm, a fencing agent commonly used in virtual deployments, did not respect the delay parameter as specified in the cluster.conf file. With this update, the delay support has been added and the fence_xvm agent now works only after the specified delay.

BZ#856214

Under some circumstances, cman returned the file descriptor for the /dev/zero file, which is always active. If the client application stored this /dev/zero file instead of the one it expected, cman entered an infinite loop. This update addresses the bug by making sure that the fence daemon refreshes the file descriptor on each operation.

BZ#876731

In a two node cluster where the network was not always reliable, and a token was lost but recovered before fencing was complete, the two nodes simultaneously killed each other. To fix this bug, only one node has been allowed to kill the other in a deterministic fashion. A cluster restart, one node at a time, is required for this change to take effect.

BZ#881217

Prior to this update, fenced, the daemon in charge of evicting cluster nodes, could suffer from a time-out while communicating with the ccsd cluster configuration daemon. The fenced daemon has been reconnected to ccsd when certain operations take too long to complete, thus fixing this bug.

BZ#883816

Previously, man pages had executable flags set. The manual pages permissions have been edited to agree with FHS standard, thus fixing this bug.

BZ#904195

Prior to this update, the end-of-line automatic character detection worked properly only when using

ssh on certain Dell DRAC devices. With this update, the end-of-line character detection has been fixed and fencing works as expected.

BZ#886612

Prior to this update, APC power switches with firmware version 5.x were not supported. Consequently, the fence_apc fencing script could not login to the device. With this update, new firmware is supported and the fencing script is able to log in.

BZ#961119

Previously, the fence agent for Intel IPMILAN standard did not return exit code correctly when using the 'cycle' method. A patch has been provided to fix this bug and exit codes are now returned as expected.

BZ#963251

Prior to this update, the cman(5) man page did not document how to enable detailed logging in the CMAN subsystem. This update documents this facility in more detail.

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

4.13.4. RHBA-2013:0678 — cman bug fix update

Updated cman packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The Cluster Manager (cman) utility provides user-level services for managing a Linux cluster.

Bug Fix

BZ#923861

In a two node cluster, under some circumstances where the network was not always reliable, and a token was lost but recovered before fencing was complete, then the two nodes simultaneously killed each other. With this update, the problem is solved by allowing only one node to kill the other in a deterministic fashion. A cluster restart, one node at a time, is required for this change to take effect.

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

4.14. conga

4.14.1. RHBA-2013:1358 — conga bug fix update

Updated conga packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

Conga is an agent/server architecture for remote administration of systems. It provides a convenient method for creating and managing clusters built with Red Hat Cluster Suite. It also offers an interface for managing sophisticated storage configurations like those often built to support clusters. The agent component is called "ricci", and the server (or the web-based front end of the Conga cluster management) is called "luci".

Bug Fixes

BZ#514679

Previously, a non-English locale caused luci, to display improper copyright information in the pages' footer. The respective template has been fixed so as not to translate the application-specific part and the whole footer now displays information correctly even in non-English locales.

BZ#853018

Prior to this update, luci contained non-visual links dedicated to better browsing experience in the agents supporting it, such as navigation to the site map, the access to which resulted in an error. The page titles also contained some rare inconsistencies. The luci templates clean-up has been provided to fix respective corner cases.

BZ#872645

For extremely large cluster.conf files, the luci serializer could not handle the complexity of a cluster configuration object as the serializer run into the recursion depth limit. Consequently, error messages were returned in luci. Caching of the object representing cluster configuration has been abandoned so that this error no longer occurs.

BZ#883804

Previously, the ricci(8) and luci_admin(8) manual pages of the respective conga packages were installed with incorrect permissions. File permissions have been corrected in the installation procedure and the manual pages are now installed correctly.

BZ#887170

Each time luci was used to start or restart a cluster, or to have previously inactivated node rejoined the cluster, it made cluster services such as cman, rgmanager or clvmd enabled on boot on the respective cluster nodes. This can interfere with the user's preferences, for instance, when running a 2-nodes cluster without a quorum disk and having the services disabled on purpose on one of the nodes to prevent fence races. To avoid this, Conga has been changed so that it no longer modifies the existing settings in the mentioned cases, while still enabling the services when the cluster is created or a new node is added.

BZ#965785

Previously, a segmentation fault occurred in the ricci daemon when processing cluster.conf files with very large values. This was caused by allocating large amounts of memory that were not available on the stack. A patch has been introduced to allocate memory on the heap and provide ar error message if not enough memory is available. As a result, the segmentation fault no longer occurs.

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

4.15. coolkey

4.15.1. RHEA-2013:1324 — coolkey enhancement update

Updated coolkey packages that add one enhancement are now available for Red Hat Enterprise Linux 5.

Coolkey is a smart card support library for the CoolKey, CAC, and PIV smart cards.

Enhancement

BZ#948649

Support for tokens containing ECC certificates has been added to the coolkey package.

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

4.16. cpio

4.16.1. RHBA-2013:1299 — cpio bug fix update

Updated cpio packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The cpio packages provide the GNU cpio utility for creating and extracting archives, or copying files from one place to another.

Bug Fix

BZ#867834

Previously, the cpio command was unable to split file names longer than 155 bytes into two parts during the creation of archives of the "ustar" format. Consequently, cpio could store malformed file names or terminate unexpectedly with a segmentation fault. With this update, cpio now handles long file names without problems, and crashes no longer occur in the described scenario.

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

4.17. cups

4.17.1. RHSA-2013:0580 — Moderate: cups security update

Updated cups packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

The Common UNIX Printing System (CUPS) provides a portable printing layer for Linux, UNIX, and similar operating systems.

Security Fix

CVE-2012-5519

It was discovered that CUPS administrative users (members of the SystemGroups groups) who are permitted to perform CUPS configuration changes via the CUPS web interface could manipulate the CUPS configuration to gain unintended privileges. Such users could read or write arbitrary files with the privileges of the CUPS daemon, possibly allowing them to run arbitrary code with root privileges.

After installing this update, the ability to change certain CUPS configuration directives remotely will be disabled by default. The newly introduced ConfigurationChangeRestriction directive can be used to enable the changing of the restricted directives remotely. Refer to Red Hat Bugzilla bug 875898 for more details and the list of restricted directives.

All users of cups are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the cupsd daemon will be restarted automatically.

4.18. curl

4.18.1. RHSA-2013:0771 — Moderate: curl security update

Updated curl packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

cURL provides the libcurl library and a command line tool for downloading files from servers using various protocols, including HTTP, FTP, and LDAP.

Security Fix

CVE-2013-1944

A flaw was found in the way libcurl matched domains associated with cookies. This could lead to cURL or an application linked against libcurl sending the wrong cookie if only part of the domain name matched the domain associated with the cookie, disclosing the cookie to unrelated hosts.

Red Hat would like to thank the cURL project for reporting this issue. Upstream acknowledges YAMADA Yasuharu as the original reporter.

Users of curl should upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications using libcurl must be restarted for the update to take effect.

4.18.2. RHSA-2013:0983 — Moderate: curl security update

Updated curl packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

cURL provides the libcurl library and a command line tool for downloading files from servers using various protocols, including HTTP, FTP, and LDAP.

Security Fix

CVE-2013-2174

A heap-based buffer overflow flaw was found in the way libcurl unescaped URLs. A remote attacker could provide a specially-crafted URL that, when processed by an application using libcurl that handles untrusted URLs, would possibly cause it to crash or, potentially, execute arbitrary code.

Red Hat would like to thank the cURL project for reporting this issue. Upstream acknowledges Timo Sirainen as the original reporter.

Users of curl should upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications using libcurl must be restarted for the update to take effect.

4.19. dbus

4.19.1. RHBA-2013:1361 — dbus bug fix update

Updated dbus packages that fix one bug are now available for Red Hat Enterprise Linux 5.

D-Bus is a system for sending messages between applications. It is used for the system-wide message bus service and as a per-user-login-session messaging facility.

Bug Fix

BZ#517169

Due to improper holding of file handles by D-Bus and gnome-vfs-daemon (specifically in the gtk_file_chooser_dialog_new() function), running a firmware update application on an IBM tape device caused a file handle to be opened for that tape device and never released. With this update, all open file handles are now properly closed, and the aforementioned application no longer holds the tape device indefinitely.

Users of dbus are advised to upgrade to these updated packages, which fix this bug. For the update to take effect, all running instances of dbus-daemon and all running applications using the libdbus library must be restarted, or the system rebooted.

4.20. dbus-glib

4.20.1. RHSA-2013:0568 — Important: dbus-glib security update

Updated dbus-glib packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

dbus-glib is an add-on library to integrate the standard D-Bus library with the GLib main loop and threading model.

Security Fix

CVE-2013-0292

A flaw was found in the way dbus-glib filtered the message sender (message source subject) when the "NameOwnerChanged" signal was received. This could trick a system service using dbus-glib (such as fprintd) into believing a signal was sent from a privileged process, when it was not. A local attacker could use this flaw to escalate their privileges.

All dbus-glib users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications linked against dbus-glib, such as fprintd and NetworkManager, must be restarted for this update to take effect.

4.21. device-mapper-multipath

4.21.1. RHBA-2013:0779 — device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The device-mapper-multipath packages provide tools to manage multipath devices using the device-mapper multipath kernel module.

Bug Fix

BZ#951435

Previously, the multipathd daemon did not stop and wait for all of its threads on shutdown, which caused multipathd to occasionally terminate unexpectedly with a segmentation fault during shutdown. With this update, multipathd now correctly stops and waits for its threads during shutdown, and crashes no longer occur in the described scenario.

Users of device-mapper-multipath are advised to upgrade to these updated packages, which fix this bug.

4.21.2. RHBA-2013:0226 — device-mapper-multipath bug fix update

Updated device-mapper-multipath packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The device-mapper-multipath packages provide tools to manage multipath devices using the device-mapper multipath kernel module.

Bug Fix

BZ#904106

Previously, the uev_discard() function did not take into account trailing NULL bytes in stack variables. Consequently, on 32-bit systems with the cciss disk controller driver that uses long device names, the multipathd daemon could terminate unexpectedly with a segmentation fault. A patch has been provided to fix uev_discard() and the crashes no longer occur in the described scenario.

All users of device-mapper-multipath are advised to upgrade to these updated packages, which fix this bug.

4.21.3. RHBA-2013:1314 — 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 5.

The device-mapper-multipath packages provide tools to manage multipath devices using the device-mapper multipath kernel module.

Bug Fixes

BZ#522108

Multipath was not correctly getting the vendor, product, and revision strings for certain devices. Consequently, users were unable to correctly configure or use these devices with multipath. With this update, multipath now uses a SCSI inquiry IOCTL request to correctly get this information, and multipath is now able to configure and use these devices.

BZ#855147

When a partition was resized, kpartx reloaded the partition device with the NOFLUSH flag enabled, which device-mapper does not allow, causing the device to be left in a suspended state. Users had to manually resume the devices to restore their use. However, this did not fix the partition device size, and the partitioned device would become unusable again the next time kpartx was run on the device. With this update, kpartx now checks if the partition has changed size, and does not set the NOFLUSH flag when reloading a partitioned device with a new size. Now, users can repartition devices with kpartx without those devices becoming unusable.

BZ#860185

Previously, the multipathd daemon did not stop and wait for all of its threads on shutdown, which caused multipathd to occasionally terminate unexpectedly with a segmentation fault during shutdown. With this update, multipathd now correctly stops and waits for its threads during shutdown, and crashes no longer occur in the described scenario.

BZ#872439

Previously, the multipathd daemon terminated unexpectedly with a segmentation fault on 32-bit systems with a cciss disk controller. This was caused by a stack corruption in uev_discard() function. This update corrects the code in the uev_discard() function, and crashes no longer occur in the described scenario.

BZ#910585

If the /var/cache directory was a separate file system, the multipathd daemon unmounted it in its private namespace on start up. However, multipath requires the /var/cache directory to properly setup its private namespace. Consequently, the multipathd daemon failed to start on machines where the /var/cache directory was a separate file system. With this update, the multipathd daemon no longer unmounts the /var/cache directory from its private namespace, and multipathd will now correctly start up on machines where the /var/cache directory is a separate file system.

BZ#948309

Multipath switched to use the cciss_id callout for HP P2000 G3 SAS storage devices, which did not correctly provide the UUID. Consequently, multipath was unable to correctly configure HP P2000 G3 SAS devices. With this update, multipath switched back to using the scsi_id callout with the "-n" option to enable it to function with cciss devices, and multipath can now correctly configure HP P2000 G3 SAS devices.

Enhancements

BZ#799907

This update adds a built-in configuration for the IBM XIV Storage System.

BZ#839983

With this update, when multipath is set to log level 3, it will now print messages whenever it forks to execute a callout. This update helps debug a segmentation fault with multipath on Xen setups.

BZ#916630

With this update, the default configuration for NetApp devices now includes the "flush_on_last_del yes" parameter. With the default configuration, when all path devices to a NetApp LUN have been removed from the system, the multipath device for that LUN stops queuing I/O.

Users of device-mapper-multipath are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.22. dhcp

4.22.1. RHBA-2013:0183 — dhcp bug fix update

Updated dhcp packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The Dynamic Host Configuration Protocol (DHCP) is a protocol that allows individual devices on an IP network to get their own network configuration information, including an IP address, a subnet mask, and a broadcast address. The dhcp packages provide a relay agent and ISC DHCP service required to enable and administer DHCP on a network.

Bug Fix

BZ#902359

When the dhclient utility was executed with the "-1" command-line option, and then issued a DHCPDECLINE message, it restarted the process of acquiring a lease instead of exiting, as is expected with the "-1" option. A patch has been provided to address this bug and now, after sending a DHCPDECLINE message, dhclient prints out an error message and exits properly.

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

4.23. dovecot

4.23.1. RHBA-2013:0976 — dovecot bug fix update

Updated dovecot packages that fix one bug are now available for Red Hat Enterprise Linux 5.

Dovecot is an IMAP server for Linux and other UNIX-like systems, primarily written with security in mind. It also contains a small POP3 server. It supports email in either the maildir or mbox format. The SQL drivers and authentication plug-ins are provided as sub-packages.

Bug Fix

BZ#968377

Previously, the dovecot package contained a bug in the LDAP-related code and could get into an infinite loop when an LDAP connection was unstable, making it impossible for users to log in and read emails. This update fixes the LDAP code and dovecot now handles unstable connections with an LDAP server without problems.

Users of dovecot are advised to upgrade to these updated packages, which contain backported patches to fix this bug. After installing the updated packages, the dovecot service will be restarted automatically.

4.24. e2fsprogs

4.24.1. RHBA-2013:0793 — e2fsprogs bug fix update

Updated e2fsprogs packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The e2fsprogs packages provide a number of utilities for creating, checking, modifying, and correcting any inconsistencies in the ext2 file systems.

Bug Fix

BZ#949435

A bug in the libblkid library allowed an access to the already freed memory when reading block device entries in cache during kernel installation using the grubby tool. As a consequence, grubby could terminate unexpectedly with a segmentation fault causing the installation to fail. This update modifies libblkid so that it now properly handles pointers to the device structure, and the kernel can

now be installed as expected when using grubby.

Users of e2fsprogs are advised to upgrade to these updated packages, which fix this bug.

4.25. elinks

4.25.1. RHSA-2013:0250 — Moderate: elinks security update

An updated elinks package that fixes one security issue is now available for Red Hat Enterprise Linux 5 and 6.

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

ELinks is a text-based web browser. ELinks does not display any images, but it does support frames, tables, and most other HTML tags.

Security Fix

CVE-2012-4545

It was found that ELinks performed client credentials delegation during the client-to-server GSS security mechanisms negotiation. A rogue server could use this flaw to obtain the client's credentials and impersonate that client to other servers that are using GSSAPI.

This issue was discovered by Marko Myllynen of Red Hat.

All ELinks users are advised to upgrade to this updated package, which contains a backported patch to resolve the issue.

4.26. esc

4.26.1. RHBA-2013:0734 — esc bug fix update

Updated esc packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The esc packages contain the Smart Card Manager GUI, which allows user to manage security smart cards. The primary function of the tool is to enroll smart cards, so that they can be used for common cryptographic operations, such as secure e-mail and website access.

Bug Fix

BZ#921957

The ESC utility did not start when the latest 17 series release of the XULRunner runtime environment was installed on the system. This update includes necessary changes to ensure that ESC works as expected with the latest version of XULRunner.

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

4.27. firefox

4.27.1. RHSA-2013:0271 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2013-0775, **CVE-2013-0780**, **CVE-2013-0782**, **CVE-2013-0783**

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-0776

It was found that, after canceling a proxy server's authentication prompt, the address bar continued to show the requested site's address. An attacker could use this flaw to conduct phishing attacks by tricking a user into believing they are viewing a trusted site.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Nils, Abhishek Arya, Olli Pettay, Christoph Diehl, Gary Kwong, Jesse Ruderman, Andrew McCreight, Joe Drew, Wayne Mery, and Michal Zalewski as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 17.0.3 ESR.

Note that due to a Kerberos credentials change, the following configuration steps may be required when using Firefox 17.0.3 ESR with the Enterprise Identity Management (IPA) web interface:

https://access.redhat.com/knowledge/solutions/294303

Important: Firefox 17 is not completely backwards-compatible with all Mozilla add-ons and Firefox plug-ins that worked with Firefox 10.0. Firefox 17 checks compatibility on first-launch, and, depending on the individual configuration and the installed add-ons and plug-ins, may disable said Add-ons and plug-ins, or attempt to check for updates and upgrade them. Add-ons and plug-ins may have to be manually updated.

All Firefox users should upgrade to these updated packages, which contain Firefox version 17.0.3 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.27.2. RHSA-2013:1140 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2013-1701

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-1710

A flaw was found in the way Firefox generated Certificate Request Message Format (CRMF) requests. An attacker could use this flaw to perform cross-site scripting (XSS) attacks or execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-1709

A flaw was found in the way Firefox handled the interaction between frames and browser history. An attacker could use this flaw to trick Firefox into treating malicious content as if it came from the browser history, allowing for XSS attacks.

CVE-2013-1713

It was found that the same-origin policy could be bypassed due to the way Uniform Resource Identifiers (URI) were checked in JavaScript. An attacker could use this flaw to perform XSS attacks, or install malicious add-ons from third-party pages.

CVE-2013-1714

It was found that web workers could bypass the same-origin policy. An attacker could use this flaw to perform XSS attacks.

CVE-2013-1717

It was found that, in certain circumstances, Firefox incorrectly handled Java applets. If a user launched an untrusted Java applet via Firefox, the applet could use this flaw to obtain read-only access to files on the user's local system.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Jeff Gilbert, Henrik Skupin, moz_bug_r_a4, Cody Crews, Federico Lanusse, and Georgi Guninski as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 17.0.8 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 17.0.8 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.27.3. RHSA-2013:0981 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2013-1682, **CVE-2013-1684**, **CVE-2013-1685**, **CVE-2013-1686**, **CVE-2013-1687**, **CVE-2013-1690**

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-1692

It was found that Firefox allowed data to be sent in the body of XMLHttpRequest (XHR) HEAD requests. In some cases this could allow attackers to conduct Cross-Site Request Forgery (CSRF) attacks.

CVE-2013-1693

Timing differences in the way Firefox processed SVG image files could allow an attacker to read data across domains, potentially leading to information disclosure.

CVE-2013-1694, **CVE-2013-1697**

Two flaws were found in the way Firefox implemented some of its internal structures (called wrappers). An attacker could use these flaws to bypass some restrictions placed on them. This could lead to unexpected behavior or a potentially exploitable crash.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Gary Kwong, Jesse Ruderman, Andrew McCreight, Abhishek Arya, Mariusz Mlynski, Nils, Johnathan Kuskos, Paul Stone, Boris Zbarsky, and moz_bug_r_a4 as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 17.0.7 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 17.0.7 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.27.4. RHSA-2013:0696 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2013-0788

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-0795

A flaw was found in the way Same Origin Wrappers were implemented in Firefox. A malicious site could use this flaw to bypass the same-origin policy and execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-0796

A flaw was found in the embedded WebGL library in Firefox. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox. Note: This issue only affected systems using the Intel Mesa graphics drivers.

CVE-2013-0800

An out-of-bounds write flaw was found in the embedded Cairo library in Firefox. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-0793

A flaw was found in the way Firefox handled the JavaScript history functions. A malicious site could cause a web page to be displayed that has a baseURI pointing to a different site, allowing cross-site scripting (XSS) and phishing attacks.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Olli Pettay, Jesse Ruderman, Boris Zbarsky, Christian Holler, Milan Sreckovic, Joe Drew, Cody Crews, miaubiz, Abhishek Arya, and Mariusz Mlynski as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 17.0.5 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 17.0.5 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.27.5. RHSA-2013:1268 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2013-1718, **CVE-2013-1722**, **CVE-2013-1725**, **CVE-2013-1730**, **CVE-2013-1732**, **CVE-2013-1735**, **CVE-2013-1736**

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-1737

A flaw was found in the way Firefox handled certain DOM JavaScript objects. An attacker could use this flaw to make JavaScript client or add-on code make incorrect, security sensitive decisions.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges André Bargull, Scoobidiver, Bobby Holley, Reuben Morais, Abhishek Arya, Ms2ger, Sachin Shinde, Aki Helin, Nils, and Boris Zbarsky as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 17.0.9 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 17.0.9 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.27.6. RHSA-2013:0820 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla Firefox.

Security Fixes

CVE-2013-0801, CVE-2013-1674, CVE-2013-1675, CVE-2013-1676, CVE-2013-1677, CVE-2013-1678, CVE-2013-1679, CVE-2013-1680, CVE-2013-1681

Several flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-1670

A flaw was found in the way Firefox handled Content Level Constructors. A malicious site could use this flaw to perform cross-site scripting (XSS) attacks.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Christoph Diehl, Christian Holler, Jesse Ruderman, Timothy Nikkel, Jeff Walden, Nils, Ms2ger, Abhishek Arya, and Cody Crews as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 17.0.6 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 17.0.6 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.28. flash-plugin

4.28.1. RHSA-2013:0941 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes one security issue is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2013-3343

This update fixes one vulnerability in Adobe Flash Player. This vulnerability is detailed in the Adobe Security bulletin APSB13-16. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the malicious SWF content.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.291.

4.28.2. RHSA-2013:0643 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2013-0646, **CVE-2013-0650**, **CVE-2013-1371**, **CVE-2013-1375**

This update fixes multiple vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB13-09. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the malicious SWF content.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.275.

4.28.3. RHSA-2013:1256 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes four security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2013-3361, **CVE-2013-3362**, **CVE-2013-3363**, **CVE-2013-5324**

This update fixes four vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB13-21. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the malicious SWF content.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.310.

4.28.4. RHSA-2013:0825 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2013-2728, **CVE-2013-3324**, **CVE-2013-3325**, **CVE-2013-3326**, **CVE-2013-3327**, **CVE-2013-3328**, **CVE-2013-3329**, **CVE-2013-3330**, **CVE-2013-3331**, **CVE-2013-3332**, **CVE-2013-3333**, **CVE-2013-3334**, **CVE-2013-3335**

This update fixes multiple vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB13-14. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the malicious SWF content.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.285.

4.28.5. RHSA-2013:0243 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes two security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2013-0633, **CVE-2013-0634**

This update fixes two vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB13-04. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the malicious SWF content.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.262.

4.28.6. RHSA-2013:0574 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes three security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fixes

CVE-2013-0504, **CVE-2013-0648**

This update fixes two vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB13-08. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the malicious SWF content.

CVE-2013-0643

This update also fixes a permissions issue with the Adobe Flash Player Firefox sandbox.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.273.

4.28.7. RHSA-2013:0730 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2013-1378, **CVE-2013-1379**, **CVE-2013-1380**, **CVE-2013-2555**

This update fixes multiple vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB13-11. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the malicious SWF content.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.280.

4.28.8. RHSA-2013:1035 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes three security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2013-3344, **CVE-2013-3345**, **CVE-2013-3347**

This update fixes three vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB13-17. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the malicious SWF content.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.297.

4.28.9. RHSA-2013:0149 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes one security issue is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2013-0630

This update fixes one vulnerability in Adobe Flash Player. This vulnerability is detailed in the Adobe Security bulletin APSB13-01. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the malicious SWF content.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.261.

4.28.10. RHSA-2013:0254 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fixes

CVE-2013-0638, **CVE-2013-0639**, **CVE-2013-0642**, **CVE-2013-0644**, **CVE-2013-0645**, **CVE-2013-0647**, **CVE-2013-0649**, **CVE-2013-1365**, **CVE-2013-1366**, **CVE-2013-1367**, **CVE-2013-1368**, **CVE-2013-1369**, **CVE-2013-1370**, **CVE-2013-1372**, **CVE-2013-1373**, **CVE-2013-1374**

This update fixes several vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB13-05. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the malicious SWF content.

CVE-2013-0637

A flaw in flash-plugin could allow an attacker to obtain sensitive information if a victim were tricked into visiting a specially-crafted web page.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.270.

4.29. freetype

4.29.1. RHSA-2013:0216 — Important: freetype security update

Updated freetype packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

FreeType is a free, high-quality, portable font engine that can open and manage font files. It also loads, hints, and renders individual glyphs efficiently.

Security Fix

CVE-2012-5669

A flaw was found in the way the FreeType font rendering engine processed certain Glyph Bitmap Distribution Format (BDF) fonts. If a user loaded a specially-crafted font file with an application linked against FreeType, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. The X server must be restarted (log out, then log back in) for this update to take effect.

4.30. gdm

4.30.1. RHSA-2013:1213 — Important: gdm security update

Updated gdm and initscripts packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

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

The GNOME Display Manager (GDM) provides the graphical login screen, shown shortly after boot up, log out, and when user-switching.

Security Fix

CVE-2013-4169

A race condition was found in the way GDM handled the X server sockets directory located in the system temporary directory. An unprivileged user could use this flaw to perform a symbolic link attack, giving them write access to any file, allowing them to escalate their privileges to root.

Note that this erratum includes an updated initscripts package. To fix CVE-2013-4169, the vulnerable code was removed from GDM and the initscripts package was modified to create the affected directory safely during the system boot process. Therefore, this update will appear on all systems, however systems without GDM installed are not affected by this flaw.

Red Hat would like to thank the researcher with the nickname vladz for reporting this issue.

All users should upgrade to these updated packages, which correct this issue. The system must be rebooted for this update to take effect.

4.31. gfs2-utils

4.31.1. RHBA-2013:1339 — gfs2-utils bug fix update

Updated gfs2-utils packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The gfs2-utils packages contain a number of utilities for creating, checking, modifying, and correcting any inconsistencies in GFS2 file systems.

Bug Fixes

BZ#877150

Previously, a bug in the fsck.gfs2 utility caused files to be placed in the /lost+found/ directory, and these files could not be deleted in some circumstances. As a result, the fsck.gfs2 utility in Red Hat Enterprise Linux 6.4 was better able to repair GFS2 file system damage than in 5.9 or earlier versions. This update corrects these issues by including several fixes for the bugs from a newer version of the fsck.gfs2 utility, and Red Hat Enterprise Linux version 5.10 is able to fix GFS2 file systems as well as in version 6.4.

BZ#883864

Prior to this update, the manual pages included in the gfs2-utils package were incorrectly installed with permissions set to 0755. This was not necessary, because manual pages do not contain executable data. This update fixes the problem by updating the package to install these manual pages with permissions set to 0644, which is similar to other manual pages.

BZ#887374

The gfs2_convert utility allows the user to convert a file system from GFS to GFS2. Previously, this utility did not properly convert files and directories with certain metadata characteristics. As a consequence, running the fsck.gfs2 utility after such a conversion produced a number of errors. This update fixes the gfs2_convert tool so that it properly handles those file and directory metadata characteristics. As a result, the fsck.gfs2 utility no longer reports errors when run after a conversion.

BZ#994643

Prior to this update, if one of gfs2_tool, gfs2_quota, gfs2_grow, or gfs2_jadd was killed unexpectedly, a temporary GFS2 metadata mount point used by those tools could be left mounted. The mount point was also not registered in /etc/mtab and so the "umount -a -t gfs2" command would not unmount it. This mount point could prevent systems from rebooting properly, and cause the kernel to panic in cases where it was manually unmounted after the normal GFS2 mount point. This update fixes the problem by creating an mtab entry for the temporary mount point and unmounting it before exiting when signals are received.

Users of gfs2-utils are advised to upgrade to these updated packages, which fix these bugs.

4.31.2. RHBA-2013:0902 — gfs2-utils bug fix update

Updated gfs2-utils packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The gfs2-utils package provides the user-space utilities necessary to mount, create, maintain and test GFS2 file systems.

Bug Fix

BZ#956030

Previously, the gfs2_convert tool, which converts file systems from GFS to GFS2, did not properly convert files and directories with certain metadata characteristics. This caused errors to be reported when fsck.gfs2 was run after the conversion. This update fixes the gfs2_convert tool so that it properly handles those file and directory metadata characteristics. As a result, no errors should be reported when fsck.gfs2 is run after the conversion.

Users of gfs2-utils are advised to upgrade to these updated packages, which fix this bug.

4.32. ghostscript

4.32.1. RHBA-2013:1277 — ghostscript bug fix update

Updated ghostscript packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The Ghostscript suite contains utilities for rendering PostScript and PDF documents. Ghostscript translates PostScript code to common, bitmap formats so that the code can be displayed or printed.

Bug Fix

BZ#1006165

Previously, some PDF files with incomplete ASCII base-85 encoded images caused the ghostscript utility to terminate with the following error:

```
/syntaxerror in ID
```

The problem occurred when the image ended with "~" (tilde) instead of "~>" (tilde, right angle bracket) as defined in the PDF specification. An upstream patch has been applied and ghostscript now handles these PDF files without errors.

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

4.33. glibc

4.33.1. RHBA-2013:1308 — glibc bug fix update

Updated glibc packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The glibc packages provide the standard C libraries (libc), POSIX thread libraries (libpthread), standard math libraries (libm), and the Name Server Caching Daemon (nscd) used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

Bug Fixes

BZ#706571

The library uses the compat_call() function which in turn uses the getgrent_r() function which is reentrant safe, but not thread safe. As a result, if multiple threads call getgrent_r() using compat_call(), they may race against each other, resulting in some groups not being properly reported. With this update, locking was added to the compat_call() function to prevent multiple threads from racing. All groups are now properly reported.

BZ#816647

A library security mechanism failed to correctly run the initialization function of dynamically-loaded

character conversion routines. Consequently, glibc could sometimes terminate unexpectedly with a segmentation fault when attempting to use one dynamically-loaded character conversion routine. The library security mechanism has been fixed to correctly run the initialization function. After this update, the aforementioned problem no longer occurs in this situation.

BZ#835828

Various bugs in the wide character version of the fseek() function resulted in the internal FILE offset field being set incorrectly in wide character streams. As a result, the offset returned by the ftell() function was incorrect, and sometimes, data could be overwritten. The ftell() function was fixed to correctly set the internal FILE offset field for wide characters. The ftell() and fseek() functions now handle offsets for wide characters correctly.

BZ#861871

A fix to prevent logic errors in various mathematical functions, including exp(), exp2(), expf(), exp2f(), pow(), sin(), tan(), and rint(), caused by inconsistent results when the functions were used with the non-default rounding mode, creates performance regressions for certain inputs. The performance regressions have been analyzed and the core routines have been optimized to improve performance.

BZ#929035

A defect in the nscd daemon caused it to cache results for DNS entries with a TTL value of zero. This caused DNS lookups to return stale results. The nscd daemon has been fixed to correctly respect DNS TTL entries of zero. The nscd daemon no longer cache DNS entries with a TTL of zero and lookups for those entries return the correct and current results.

BZ#957089

A defect in the library localization routines resulted in unexpected termination of the application in low-memory conditions. The affected routines have been fixed to correctly detect and report errors when a low-memory condition prevents their correct operation. Applications running under low-memory conditions no longer terminate unexpectedly while calling localization routines.

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

4.33.2. RHBA-2013:0885 — glibc bug fix update

Updated glibc packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

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, a Linux system cannot function correctly.

Bug Fixes

BZ#962903

A bug in the nscd daemon caused it to cache results for DNS entries with a TTL value of zero. Consequently, DNS lookups returned stale results. The nscd daemon has been fixed to correctly respect DNS TTL entries of zero. Now, nscd no longer caches DNS entries with a TTL of zero and lookups for those entries return correct and current results.

BZ#963812

Previously, a library-security mechanism failed to correctly run the initialization functions of dynamically loaded character-conversion routines. This could lead to an unexpected termination with a segmentation fault when trying to use such a routine. With this update, the library-security

mechanism has been fixed to correctly run the initialization functions and the character-conversion routines no longer cause crashes.

BZ#963813

Due to a bug in the library-localization routines, applications could terminate unexpectedly in low-memory conditions. The affected routines have been fixed to correctly detect and report errors in the event of a low-memory condition preventing their correct operation. As a result, applications running under low-memory conditions no longer crash while calling localization routines.

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

4.33.3. RHBA-2013:0732 — glibc bug fix update

Updated glibc packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The glibc packages provide the standard C and standard math libraries used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

Bug Fix

BZ#924825

The C library security mechanism was unable to handle dynamically loaded character conversion routines when loaded at specific virtual addresses. This resulted in an unexpected termination with a segmentation fault when trying to use the dynamically loaded character conversion routine. This update enhances the C library security mechanism to handle dynamically loaded character conversion routines at any virtual memory address and the crashes no longer occur in the described scenario.

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

4.33.4. RHSA-2013:0769 — Low: glibc security and bug fix update

Updated glibc packages that fix two security issues and two bugs are now available for Red Hat Enterprise Linux 5.

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

The 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-2013-1914

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.

CVE-2013-0242

A flaw was found in the regular expression matching routines that process multibyte character input. If an application utilized the glibc regular expression matching mechanism, an attacker could provide specially-crafted input that, when processed, would cause the application to crash.

Bug Fixes

BZ#950535

The improvements RHSA-2012:1207 made to the accuracy of floating point functions in the math library caused performance regressions for those functions. The performance regressions were analyzed and a fix was applied that retains the current accuracy but reduces the performance penalty to acceptable levels. Refer to Red Hat Knowledge solution 229993 for further information.

BZ#951493

It was possible that a memory location freed by the localization code could be accessed immediately after, resulting in a crash. The fix ensures that the application does not crash by avoiding the invalid memory access.

Users of glibc are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

4.34. gnome-vfs2

4.34.1. RHBA-2013:1039 — gnome-vfs2 bug fix update

Updated gnome-vfs2 packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The gnome-vfs2 packages provide the GNOME virtual file system (GNOME VFS) which is the foundation of the Nautilus file manager.

Bug Fix

BZ#972702

A recent upgrade that modified the behavior of the stat() function to better support symbolic links caused the Nautilus file manager to not display the items in the Trash directory. The underlying source code was unable to find the right path of the Trash directory, making the Trash directory appear empty. With this update, an extra stat() call is in place to ensure the right information is provided, and moving files to the Trash directory now works as expected.

Users of gnome-vfs2 are advised to upgrade to these updated packages, which fix this bug.

4.35. gnutls

4.35.1. RHSA-2013:0883 — Important: gnutls security update

Updated gnutls packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

The GnuTLS library provides support for cryptographic algorithms and for protocols such as Transport Layer Security (TLS).

Security Fix

CVE-2013-2116

It was discovered that the fix for the CVE-2013-1619 issue released via RHSA-2013:0588 introduced a regression in the way GnuTLS decrypted TLS/SSL encrypted records when CBC-mode cipher suites were used. A remote attacker could possibly use this flaw to crash a server or client application that uses GnuTLS.

Users of GnuTLS are advised to upgrade to these updated packages, which correct this issue. For the update to take effect, all applications linked to the GnuTLS library must be restarted.

4.35.2. RHSA-2013:0588 — Moderate: gnutls security update

Updated gnutls packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

The GnuTLS library provides support for cryptographic algorithms and for protocols such as Transport Layer Security (TLS).

Security Fix

CVE-2013-1619

It was discovered that GnuTLS leaked timing information when decrypting TLS/SSL protocol encrypted records when CBC-mode cipher suites were used. A remote attacker could possibly use this flaw to retrieve plain text from the encrypted packets by using a TLS/SSL server as a padding oracle.

Users of GnuTLS are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. For the update to take effect, all applications linked to the GnuTLS library must be restarted, or the system rebooted.

4.36. gtk2

4.36.1. RHBA-2013:1366 — gtk2 bug fix update

Updated gtk2 packages that fix one bug are now available for Red Hat Enterprise Linux 5.

GIMP Toolkit (GTK+) is a multi-platform toolkit for creating graphical user interfaces.

Bug Fix

BZ#649682

Previously, a post-installation process error occurred when updating GTK2 on systems using Itanium processors due to an incorrect usage of hard coded paths that were not translated correctly on the Itanium architecture. This update corrects the errors in the hard coded paths, and it is now possible to update GTK2 on Itanium processors.

Users of gtk2 are advised to upgrade to these updated packages, which fix this bug.

4.37. httpd

4.37.1. RHSA-2013:0815 — Moderate: httpd security update

Updated httpd packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having 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 Apache HTTP Server is a popular web server.

Security Fixes

CVE-2012-4558

Cross-site scripting (XSS) flaws were found in the mod_proxy_balancer module's manager web interface. If a remote attacker could trick a user, who was logged into the manager web interface, into visiting a specially-crafted URL, it would lead to arbitrary web script execution in the context of the user's manager interface session.

CVE-2013-1862

It was found that mod_rewrite did not filter terminal escape sequences from its log file. If mod_rewrite was configured with the RewriteLog directive, a remote attacker could use specially-crafted HTTP requests to inject terminal escape sequences into the mod_rewrite log file. If a victim viewed the log file with a terminal emulator, it could result in arbitrary command execution with the privileges of that user.

CVE-2012-3499

Cross-site scripting (XSS) flaws were found in the mod_info, mod_status, mod_imagemap, mod_ldap, and mod_proxy_ftp modules. An attacker could possibly use these flaws to perform XSS attacks if they were able to make the victim's browser generate an HTTP request with a specially-crafted Host header.

All httpd users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the httpd daemon will be restarted automatically.

4.37.2. RHSA-2013:1156 — Moderate: httpd security update

Updated httpd packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

The Apache HTTP Server is a popular web server.

Security Fix

CVE-2013-1896

A flaw was found in the way the mod_dav module of the Apache HTTP Server handled merge requests. An attacker could use this flaw to send a crafted merge request that contains URIs that are not configured for DAV, causing the httpd child process to crash.

All httpd users should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, the httpd daemon will be restarted automatically.

4.37.3. RHBA-2013:0984 — httpd bug fix update

Updated httpd packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server.

Bug Fix

BZ#974162

Due to a bug in the mod_mem_cache module, child processes sometimes terminated unexpectedly with a segmentation fault while using the threaded "worker" Multi-Processing Modules (MPM) (/usr/sbin/httpd.worker). This update fixes mod_mem_cache to repair thread-safety issues, and crashes no longer occur in the described scenario.

Users of httpd are advised to upgrade to these updated packages, which fix this bug. After installing the updated packages, the httpd daemon will be restarted automatically.

4.38. hwcert-client-1.5

4.38.1. RHBA-2013:1125 — hwcert-client-1.5 bug fix and enhancement update

An updated hwcert-client package that fixes several bugs and adds multiple enhancements is now available for Red Hat Enterprise Linux Hardware Certification.

hwcert-client, the Red Hat Enterprise Linux hardware certification test suite, verifies the compatibility of hardware devices. Each hwcert-client test run builds a results database for submission to Red Hat's hardware catalog as an RPM package. hwcert-client replaces v7, and Red Hat Hardware Test Suite (HTS) for certifying hardware for use with Red Hat Enterprise Linux.

This updated hwcert-client package includes numerous bug fixes and enhancements. Space precludes documenting all of these changes in this advisory. Documentation for these changes will be available shortly from the Test Suite Release Notes:

https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux_Hardware_Certification/1/html-single/Test_Suite_Release_Notes/index.html

All users of hwcert-client are advised to upgrade to this updated package, which provides numerous bug fixes and enhancements.

4.39. hwdata

4.39.1. RHEA-2013:1342 — hwdata enhancement update

Updated hwdata packages that add one enhancement are now available for Red Hat Enterprise Linux 5.

The hwdata packages contain various hardware identification and configuration data.

Enhancement

BZ#963249

The PCI ID numbers have been updated for the Beta and the Final compose lists.

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

4.40. hypervkvpd

4.40.1. RHSA-2013:0807 — Low: hypervkvpd security and bug fix update

An updated hypervkvpd package that fixes one security issue and one bug is now available for Red Hat Enterprise Linux 5.

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

The hypervkvpd package contains hypervkvpd, the guest Microsoft Hyper-V Key-Value Pair (KVP) daemon. The daemon passes basic information to the host through VMBus, such as the guest IP address, fully qualified domain name, operating system name, and operating system release number.

Security Fix

CVE-2012-5532

A denial of service flaw was found in the way hypervkvpd processed certain Netlink messages. A local, unprivileged user in a guest (running on Microsoft Hyper-V) could send a Netlink message that, when processed, would cause the guest's hypervkvpd daemon to exit.

The CVE-2012-5532 issue was discovered by Florian Weimer of the Red Hat Product Security Team.

Bug Fix

BZ#953502

The hypervkvpd daemon did not close the file descriptors for pool files when they were updated. This could eventually lead to hypervkvpd crashing with a "KVP: Failed to open file, pool: 1" error after consuming all available file descriptors. With this update, the file descriptors are closed, correcting this issue.

Users of hypervkvpd are advised to upgrade to this updated package, which contains backported patches to correct these issues. After installing the update, it is recommended to reboot all guest machines.

4.41. initscripts

4.41.1. RHBA-2013:1300 — initscripts bug fix update

Updated *initscripts* packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The *initscripts* package contains system scripts to boot your system, change runlevels, activate and deactivate most network interfaces, and shut the system down cleanly.

Bug Fixes

BZ#545881

Previously, the information in the sysconfig.txt file was not precise enough and could mislead the users:

```
Enable or disable IPv6 configuration for this interface
```

The text has been updated to the following form:

```
Enable or disable IPv6 static, DHCP, or autoconf configuration for
this interface
```

From the updated information it is now clear that the **IPV6INIT=no** setting does not mean that the whole IPv6 is disabled.

BZ#636861

Previously, the shutdown script ran the **hardware clock** tool, which attempted to access the **/dev/rtc** device even if it did not exist. A patch has been provided to fix this bug and **initscripts** now verifies if the **/dev/rtc** device exists before attempting to run the **hardware clock** tool.

BZ#735982

Prior to this update, the **sysctl.d** feature was not included in the **sysctl** utility manual page. The manual page has been updated, thus fixing the bug.

BZ#747418

Previously, primary slave was set before bond initialization, which led to error messages being returned. To fix this bug, the **primary=** option is ignored before slaves are set up and this value is set after the enslavement. As a result, no error messages are returned.

BZ#814058

When kernel module required a device removal, the **/etc/sysconfig/network-scripts/net.hotplug** utility tried to remove the device. As the device was not present, it led to an error message being returned. The patched version checks whether the **/sys/class/net/$DEVICE** device is present and if not, the device is now ignored.

BZ#843386

After sending a **TERM** signal, the **killproc()** function always waited a number of seconds before it checked the process again. Consequently, the user waited unnecessarily long. A patch has been provided to check the process multiple times during the delay. As a result, **killproc()** can continue almost immediately after the process ends.

BZ#844671

The previous version of the **kpartx** tool was not called with **-p p** option, which led to inconsistent partition mappings on some disks or partitions not mapped at all. A patch has been provided to fix this bug. All configured devices are now properly represented in the **/dev/mapper** application and have the correct partition mappings present with consistent delimiter usage.

BZ#852967

When the names of **initscripts** and **lockfile** differed, the **status()** function was not able to determine whether the subsystem was locked. The possibility to specify explicitly the name of lockfile through the **-l** option has been added and the **status()** function can now determine whether the subsystem is locked.

BZ#853038

The previous version of **initscripts** did not support the IPv6 routing in the same way the IPv4 routing did. IPv6 addressing and routing could be achieved only by specifying the **ip** commands explicitly with the **-6** flag in the **/etc/sysconfig/network-scripts/route-DEVICE_NAME** configuration file (where **DEVICE_NAME** is the name of the respective network interface). With this

update, related network scripts have been modified to provide support for IPv6 routing. IPv6 routing is now configured separately in the the **/etc/sysconfig/network-scripts/route6-DEVICE_NAME** file, thus fixing this bug.

BZ#860252

Previous version of sysconfig.txt file led users to insert the **VLAN=yes** option into the global configuration file. Consequently, an interface with a name containing a dot (brbond0.XX) was recognized as a VLAN interface. To fix this bug, sysconfig.txt has been changed and VLAN stanza has been added to the interface configuration file. As a result, the above mentioned devices are no longer recognized as VLAN interfaces.

BZ#862597

The descriptions of the ***kernel.msgmax*** parameter:

```
Controls the default maxmimum size of a message queue
```

and the ***kernel.msgmnb*** parameter:

```
Controls the maximum size of a message, in bytes
```

in the default **/etc/sysctl.conf** were incorrect. As the actual definitions are vice versa, the descriptions have been swapped, thus fixing the bug.

BZ#880890

If a network bond device had a name that was a substring of another bond device, both devices changed their states due to the incorrect bond device name test. A patch has been provided in the regular expression test and bond devices now change their states as expected.

BZ#957109

Previously, the sysconfig.txt file advised users to use an incorrect command, **saslauthd -a** instead of **saslauthd -v**. Consequently, the command failed with an error message. The instruction in the sysconfig.txt file has been corrected and the **saslauthd -v** command now returns expected results.

Enhancements

BZ#705218

Users can now set the NIS (Network Information Service) domain name by configuring the ***NISDOMAIN*** parameter in the **/etc/sysconfig/network** file, or other relevant configuration files.

Users of *initscripts* are advised to upgrade to these updated packages, which fix these bugs and add one enhancement.

4.42. ipa-client

4.42.1. RHSA-2013:0189 — Important: ipa-client security update

An updated ipa-client package that fixes one security issue is now available for Red Hat Enterprise Linux 5.

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

Red Hat Identity Management is a centralized authentication, identity management and authorization solution for both traditional and cloud-based enterprise environments.

Security Fix

CVE-2012-5484

A weakness was found in the way IPA clients communicated with IPA servers when initially attempting to join IPA domains. As there was no secure way to provide the IPA server's Certificate Authority (CA) certificate to the client during a join, the IPA client enrollment process was susceptible to man-in-the-middle attacks. This flaw could allow an attacker to obtain access to the IPA server using the credentials provided by an IPA client, including administrative access to the entire domain if the join was performed using an administrator's credentials.

Note: This weakness was only exposed during the initial client join to the realm, because the IPA client did not yet have the CA certificate of the server. Once an IPA client has joined the realm and has obtained the CA certificate of the IPA server, all further communication is secure. If a client were using the OTP (one-time password) method to join to the realm, an attacker could only obtain unprivileged access to the server (enough to only join the realm).

Red Hat would like to thank Petr Menšík for reporting this issue.

When a fix for this flaw has been applied to the client but not yet the server, ipa-client-install, in unattended mode, will fail if you do not have the correct CA certificate locally, noting that you must use the "--force" option to insecurely obtain the certificate. In interactive mode, the certificate will try to be obtained securely from LDAP. If this fails, you will be prompted to insecurely download the certificate via HTTP. In the same situation when using OTP, LDAP will not be queried and you will be prompted to insecurely download the certificate via HTTP.

Users of ipa-client are advised to upgrade to this updated package, which corrects this issue.

4.42.2. RHBA-2013:1334 — ipa-client bug fix update

Updated ipa-client packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

IPA (Identity, Policy, Audit) is an integrated solution to provide centrally managed identity, that is, machine, user, virtual machines, groups, and authentication credentials. The ipa-client package provides a tool to enroll a machine to an IPA version 2 server.

Bug Fixes

BZ#821500

If the IPA CA (Certification Authority) could not be added to the shared NSS database in the /etc/pki/nssdb/ directory, the client installer terminated unexpectedly with a fatal error message. The location of the directory has been fixed and the client installer no longer crashes.

BZ#907071

Due to a missing dependency on the pyOpenSSL package, installation of the ipa-client package failed. The missing dependency has been added and ipa-client can now be installed as expected.

BZ#915504

In some cases, a CA certificate was stored in the base64-encoded form (PEM) instead of the binary form (DER). The wrong CA format caused ipa-client to act as if no CA was available and the system enrollment to terminate unexpectedly. The ipa-client-install utility has been fixed to make the client more flexible and be able to handle the data stored in either format. As a result, the system enrollment as an IPA client now succeeds.

BZ#949632

Due to a bug, if one of the IPA masters was unavailable during enrollment, the ipa-client-install did not fail over to another master. Consequently, the ipa-client installation terminated unexpectedly. This bug has been fixed, and ipa-client-install now fails over to a functional replica as expected.

BZ#961132

Previously, there was more than one code path where a cleanup routine could be called. If the xmlrpc_env_clean() function preceded the initializing xmlrpc_env_init() function, the unenrolling of a client could fail. The order of the calls in xmlrpc-c has been edited and unenrolling a client no longer fails.

BZ#976372

In some cases, if replication between two IPA masters was slow, there was a short time period where the client was not known to one of the masters. Consequently, the kinit utility failed. The installation process has been reordered so that all operations are done against the same master the enrollment is initiated with.

Users of ipa-client are advised to upgrade to these updated packages, which fix these bugs.

4.43. jakarta-commons-httpclient

4.43.1. RHSA-2013:0270 — Moderate: jakarta-commons-httpclient security update

Updated jakarta-commons-httpclient packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

The Jakarta Commons HttpClient component can be used to build HTTP-aware client applications (such as web browsers and web service clients).

Security Fix

CVE-2012-5783

The Jakarta Commons HttpClient component did not verify that the server hostname matched the domain name in the subject's Common Name (CN) or subjectAltName field in X.509 certificates. This could allow a man-in-the-middle attacker to spoof an SSL server if they had a certificate that was valid for any domain name.

All users of jakarta-commons-httpclient are advised to upgrade to these updated packages, which correct this issue. Applications using the Jakarta Commons HttpClient component must be restarted for this update to take effect.

4.44. java-1.5.0-ibm

4.44.1. RHSA-2013:1081 — Important: java-1.5.0-ibm security update

Updated java-1.5.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM J2SE version 5.0 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

> CVE-2013-1500, CVE-2013-1571, CVE-2013-2443, CVE-2013-2444, CVE-2013-2446, CVE-2013-2447, CVE-2013-2448, CVE-2013-2450, CVE-2013-2452, CVE-2013-2454, CVE-2013-2455, CVE-2013-2456, CVE-2013-2457, CVE-2013-2459, CVE-2013-2463, CVE-2013-2464, CVE-2013-2465, CVE-2013-2469, CVE-2013-2470, CVE-2013-2471, CVE-2013-2472, CVE-2013-2473, CVE-2013-3743
>
> This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

Red Hat would like to thank Tim Brown for reporting CVE-2013-1500, and US-CERT for reporting CVE-2013-1571. US-CERT acknowledges Oracle as the original reporter of CVE-2013-1571.

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM J2SE 5.0 SR16-FP3 release. All running instances of IBM Java must be restarted for this update to take effect.

4.44.2. RHSA-2013:0855 — Important: java-1.5.0-ibm security update

Updated java-1.5.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM J2SE version 5.0 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

> CVE-2013-0169, CVE-2013-0401, CVE-2013-1491, CVE-2013-1537, CVE-2013-1557, CVE-2013-1569, CVE-2013-2383, CVE-2013-2384, CVE-2013-2394, CVE-2013-2417, CVE-2013-2419, CVE-2013-2420, CVE-2013-2424, CVE-2013-2429, CVE-2013-2430, CVE-2013-2432
>
> This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM J2SE 5.0 SR16-FP2 release. All running instances of IBM Java must be restarted for this update to take effect.

4.44.3. RHSA-2013:0624 — Critical: java-1.5.0-ibm security update

Updated java-1.5.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM J2SE version 5.0 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

CVE-2013-0409, CVE-2013-0424, CVE-2013-0425, CVE-2013-0426, CVE-2013-0427, CVE-2013-0428, CVE-2013-0432, CVE-2013-0433, CVE-2013-0434, CVE-2013-0440, CVE-2013-0442, CVE-2013-0443, CVE-2013-0445, CVE-2013-0450, CVE-2013-0809, CVE-2013-1476, CVE-2013-1478, CVE-2013-1480, CVE-2013-1481, CVE-2013-1486, CVE-2013-1493

> This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM J2SE 5.0 SR16 release. All running instances of IBM Java must be restarted for this update to take effect.

4.45. java-1.6.0-ibm

4.45.1. RHSA-2013:0625 — Critical: java-1.6.0-ibm security update

Updated java-1.6.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM Java SE version 6 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

CVE-2012-1541, CVE-2012-3213, CVE-2012-3342, CVE-2013-0351, CVE-2013-0409, CVE-2013-0419, CVE-2013-0423, CVE-2013-0424, CVE-2013-0425, CVE-2013-0426, CVE-2013-0427, CVE-2013-0428, CVE-2013-0432, CVE-2013-0433, CVE-2013-0434, CVE-2013-0435, CVE-2013-0438, CVE-2013-0440, CVE-2013-0441, CVE-2013-0442, CVE-2013-0443, CVE-2013-0445, CVE-2013-0446, CVE-2013-0450, CVE-2013-0809, CVE-2013-1473, CVE-2013-1476, CVE-2013-1478, CVE-2013-1480, CVE-2013-1481, CVE-2013-1486, CVE-2013-1487, CVE-2013-1493

> This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM Java SE 6 SR13 release. All running instances of IBM Java must be restarted for the update to take effect.

4.45.2. RHSA-2013:1059 — Critical: java-1.6.0-ibm security update

Updated java-1.6.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM Java SE version 6 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

CVE-2013-1500, CVE-2013-1571, CVE-2013-2407, CVE-2013-2412, CVE-2013-2437, CVE-2013-2442, CVE-2013-2443, CVE-2013-2444, CVE-2013-2446, CVE-2013-2447, CVE-2013-2448, CVE-2013-2450, CVE-2013-2451, CVE-2013-2452, CVE-2013-2453, CVE-2013-2454, CVE-2013-2455, CVE-2013-2456, CVE-2013-2457, CVE-2013-2459, CVE-2013-2463, CVE-2013-2464, CVE-2013-2465, CVE-2013-2466, CVE-2013-2468, CVE-2013-2469, CVE-2013-2470, CVE-2013-2471, CVE-2013-2472, CVE-2013-2473, CVE-2013-3743

> This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

Red Hat would like to thank Tim Brown for reporting CVE-2013-1500, and US-CERT for reporting CVE-2013-1571. US-CERT acknowledges Oracle as the original reporter of CVE-2013-1571.

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM Java SE 6 SR14 release. All running instances of IBM Java must be restarted for the update to take effect.

4.45.3. RHSA-2013:0823 — Critical: java-1.6.0-ibm security update

Updated java-1.6.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM Java SE version 6 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

CVE-2013-0169, CVE-2013-0401, CVE-2013-1491, CVE-2013-1537, CVE-2013-1540, CVE-2013-1557, CVE-2013-1563, CVE-2013-1569, CVE-2013-2383, CVE-2013-2384, CVE-2013-2394, CVE-2013-2417, CVE-2013-2418, CVE-2013-2419, CVE-2013-2420, CVE-2013-2422, CVE-2013-2424, CVE-2013-2429, CVE-2013-2430, CVE-2013-2432, CVE-2013-2433, CVE-2013-2435, CVE-2013-2440

> This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM Java SE 6 SR13-FP2 release. All running instances of IBM Java must be restarted for the update to take effect.

4.46. java-1.6.0-openjdk

4.46.1. RHSA-2013:0604 — Important: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

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

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2013-0809

An integer overflow flaw was found in the way the 2D component handled certain sample model instances. A specially-crafted sample model instance could cause Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with virtual machine privileges.

CVE-2013-1493

It was discovered that the 2D component did not properly reject certain malformed images. Specially-crafted raster parameters could cause Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with virtual machine privileges.

This erratum also upgrades the OpenJDK package to IcedTea6 1.11.9. Refer to the NEWS file for further information.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.46.2. RHSA-2013:0770 — Important: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2013-1569, **CVE-2013-2383**, **CVE-2013-2384**

Multiple flaws were discovered in the font layout engine in the 2D component. An untrusted Java application or applet could possibly use these flaws to trigger Java Virtual Machine memory corruption.

CVE-2013-1558, **CVE-2013-2422**, **CVE-2013-1518**, **CVE-2013-1557**

Multiple improper permission check issues were discovered in the Beans, Libraries, JAXP, and RMI components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-1537

The previous default value of the java.rmi.server.useCodebaseOnly property permitted the RMI implementation to automatically load classes from remotely specified locations. An attacker able to connect to an application using RMI could use this flaw to make the application execute arbitrary code.

CVE-2013-2420

Note: The fix for CVE-2013-1537 changes the default value of the property to true, restricting class loading to the local CLASSPATH and locations specified in the java.rmi.server.codebase property. Refer to Red Hat Bugzilla bug 952387 for additional details.

The 2D component did not properly process certain images. An untrusted Java application or applet could possibly use this flaw to trigger Java Virtual Machine memory corruption.

CVE-2013-2431, **CVE-2013-2421**

It was discovered that the Hotspot component did not properly handle certain intrinsic frames, and did not correctly perform MethodHandle lookups. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-2429, **CVE-2013-2430**

It was discovered that JPEGImageReader and JPEGImageWriter in the ImageIO component did not protect against modification of their state while performing certain native code operations. An untrusted Java application or applet could possibly use these flaws to trigger Java Virtual Machine memory corruption.

CVE-2013-1488, **CVE-2013-2426**

The JDBC driver manager could incorrectly call the toString() method in JDBC drivers, and the ConcurrentHashMap class could incorrectly call the defaultReadObject() method. An untrusted Java application or applet could possibly use these flaws to bypass Java sandbox restrictions.

CVE-2013-0401

The sun.awt.datatransfer.ClassLoaderObjectInputStream class may incorrectly invoke the system class loader. An untrusted Java application or applet could possibly use this flaw to bypass certain Java sandbox restrictions.

CVE-2013-2417, **CVE-2013-2419**

Flaws were discovered in the Network component's InetAddress serialization, and the 2D component's font handling. An untrusted Java application or applet could possibly use these flaws to crash the Java Virtual Machine.

CVE-2013-2424

The MBeanInstantiator class implementation in the OpenJDK JMX component did not properly check class access before creating new instances. An untrusted Java application or applet could use this flaw to create instances of non-public classes.

CVE-2013-2415

It was discovered that JAX-WS could possibly create temporary files with insecure permissions. A local attacker could use this flaw to access temporary files created by an application using JAX-WS.

This erratum also upgrades the OpenJDK package to IcedTea6 1.11.10. Refer to the NEWS file for further information.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.46.3. RHSA-2013:0246 — Important: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix several security issues are now available for Red Hat Enterprise Linux 5.

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

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2013-0442, **CVE-2013-0445**, **CVE-2013-0441**, **CVE-2013-1475**, **CVE-2013-1476**, **CVE-2013-0429**, **CVE-2013-0450**, **CVE-2013-0425**, **CVE-2013-0426**, **CVE-2013-0428**

Multiple improper permission check issues were discovered in the AWT, CORBA, JMX, and Libraries components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-1478, **CVE-2013-1480**

Multiple flaws were found in the way image parsers in the 2D and AWT components handled image raster parameters. A specially-crafted image could cause Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with the virtual machine privileges.

CVE-2013-0432

A flaw was found in the AWT component's clipboard handling code. An untrusted Java application or applet could use this flaw to access clipboard data, bypassing Java sandbox restrictions.

CVE-2013-0435

The default Java security properties configuration did not restrict access to certain com.sun.xml.internal packages. An untrusted Java application or applet could use this flaw to access information, bypassing certain Java sandbox restrictions. This update lists the whole package as restricted.

CVE-2013-0427, **CVE-2013-0433**, **CVE-2013-0434**

Multiple improper permission check issues were discovered in the Libraries, Networking, and JAXP components. An untrusted Java application or applet could use these flaws to bypass certain Java sandbox restrictions.

CVE-2013-0424

It was discovered that the RMI component's CGIHandler class used user inputs in error messages without any sanitization. An attacker could use this flaw to perform a cross-site scripting (XSS) attack.

CVE-2013-0440

It was discovered that the SSL/TLS implementation in the JSSE component did not properly enforce handshake message ordering, allowing an unlimited number of handshake restarts. A remote attacker could use this flaw to make an SSL/TLS server using JSSE consume an excessive amount of CPU by continuously restarting the handshake.

CVE-2013-0443

It was discovered that the JSSE component did not properly validate Diffie-Hellman public keys. An SSL/TLS client could possibly use this flaw to perform a small subgroup attack.

This erratum also upgrades the OpenJDK package to IcedTea6 1.11.6. Refer to the NEWS file for further information.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.46.4. RHSA-2013:1014 — Important: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2013-2470, **CVE-2013-2471**, **CVE-2013-2472**, **CVE-2013-2473**, **CVE-2013-2463**, **CVE-2013-2465**, **CVE-2013-2469**

Multiple flaws were discovered in the ImagingLib and the image attribute, channel, layout and raster processing in the 2D component. An untrusted Java application or applet could possibly use these flaws to trigger Java Virtual Machine memory corruption.

CVE-2013-2459

Integer overflow flaws were found in the way AWT processed certain input. An attacker could use these flaws to execute arbitrary code with the privileges of the user running an untrusted Java applet or application.

CVE-2013-2448, **CVE-2013-2457**, **CVE-2013-2453**

Multiple improper permission check issues were discovered in the Sound and JMX components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-2456, **CVE-2013-2447**, **CVE-2013-2455**, **CVE-2013-2452**, **CVE-2013-2443**, **CVE-2013-2446**

Multiple flaws in the Serialization, Networking, Libraries and CORBA components can be exploited by an untrusted Java application or applet to gain access to potentially sensitive information.

CVE-2013-2445

It was discovered that the Hotspot component did not properly handle out-of-memory errors. An untrusted Java application or applet could possibly use these flaws to terminate the Java Virtual Machine.

CVE-2013-2444, **CVE-2013-2450**

It was discovered that the AWT component did not properly manage certain resources and that the ObjectStreamClass of the Serialization component did not properly handle circular references. An untrusted Java application or applet could possibly use these flaws to cause a denial of service.

CVE-2013-2407, **CVE-2013-2461**

It was discovered that the Libraries component contained certain errors related to XML security and the class loader. A remote attacker could possibly exploit these flaws to bypass intended security mechanisms or disclose potentially sensitive information and cause a denial of service.

CVE-2013-2412

It was discovered that JConsole did not properly inform the user when establishing an SSL connection failed. An attacker could exploit this flaw to gain access to potentially sensitive information.

CVE-2013-1571

It was found that documentation generated by Javadoc was vulnerable to a frame injection attack. If such documentation was accessible over a network, and a remote attacker could trick a user into visiting a specially-crafted URL, it would lead to arbitrary web content being displayed next to the documentation. This could be used to perform a phishing attack by providing frame content that spoofed a login form on the site hosting the vulnerable documentation.

CVE-2013-1500

It was discovered that the 2D component created shared memory segments with insecure permissions. A local attacker could use this flaw to read or write to the shared memory segment.

Red Hat would like to thank US-CERT for reporting CVE-2013-1571, and Tim Brown for reporting CVE-2013-1500. US-CERT acknowledges Oracle as the original reporter of CVE-2013-1571.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.46.5. RHSA-2013:0274 — Important: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

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

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2013-1486

An improper permission check issue was discovered in the JMX component in OpenJDK. An untrusted Java application or applet could use this flaw to bypass Java sandbox restrictions.

CVE-2013-0169

It was discovered that OpenJDK leaked timing information when decrypting TLS/SSL protocol encrypted records when CBC-mode cipher suites were used. A remote attacker could possibly use this flaw to retrieve plain text from the encrypted packets by using a TLS/SSL server as a padding oracle.

This erratum also upgrades the OpenJDK package to IcedTea6 1.11.8. Refer to the NEWS file for further information.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.47. java-1.6.0-sun

4.47.1. RHSA-2013:0531 — Critical: java-1.6.0-sun security update

Updated java-1.6.0-sun packages that fix three security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

Oracle Java SE version 6 includes the Oracle Java Runtime Environment and the Oracle Java Software Development Kit.

Security Fix

CVE-2013-0169, **CVE-2013-1486**, **CVE-2013-1487**

This update fixes three vulnerabilities in the Oracle Java Runtime Environment and the Oracle Java Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch Update Advisory page.

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which provide Oracle Java 6 Update 41. All running instances of Oracle Java must be restarted for the update to take effect.

4.47.2. RHSA-2013:0758 — Critical: java-1.6.0-sun security update

Updated java-1.6.0-sun packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

Oracle Java SE version 6 includes the Oracle Java Runtime Environment and the Oracle Java Software Development Kit.

Security Fix

CVE-2013-0401, **CVE-2013-1491**, **CVE-2013-1518**, **CVE-2013-1537**, **CVE-2013-1540**, **CVE-2013-1557**, **CVE-2013-1558**, **CVE-2013-1563**, **CVE-2013-1569**, **CVE-2013-2383**, **CVE-2013-2384**, **CVE-2013-2394**, **CVE-2013-2417**, **CVE-2013-2418**, **CVE-2013-2419**, **CVE-2013-2420**, **CVE-2013-2422**, **CVE-2013-2424**, **CVE-2013-2429**, **CVE-2013-2430**, **CVE-2013-2432**, **CVE-2013-2433**, **CVE-2013-2435**, **CVE-2013-2439**, **CVE-2013-2440**

This update fixes several vulnerabilities in the Oracle Java Runtime Environment and the Oracle

Java Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch Update Advisory page.

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which provide Oracle Java 6 Update 45. All running instances of Oracle Java must be restarted for the update to take effect.

4.47.3. RHSA-2013:0236 — Critical: java-1.6.0-sun security update

Updated java-1.6.0-sun packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

Oracle Java SE version 6 includes the Oracle Java Runtime Environment and the Oracle Java Software Development Kit.

Security Fix

CVE-2012-1541, CVE-2012-3213, CVE-2012-3342, CVE-2013-0351, CVE-2013-0409, CVE-2013-0419, CVE-2013-0423, CVE-2013-0424, CVE-2013-0425, CVE-2013-0426, CVE-2013-0427, CVE-2013-0428, CVE-2013-0429, CVE-2013-0430, CVE-2013-0432, CVE-2013-0433, CVE-2013-0434, CVE-2013-0435, CVE-2013-0438, CVE-2013-0440, CVE-2013-0441, CVE-2013-0442, CVE-2013-0443, CVE-2013-0445, CVE-2013-0446, CVE-2013-0450, CVE-2013-1473, CVE-2013-1475, CVE-2013-1476, CVE-2013-1478, CVE-2013-1480, CVE-2013-1481

This update fixes several vulnerabilities in the Oracle Java Runtime Environment and the Oracle Java Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch Update Advisory page.

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which provide Oracle Java 6 Update 39. All running instances of Oracle Java must be restarted for the update to take effect.

4.47.4. RHSA-2013:0601 — Critical: java-1.6.0-sun security update

Updated java-1.6.0-sun packages that fix two security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

Oracle Java SE version 6 includes the Oracle Java Runtime Environment and the Oracle Java Software Development Kit.

Security Fix

CVE-2013-0809, CVE-2013-1493

This update fixes two vulnerabilities in the Oracle Java Runtime Environment and the Oracle Java Software Development Kit. Further information about these flaws can be found on the Oracle Security Alert page.

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which provide Oracle Java 6 Update 43. All running instances of Oracle Java must be restarted for the update to take effect.

4.48. java-1.7.0-ibm

4.48.1. RHSA-2013:1060 — Critical: java-1.7.0-ibm security update

Updated java-1.7.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM Java SE version 7 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

> CVE-2013-1500, CVE-2013-1571, CVE-2013-2400, CVE-2013-2407, CVE-2013-2412, CVE-2013-2437, CVE-2013-2442, CVE-2013-2444, CVE-2013-2446, CVE-2013-2447, CVE-2013-2448, CVE-2013-2449, CVE-2013-2450, CVE-2013-2451, CVE-2013-2452, CVE-2013-2453, CVE-2013-2454, CVE-2013-2455, CVE-2013-2456, CVE-2013-2457, CVE-2013-2458, CVE-2013-2459, CVE-2013-2460, CVE-2013-2462, CVE-2013-2463, CVE-2013-2464, CVE-2013-2465, CVE-2013-2466, CVE-2013-2468, CVE-2013-2469, CVE-2013-2470, CVE-2013-2471, CVE-2013-2472, CVE-2013-2473, CVE-2013-3744
>
> This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

Red Hat would like to thank Tim Brown for reporting CVE-2013-1500, and US-CERT for reporting CVE-2013-1571. US-CERT acknowledges Oracle as the original reporter of CVE-2013-1571.

All users of java-1.7.0-ibm are advised to upgrade to these updated packages, containing the IBM Java SE 7 SR5 release. All running instances of IBM Java must be restarted for the update to take effect.

4.48.2. RHSA-2013:0626 — Critical: java-1.7.0-ibm security update

Updated java-1.7.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM Java SE version 7 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

> CVE-2012-1541, CVE-2012-3174, CVE-2012-3213, CVE-2012-3342, CVE-2013-0351, CVE-2013-0409, CVE-2013-0419, CVE-2013-0422, CVE-2013-0423, CVE-2013-0424, CVE-2013-0425, CVE-2013-0426, CVE-2013-0427, CVE-2013-0428, CVE-2013-0431, CVE-2013-0432, CVE-2013-0433, CVE-2013-0434, CVE-2013-0435, CVE-2013-0437, CVE-2013-0438, CVE-2013-0440, CVE-2013-0441, CVE-2013-0442, CVE-2013-0443, CVE-2013-0444, CVE-2013-0445, CVE-2013-0446, CVE-2013-0449, CVE-2013-0450, CVE-2013-0809, CVE-2013-1473, CVE-2013-1476, CVE-2013-1478, CVE-2013-1480, CVE-2013-1484, CVE-2013-1485, CVE-2013-1486, CVE-2013-1487, CVE-2013-1493

This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.7.0-ibm are advised to upgrade to these updated packages, containing the IBM Java SE 7 SR4 release. All running instances of IBM Java must be restarted for the update to take effect.

4.48.3. RHSA-2013:0822 — Critical: java-1.7.0-ibm security update

Updated java-1.7.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM Java SE version 7 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

CVE-2013-0169, CVE-2013-0401, CVE-2013-1488, CVE-2013-1491, CVE-2013-1537, CVE-2013-1540, CVE-2013-1557, CVE-2013-1558, CVE-2013-1563, CVE-2013-1569, CVE-2013-2383, CVE-2013-2384, CVE-2013-2394, CVE-2013-2415, CVE-2013-2416, CVE-2013-2417, CVE-2013-2418, CVE-2013-2419, CVE-2013-2420, CVE-2013-2422, CVE-2013-2423, CVE-2013-2424, CVE-2013-2426, CVE-2013-2429, CVE-2013-2430, CVE-2013-2432, CVE-2013-2433, CVE-2013-2434, CVE-2013-2435, CVE-2013-2436, CVE-2013-2438, CVE-2013-2440

This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.7.0-ibm are advised to upgrade to these updated packages, containing the IBM Java SE 7 SR4-FP2 release. All running instances of IBM Java must be restarted for the update to take effect.

4.49. java-1.7.0-openjdk

4.49.1. RHSA-2013:0247 — Important: java-1.7.0-openjdk security update

Updated java-1.7.0-openjdk packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

These packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Software Development Kit.

Security Fixes

CVE-2013-0442, CVE-2013-0445, CVE-2013-0441, CVE-2013-1475, CVE-2013-1476, CVE-2013-0429, CVE-2013-0450, CVE-2013-0425, CVE-2013-0426, CVE-2013-0428, CVE-2013-0444

Multiple improper permission check issues were discovered in the AWT, CORBA, JMX, Libraries, and Beans components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-1478, **CVE-2013-1480**

Multiple flaws were found in the way image parsers in the 2D and AWT components handled image raster parameters. A specially-crafted image could cause Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with the virtual machine privileges.

CVE-2013-0432

A flaw was found in the AWT component's clipboard handling code. An untrusted Java application or applet could use this flaw to access clipboard data, bypassing Java sandbox restrictions.

CVE-2013-0435

The default Java security properties configuration did not restrict access to certain com.sun.xml.internal packages. An untrusted Java application or applet could use this flaw to access information, bypassing certain Java sandbox restrictions. This update lists the whole package as restricted.

CVE-2013-0431, **CVE-2013-0427**, **CVE-2013-0433**, **CVE-2013-0434**

Multiple improper permission check issues were discovered in the JMX, Libraries, Networking, and JAXP components. An untrusted Java application or applet could use these flaws to bypass certain Java sandbox restrictions.

CVE-2013-0424

It was discovered that the RMI component's CGIHandler class used user inputs in error messages without any sanitization. An attacker could use this flaw to perform a cross-site scripting (XSS) attack.

CVE-2013-0440

It was discovered that the SSL/TLS implementation in the JSSE component did not properly enforce handshake message ordering, allowing an unlimited number of handshake restarts. A remote attacker could use this flaw to make an SSL/TLS server using JSSE consume an excessive amount of CPU by continuously restarting the handshake.

CVE-2013-0443

It was discovered that the JSSE component did not properly validate Diffie-Hellman public keys. An SSL/TLS client could possibly use this flaw to perform a small subgroup attack.

This erratum also upgrades the OpenJDK package to IcedTea7 2.3.5. Refer to the NEWS file for further information.

All users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.49.2. RHSA-2013:0275 — Important: java-1.7.0-openjdk security update

Updated java-1.7.0-openjdk packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

These packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Software Development Kit.

Security Fixes

CVE-2013-1486, **CVE-2013-1484**

Multiple improper permission check issues were discovered in the JMX and Libraries components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-1485

An improper permission check issue was discovered in the Libraries component in OpenJDK. An untrusted Java application or applet could use this flaw to bypass certain Java sandbox restrictions.

CVE-2013-0169

It was discovered that OpenJDK leaked timing information when decrypting TLS/SSL protocol encrypted records when CBC-mode cipher suites were used. A remote attacker could possibly use this flaw to retrieve plain text from the encrypted packets by using a TLS/SSL server as a padding oracle.

This erratum also upgrades the OpenJDK package to IcedTea7 2.3.7. Refer to the NEWS file for further information.

All users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.49.3. RHSA-2013:0958 — Important: java-1.7.0-openjdk security update

Updated java-1.7.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 5.

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

These packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Software Development Kit.

Security Fixes

CVE-2013-2470, **CVE-2013-2471**, **CVE-2013-2472**, **CVE-2013-2473**, **CVE-2013-2463**, **CVE-2013-2465**, **CVE-2013-2469**

Multiple flaws were discovered in the ImagingLib and the image attribute, channel, layout and raster processing in the 2D component. An untrusted Java application or applet could possibly use these flaws to trigger Java Virtual Machine memory corruption.

CVE-2013-2459

Integer overflow flaws were found in the way AWT processed certain input. An attacker could use these flaws to execute arbitrary code with the privileges of the user running an untrusted Java applet or application.

CVE-2013-2448, **CVE-2013-2454**, **CVE-2013-2458**, **CVE-2013-2457**, **CVE-2013-2453**, **CVE-2013-2460**

Multiple improper permission check issues were discovered in the Sound, JDBC, Libraries, JMX, and Serviceability components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-2456, **CVE-2013-2447**, **CVE-2013-2455**, **CVE-2013-2452**, **CVE-2013-2443**, **CVE-2013-2446**

Multiple flaws in the Serialization, Networking, Libraries and CORBA components can be exploited by an untrusted Java application or applet to gain access to potentially sensitive information.

CVE-2013-2445

It was discovered that the Hotspot component did not properly handle out-of-memory errors. An untrusted Java application or applet could possibly use these flaws to terminate the Java Virtual Machine.

CVE-2013-2444, **CVE-2013-2450**

It was discovered that the AWT component did not properly manage certain resources and that the ObjectStreamClass of the Serialization component did not properly handle circular references. An untrusted Java application or applet could possibly use these flaws to cause a denial of service.

CVE-2013-2407, **CVE-2013-2461**

It was discovered that the Libraries component contained certain errors related to XML security and the class loader. A remote attacker could possibly exploit these flaws to bypass intended security mechanisms or disclose potentially sensitive information and cause a denial of service.

CVE-2013-2412

It was discovered that JConsole did not properly inform the user when establishing an SSL connection failed. An attacker could exploit this flaw to gain access to potentially sensitive information.

CVE-2013-2449

It was discovered that GnomeFileTypeDetector did not check for read permissions when accessing files. An untrusted Java application or applet could possibly use this flaw to disclose potentially sensitive information.

CVE-2013-1571

It was found that documentation generated by Javadoc was vulnerable to a frame injection attack. If such documentation was accessible over a network, and a remote attacker could trick a user into visiting a specially-crafted URL, it would lead to arbitrary web content being displayed next to the documentation. This could be used to perform a phishing attack by providing frame content that spoofed a login form on the site hosting the vulnerable documentation.

CVE-2013-1500

It was discovered that the 2D component created shared memory segments with insecure permissions. A local attacker could use this flaw to read or write to the shared memory segment.

Red Hat would like to thank Tim Brown for reporting CVE-2013-1500, and US-CERT for reporting CVE-2013-1571. US-CERT acknowledges Oracle as the original reporter of CVE-2013-1571.

This erratum also upgrades the OpenJDK package to IcedTea7 2.3.10. Refer to the NEWS file for further information.

All users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.49.4. RHBA-2013:1005 — java-1.7.0-openjdk bug fix update

Updated java-1.7.0-openjdk packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The java-1.7.0-openjdk packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Java Software Development Kit.

The java-1.7.0-openjdk packages have been upgraded to upstream version 2.3.10, which fixes these bugs:

- Previously, GlassFish 4 failed to start with the following message:

```
Caused by: java.util.MissingResourceException: Can't find
com.sun.enterprise.util.LogMessages bundle
```

- Picketlink on JBoss AS 7.1 failed to create SAML assertions for user names containing the vertical bar (|) symbol due to an incorrect library path. The path for the JDK image has been corrected and the problem no longer occurs.
- After application server restart on servers that were using SOAP messaging, the initialization of the service consumer failed with an ExceptionInInitializerError.
- When running GRails applications, the applications failed with a ClassNotFoundException due to an incorrect library path. (BZ#978441)

All users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which fix these bugs.

4.49.5. RHSA-2013:0603 — Important: java-1.7.0-openjdk security update

Updated java-1.7.0-openjdk packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

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

These packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Software Development Kit.

Security Fixes

CVE-2013-0809

An integer overflow flaw was found in the way the 2D component handled certain sample model instances. A specially-crafted sample model instance could cause Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with virtual machine privileges.

CVE-2013-1493

It was discovered that the 2D component did not properly reject certain malformed images. Specially-crafted raster parameters could cause Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with virtual machine privileges.

This erratum also upgrades the OpenJDK package to IcedTea7 2.3.8. Refer to the NEWS file for further information.

All users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.49.6. RHSA-2013:0165 — Important: java-1.7.0-openjdk security update

Updated java-1.7.0-openjdk packages that fix two security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

These packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Software Development Kit.

Security Fix

CVE-2012-3174, **CVE-2013-0422**

Two improper permission check issues were discovered in the reflection API in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

This erratum also upgrades the OpenJDK package to IcedTea7 2.3.4. Refer to the NEWS file for further information.

All users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.49.7. RHSA-2013:0752 — Important: java-1.7.0-openjdk security update

Updated java-1.7.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 5.

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

These packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Software Development Kit.

Security Fixes

CVE-2013-1569, **CVE-2013-2383**, **CVE-2013-2384**

Multiple flaws were discovered in the font layout engine in the 2D component. An untrusted Java application or applet could possibly use these flaws to trigger Java Virtual Machine memory corruption.

CVE-2013-1558, **CVE-2013-2422**, **CVE-2013-2436**, **CVE-2013-1518**, **CVE-2013-1557**

Multiple improper permission check issues were discovered in the Beans, Libraries, JAXP, and RMI components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-1537

The previous default value of the java.rmi.server.useCodebaseOnly property permitted the RMI implementation to automatically load classes from remotely specified locations. An attacker able to connect to an application using RMI could use this flaw to make the application execute arbitrary code.

CVE-2013-2420

Note: The fix for CVE-2013-1537 changes the default value of the property to true, restricting class loading to the local CLASSPATH and locations specified in the java.rmi.server.codebase property. Refer to Red Hat Bugzilla bug 952387 for additional details.

The 2D component did not properly process certain images. An untrusted Java application or applet could possibly use this flaw to trigger Java Virtual Machine memory corruption.

CVE-2013-2431, **CVE-2013-2421**, **CVE-2013-2423**

It was discovered that the Hotspot component did not properly handle certain intrinsic frames, and did not correctly perform access checks and MethodHandle lookups. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-2429, **CVE-2013-2430**

It was discovered that JPEGImageReader and JPEGImageWriter in the ImageIO component did not protect against modification of their state while performing certain native code operations. An untrusted Java application or applet could possibly use these flaws to trigger Java Virtual Machine memory corruption.

CVE-2013-1488, **CVE-2013-2426**

The JDBC driver manager could incorrectly call the toString() method in JDBC drivers, and the ConcurrentHashMap class could incorrectly call the defaultReadObject() method. An untrusted Java application or applet could possibly use these flaws to bypass Java sandbox restrictions.

CVE-2013-0401

The sun.awt.datatransfer.ClassLoaderObjectInputStream class may incorrectly invoke the system class loader. An untrusted Java application or applet could possibly use this flaw to bypass certain Java sandbox restrictions.

CVE-2013-2417, **CVE-2013-2419**

Flaws were discovered in the Network component's InetAddress serialization, and the 2D component's font handling. An untrusted Java application or applet could possibly use these flaws to crash the Java Virtual Machine.

CVE-2013-2424

The MBeanInstantiator class implementation in the OpenJDK JMX component did not properly check class access before creating new instances. An untrusted Java application or applet could use this flaw to create instances of non-public classes.

CVE-2013-2415

It was discovered that JAX-WS could possibly create temporary files with insecure permissions. A local attacker could use this flaw to access temporary files created by an application using JAX-WS.

This erratum also upgrades the OpenJDK package to IcedTea7 2.3.9. Refer to the NEWS file for further information.

All users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

4.50. java-1.7.0-oracle

4.50.1. RHSA-2013:0963 — Critical: java-1.7.0-oracle security update

Updated java-1.7.0-oracle packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

Oracle Java SE version 7 includes the Oracle Java Runtime Environment and the Oracle Java Software Development Kit.

Security Fix

CVE-2013-1500, CVE-2013-1571, CVE-2013-2400, CVE-2013-2407, CVE-2013-2412, CVE-2013-2437, CVE-2013-2442, CVE-2013-2443, CVE-2013-2444, CVE-2013-2445, CVE-2013-2446, CVE-2013-2447, CVE-2013-2448, CVE-2013-2449, CVE-2013-2450, CVE-2013-2451, CVE-2013-2452, CVE-2013-2453, CVE-2013-2454, CVE-2013-2455, CVE-2013-2456, CVE-2013-2457, CVE-2013-2458, CVE-2013-2459, CVE-2013-2460, CVE-2013-2461, CVE-2013-2462, CVE-2013-2463, CVE-2013-2464, CVE-2013-2465, CVE-2013-2466, CVE-2013-2468, CVE-2013-2469, CVE-2013-2470, CVE-2013-2471, CVE-2013-2472, CVE-2013-2473, CVE-2013-3744

This update fixes several vulnerabilities in the Oracle Java Runtime Environment and the Oracle Java Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch Update Advisory page.

Red Hat would like to thank Tim Brown for reporting CVE-2013-1500, and US-CERT for reporting CVE-2013-1571. US-CERT acknowledges Oracle as the original reporter of CVE-2013-1571.

All users of java-1.7.0-oracle are advised to upgrade to these updated packages, which provide Oracle Java 7 Update 25 and resolve these issues. All running instances of Oracle Java must be restarted for the update to take effect.

4.50.2. RHSA-2013:0600 — Critical: java-1.7.0-oracle security update

Updated java-1.7.0-oracle packages that fix two security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

Oracle Java SE version 7 includes the Oracle Java Runtime Environment and the Oracle Java Software Development Kit.

Security Fix

CVE-2013-0809, CVE-2013-1493

This update fixes two vulnerabilities in the Oracle Java Runtime Environment and the Oracle Java Software Development Kit. Further information about these flaws can be found on the Oracle Security Alert page.

All users of java-1.7.0-oracle are advised to upgrade to these updated packages, which provide Oracle Java 7 Update 17 and resolve these issues. All running instances of Oracle Java must be restarted for the update to take effect.

4.50.3. RHSA-2013:0757 — Critical: java-1.7.0-oracle security update

Updated java-1.7.0-oracle packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

Oracle Java SE version 7 includes the Oracle Java Runtime Environment and the Oracle Java Software Development Kit.

Security Fix

CVE-2013-0401, CVE-2013-0402, CVE-2013-1488, CVE-2013-1491, CVE-2013-1518, CVE-2013-1537, CVE-2013-1540, CVE-2013-1557, CVE-2013-1558, CVE-2013-1561, CVE-2013-1563, CVE-2013-1564, CVE-2013-1569, CVE-2013-2383, CVE-2013-2384, CVE-2013-2394, CVE-2013-2414, CVE-2013-2415, CVE-2013-2416, CVE-2013-2417, CVE-2013-2418, CVE-2013-2419, CVE-2013-2420, CVE-2013-2421, CVE-2013-2422, CVE-2013-2423, CVE-2013-2424, CVE-2013-2425, CVE-2013-2426, CVE-2013-2427, CVE-2013-2428, CVE-2013-2429, CVE-2013-2430, CVE-2013-2431, CVE-2013-2432, CVE-2013-2433, CVE-2013-2434, CVE-2013-2435, CVE-2013-2436, CVE-2013-2438, CVE-2013-2439, CVE-2013-2440

> This update fixes several vulnerabilities in the Oracle Java Runtime Environment and the Oracle Java Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch Update Advisory page.

All users of java-1.7.0-oracle are advised to upgrade to these updated packages, which provide Oracle Java 7 Update 21 and resolve these issues. All running instances of Oracle Java must be restarted for the update to take effect.

4.50.4. RHSA-2013:0237 — Critical: java-1.7.0-oracle security update

Updated java-1.7.0-oracle packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

Oracle Java SE version 7 includes the Oracle Java Runtime Environment and the Oracle Java Software Development Kit.

Security Fix

CVE-2012-1541, CVE-2012-3213, CVE-2012-3342, CVE-2013-0351, CVE-2013-0409, CVE-2013-0419, CVE-2013-0423, CVE-2013-0424, CVE-2013-0425, CVE-2013-0426, CVE-2013-0427, CVE-2013-0428, CVE-2013-0429, CVE-2013-0430, CVE-2013-0431, CVE-2013-0432, CVE-2013-0433, CVE-2013-0434, CVE-2013-0435, CVE-2013-0437, CVE-2013-0438, CVE-2013-0440, CVE-2013-0441, CVE-2013-0442, CVE-2013-0443, CVE-2013-0444, CVE-2013-0445, CVE-2013-0446, CVE-2013-0448, CVE-2013-0449, CVE-2013-0450, CVE-2013-1473, CVE-2013-1475, CVE-2013-1476, CVE-2013-1478, CVE-2013-1479, CVE-2013-1480, CVE-2013-1489

> This update fixes several vulnerabilities in the Oracle Java Runtime Environment and the Oracle Java Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch Update Advisory page.

All users of java-1.7.0-oracle are advised to upgrade to these updated packages, which provide Oracle Java 7 Update 13 and resolve these issues. All running instances of Oracle Java must be restarted for the update

to take effect.

4.50.5. RHSA-2013:0156 — Critical: java-1.7.0-oracle security update

Updated java-1.7.0-oracle packages that fix two security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

Oracle Java SE version 7 includes the Oracle Java Runtime Environment and the Oracle Java Software Development Kit.

Security Fix

CVE-2012-3174, **CVE-2013-0422**

This update fixes two vulnerabilities in the Oracle Java Runtime Environment and the Oracle Java Software Development Kit. Further information about these flaws can be found on the Oracle Security Alert page.

Red Hat is aware that a public exploit for CVE-2013-0422 is available that executes code without user interaction when a user visits a malicious web page using a browser with the Oracle Java 7 web browser plug in enabled.

All users of java-1.7.0-oracle are advised to upgrade to these updated packages, which provide Oracle Java 7 Update 11 and resolve these issues. All running instances of Oracle Java must be restarted for the update to take effect.

4.50.6. RHSA-2013:0532 — Critical: java-1.7.0-oracle security update

Updated java-1.7.0-oracle packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

Oracle Java SE version 7 includes the Oracle Java Runtime Environment and the Oracle Java Software Development Kit.

Security Fix

CVE-2013-0169, **CVE-2013-1484**, **CVE-2013-1485**, **CVE-2013-1486**, **CVE-2013-1487**

This update fixes several vulnerabilities in the Oracle Java Runtime Environment and the Oracle Java Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch Update Advisory page.

All users of java-1.7.0-oracle are advised to upgrade to these updated packages, which provide Oracle Java 7 Update 15 and resolve these issues. All running instances of Oracle Java must be restarted for the update to take effect.

4.51. kernel

4.51.1. RHSA-2014:0285 — Important: kernel security, bug fix, and enhancement update

Updated *kernel* packages that fix multiple security issues, several bugs, and add one enhancement are now available for Red Hat Enterprise Linux 5.

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

The *kernel* packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2013-6381, Important

A buffer overflow flaw was found in the way the qeth_snmp_command() function in the Linux kernel's QETH network device driver implementation handled SNMP IOCTL requests with an out-of-bounds length. A local, unprivileged user could use this flaw to crash the system or, potentially, escalate their privileges on the system.

CVE-2013-4483, 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-2013-4554, Moderate

It was found that the Xen hypervisor implementation did not correctly check privileges of hypercall attempts made by HVM guests, allowing hypercalls to be invoked from protection rings 1 and 2 in addition to ring 0. A local attacker in an HVM guest able to execute code on privilege levels 1 and 2 could potentially use this flaw to further escalate their privileges in that guest. Note: Xen HVM guests running unmodified versions of Red Hat Enterprise Linux and Microsoft Windows are not affected by this issue because they are known to only use protection rings 0 (kernel) and 3 (userspace).

CVE-2013-6383, Moderate

A flaw was found in the way the Linux kernel's Adaptec RAID controller (aacraid) checked permissions of compat IOCTLs. A local attacker could use this flaw to bypass intended security restrictions.

CVE-2013-6885, Moderate

It was found that, under specific circumstances, a combination of write operations to write-combined memory and locked CPU instructions may cause a core hang on certain AMD CPUs (for more information, refer to AMD CPU erratum 793 linked in the References section). A privileged user in a guest running under the Xen hypervisor could use this flaw to cause a denial of service on the host system. This update adds a workaround to the Xen hypervisor implementation, which mitigates the AMD CPU issue. Note: this issue only affects AMD Family 16h Models 00h-0Fh Processors. Non-AMD CPUs are not vulnerable.

CVE-2013-7263, Low

It was found that certain protocol handlers in the Linux kernel's networking implementation could set the addr_len value without initializing the associated data structure. A local, unprivileged user could use this flaw to leak kernel stack memory to user space using the recvmsg, recvfrom, and recvmmsg system calls.

CVE-2013-2929, Low

A flaw was found in the way the get_dumpable() function return value was interpreted in the ptrace subsystem of the Linux kernel. When 'fs.suid_dumpable' was set to 2, a local, unprivileged local user could use this flaw to bypass intended ptrace restrictions and obtain potentially sensitive information.

Red Hat would like to thank Vladimir Davydov of Parallels for reporting CVE-2013-4483 and the Xen project for reporting CVE-2013-4554 and CVE-2013-6885. Upstream acknowledges Jan Beulich as the original reporter of CVE-2013-4554 and CVE-2013-6885.

Bug Fixes

BZ#1044328

Due to a bug in the cifs module, the calculation of the number of virtual circuits was handled incorrectly when establishing SMB sessions. As a consequence in environments with multiple TCP connections between the same SMB client and SMB server, each time a TCP connection was established, all other TCP connections from the client to the server were reset, resulting in an endless loop. With this update, the number of virtual circuits is constantly set to 1, which ensures the correct behavior of the cifs module in this situation.

BZ#1050097

Certain storage device or storage environment failures could cause all SCSI commands and task management functions that were sent to a SCSI target to time out, without any other indication of an error. As a consequence, the Linux SCSI error handling code stopped issuing any I/O operations on the entire HBA adapter until the recovery operations completed. Additionally when using DM Multipath, I/O operations did not fail over to a working path in this situation. To resolve this problem, a new sysfs parameter, "eh_deadline", has been added to the SCSI host object. This parameter allows to set the maximum amount of time for which the SCSI error handling attempts to perform error recovery before resetting the entire HBA adapter. This timeout is disabled by default. The default value of this timeout can be reset for all SCSI HBA adapters on the system using the "eh_deadline" kernel parameter. The described scenario no longer occurs if eh_deadline is properly used.

BZ#1051535

A previous change that corrected a bug preventing communication between NICs using be2net introduced a memory leak in the be2net transmitter (Tx) code path. The memory leak has been fixed by applying a series of patches that corrects handling of socket buffers (SKBs) in the Tx code path.

Enhancement

BZ#1054055

Support for a kernel symbol that allows printing a binary blob of data as a hex dump to syslog has been added to kABI (Kernel Application Binary Interface).

All *kernel* users are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement. The system must be rebooted for this update to take effect.

4.51.2. RHSA-2013:1348 — Moderate: Red Hat Enterprise Linux 5 kernel update

Updated *kernel* packages that fix one security issue, several bugs, and add multiple enhancements are now available as part of the ongoing support and maintenance of Red Hat Enterprise Linux version 5. This is the tenth regular update.

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

The *kernel* packages contain the Linux kernel, the core of any Linux operating system.

Security Fix

CVE-2012-4398, Moderate

It was found that a deadlock could occur in the Out of Memory (OOM) killer. A process could trigger this deadlock by consuming a large amount of memory, and then causing request_module() to be called. A local, unprivileged user could use this flaw to cause a denial of service (excessive memory consumption).

Red Hat would like to thank Tetsuo Handa for reporting this issue.

Bug Fixes

BZ#995961

A recent patch fixing a problem that prevented communication between NICs using the be2net driver caused the firmware of NICs to become unresponsive, and thus triggered a kernel panic. The problem was caused by unnecessary usage of a hardware workaround that allows skipping VLAN tag insertion. A patch has been applied and the workaround is now used only when the multi-channel configuration is enabled on the NIC. Note that the bug only affected the NICs with firmware version 4.2.xxxx.

BZ#987539

A race condition in the be_open function in the be2net driver could trigger the BUG_ON() macro, which resulted in a kernel panic. A patch addressing this problem has been applied and the race condition is now avoided by enabling polling before enabling interrupts globally. The kernel no longer panics in this situation.

BZ#987244, BZ#978305

Due to a segment register that was not reset after transition to protected mode, a bug could have been triggered in certain older versions of the upstream kernel (the kernel 3.9 - 3.9.4), preventing a guest system from booting and rendering it unresponsive on certain Intel Virtualization Technology (VT) hardware. On the newer kernels, this behavior had a significant impact on the booting speed of virtual machines. This update applies a patch providing early segment setup for the VT feature which allows executing VT under WMware and KVM. Guest machines no longer hang on boot and booting process is now significantly faster when using 64-bit Intel hardware with the VT feature enabled.

BZ#981337

Due to a bug in the networking stack, the kernel could attempt to deference a NULL pointer if a VLAN was configured on top of a GRE tunnel and network packets were transmitted, which resulted in a kernel panic. A patch has been applied to fix this bug by modifying the net driver to test a VLAN hardware header for a NULL value properly. The kernel no longer panics in this scenario.

BZ#967053

A kernel panic could occur in the XEN hypervisor due to a race in the XEN's tracing infrastructure. The race allows an idle vCPU to attempt to log a trace record while another vCPU executes a hypercall to disable the active tracing: for example, when using the xenmon.py performance

monitoring utility. To avoid triggering the panic, the respective BUG_ON() routine call in the trace code has been replaced with a simple test condition. The XEN hypervisor no longer crashes due to aforementioned race condition.

BZ#965359

Due to a bug in memory management, a kernel thread process could become unresponsive for a significant amount of time, waiting for a quota of dirty pages to be met and written out, which caused a kernel panic. With this update, memory management allows processes to break out of the throttle loop if there are no more dirty pages available to be written out. This prevents a kernel panic from occurring in this situation.

BZ#957604

A previous change in the port auto-selection code allowed sharing ports with no conflicts extending its usage. Consequently, when binding a socket with the SO_REUSEADDR socket option enabled, the bind(2) function could allocate an ephemeral port that was already used. A subsequent connection attempt failed in such a case with the EADDRNOTAVAIL error code. This update applies a patch that modifies the port auto-selection code so that bind(2) now selects a non-conflict port even with the SO_REUSEADDR option enabled.

BZ#950137

Due to a bug in the be2net driver, events in the RX, TX, and MCC queues were not acknowledged before closing the respective queue. This could cause unpredictable behavior when creating RX rings during the subsequent queue opening. This update applies a patch that corrects this problem and events are now acknowledged as expected in this scenario.

BZ#948317

Incorrect locking around the cl_state_owners list could cause the NFSv4 state reclaimer thread to enter an infinite loop while holding the Big Kernel Lock (BLK). This consequently caused the NFS client to become unresponsive. With this update, safe list iteration is used, which prevents the client from hanging in this scenario.

BZ#947732

When handling requests from Intelligent Platform Management Interface (IPMI) clients, the IPMI driver previously used two different locks for an IPMI request. If two IPMI clients sent their requests at the same time, each request could receive one of the locks and then wait for the second lock to become available. This resulted in a deadlock situation and the system became unresponsive. The problem could occur more likely in environments with many IPMI clients. This update modifies the IPMI driver to handle the received messages using tasklets so the driver now uses a safe locking technique when handling IPMI requests and the mentioned deadlock can no longer occur.

BZ#928098

A bug in the autofs4 mount expiration code could cause the autofs4 module to falsely report a busy tree of NFS mounts as "not in use". Consequently, automount attempted to unmount the tree and failed with a "failed to umount offset" error, leaving the mount tree to appear as empty directories. A patch has been applied to remove an incorrectly used autofs dentry mount check and the aforementioned problem no longer occurs.

BZ#924011

Previously, the xdr routines in NFS version 2 and 3 conditionally updated the res->count variable. Read retry attempts after a short NFS read() call could fail to update the res->count variable, resulting in truncated read data being returned. With this update, the res->count variable is updated unconditionally, thus preventing this bug.

BZ#918592

Previously, the NFS Lock Manager (NLM) did not resend blocking lock requests after NFSv3 server reboot recovery. As a consequence, when an application was running on a NFSv3 mount and requested a blocking lock, the application received an -ENOLCK error. This patch ensures that NLM always resend blocking lock requests after the grace period has expired.

BZ#907524

Previously, the be2net code expected the last word of an MCC completion message from the firmware to be transferred by direct memory access (DMA) at once. However, this is not always true, and could therefore cause the BUG_ON() macro to be triggered in the be_mcc_compl_is_new() function, consequently leading to a kernel panic. The BUG_ON() macro has been removed, and a kernel panic no longer occurs in this scenario.

BZ#906909

When a process is opening a file over NFSv4, sometimes an OPEN call can succeed while the following GETATTR operation fails with an NFS4ERR_DELAY error. The NFSv4 code did not handle such a situation correctly and allowed an NFSv4 client to attempt to use the buffer that should contain the GETATTR information. However, the buffer did not contain the valid GETATTR information, which caused the client to return a "-ENOTDIR" error. Consequently, the process failed to open the requested file. This update backports a patch that adds a test condition verifying validity of the GETATTR information. If the GETATTR information is invalid, it is obtained later and the process opens the requested file as expected.

BZ#905190

The IPv4 code did not correctly update the Maximum Transfer Unit (MTU) of the designed interface when receiving ICMP Fragmentation Needed packets. Consequently, a remote host did not respond correctly to ping attempts. With this update, the IPv4 code has been modified so the MTU of the designed interface is adjusted as expected in this situation. The ping command now provides the expected output.

BZ#901547

The size of the buffer used to print the kernel taint output on kernel panic was too small, which resulted in the kernel taint output not being printed completely sometimes. With this update, the size of the buffer has been adjusted and the kernel taint output is now displayed properly.

BZ#894636

Previously, the Generic Receive Offload (GRO) functionality was not enabled by default for VLAN devices. Consequently, certain network adapters, such as Emulex Virtual Fabric Adapter (VFA) II, that use be2net driver, were dropping packets when VLAN tagging was enabled and the 8021q kernel module loaded. This update applies a patch that enables GRO by default for VLAN devices.

BZ#885125

Certain recent Intel input/output memory management unit (IOMMU) systems reported very large numbers of supported mapping domains. Consequently, if the number was too large, booting a system with the intel_iommu kernel parameter enabled (intel_iommu=on) failed with the following error message:

```
Allocating domain array failed.
```

With this update, a limit of 4000 domains is set to avoid the described problems.

BZ#881885

Previously, the Xen kernel used the memory size found at the "0x40e" address as the beginning of the Extended BIOS Data Area (EBDA). However, this is not valid on certain machines, such as Dell PowerEdge R710, which caused the system to become unresponsive during boot on these machines. This update modifies the kernel to use the multiboot structure to acquire the correct location of EBDA and the system boot now proceeds as expected in this scenario.

BZ#878316

Previously, race conditions could sometimes occur in interrupt handling on the Emulex BladeEngine 2 (BE2) controllers, causing the network adapter to become unresponsive. This update provides a series of patches for the be2net driver, which prevents the race from occurring. The network cards using BE2 chipsets no longer hang due to incorrectly handled interrupt events.

BZ#878209

Due to a regression introduced by a recent update of the be2net driver, 10Gb NICs configured to use multiple receive queues across multiple CPUs were restricted to use a single receive queue on a single CPU. This resulted in significant performance degradation. With this update, the be2net driver has been corrected to provide support for multiple receive queues on 10Gb NICs as expected.

BZ#877474

A previous change in the tg3 driver corrected a bug causing DMA read engine of the Broadcom BCM5717 Ethernet controller to initiate multiple DMA reads across the PCIe bus. However, the original bug fix used the CHIPREV_ID_5717_A0 macro which is more restrictive so that the DMA read problem was not fixed for the Broadcom BCM5718 Ethernet controller. This update modifies the code to use the ASIC_REV_5717 macro, which corrects the original bug properly.

BZ#876587

The code to print the kernel taint output contained a typographical error. Consequently, the kernel taint output, which is displayed on kernel panic, could not provide taint error messages for unsupported hardware. This update fixes the typo and the kernel taint output is now displayed correctly.

BZ#872531

The cxgb4 driver previously did not clear data structures used for firmware requests. Consequently, when initializing some Chelsio's Terminator 4 (T4) adapters, a probe request could fail because the request was incompatible with the adapter's firmware. This update modifies the cxgb4 driver to properly initialize firmware request structures before sending a request to the firmware and the problem no longer occurs.

BZ#865095

The memory management code specific to the AMD64 and Intel 64 architectures previously did not contain proper memory barriers in the smp_invalidate_interrupt() routine. As a consequence, CPUs on AMD64 and Intel 64 systems containing modulo 8 number of CPUs (8, 16, 24 and so on) could sometimes heavily compete for spinlock resources, spending most of the CPU time by attempts to acquire spinlocks. Such systems could therefore rarely appear to be unresponsive with a very slow computing progress. This update applies a patch introducing proper memory barriers in the smp_invalidate_interrupt() routine so the problem can no longer occur.

BZ#864648

Previously, the kernel's futex wait code used timeouts that had granularity in milliseconds. Also, when passing these timeouts to system calls, the kernel converted the timeouts to "jiffies". Consequently, programs could time out inaccurately which could lead to significant latency

problems in certain environments. This update modifies the futex wait code to use a high-resolution timer (hrtimer) so the timeout granularity is now in microseconds. Timeouts are no longer converted to "jiffies" when passed to system calls. Timeouts passed to programs are now accurate and the programs time out as expected.

BZ#862865

A boot-time memory allocation pool (the DMI heap) is used to keep the list of Desktop Management Interface (DMI) devices during the system boot. Previously, the size of the DMI heap was only 2048 bytes on the AMD64 and Intel 64 architectures and the DMI heap space could become easily depleted on some systems, such as the IBM System x3500 M2. A subsequent OOM failure could, under certain circumstances, lead to a NULL pointer entry being stored in the DMI device list. Consequently, scanning of such a corrupted DMI device list resulted in a kernel panic. The boot-time memory allocation pool for the AMD64 and Intel 64 architectures has been enlarged to 4096 bytes and the routines responsible for populating the DMI device list have been modified to skip entries if their name string is NULL. The kernel no longer panics in this scenario.

BZ#862520

Due to a bug in the be2net driver, the receive completion queue (RX CQ) could report completions with an incorrect fragment ID (frag_idx). This triggered a BUG_ON() macro that resulted in a kernel panic. A patch has been applied to the be2net driver ensuring that partially coalesced CQ entries are properly flushed when completion coalescing is enabled on a CQ. The kernel no longer panics in this situation.

BZ#859194

The generic allocator (genalloc) could, under certain circumstances, incorrectly allocate memory for the gen_pool structure. This could result in memory corruption where genalloc attempted to set the bits it had not allocated. A patch has been applied that ensures proper byte allocation and the memory corruption problem no longer occurs when allocating a generic memory pool.

BZ#853145

Previously, an NFS client could sometimes cache negative dentries until the page cache was flushed or the directory listing operation was performed on the parent directory. As a consequence, an incorrect dentry was never normally revalidated and a stat call always failed, providing incorrect results. This was caused by an incorrect resolution of an attribute indicating a cache change (cache_change_attribute) along with insufficient flushing of cached directories. A series of patches has been backported to resolve this problem so the cache_change_attribute is now updated properly and the cached directories are flushed more readily.

BZ#845447

Previously, when hot-unplugging a USB serial adapter device, the USB serial driver did not properly clean up used serial ports. Therefore, when hot-plugging the USB serial device again, the USB serial driver allocated new port IDs instead of using previously used ports. This update modifies the USB serial driver to clean up open ports correctly so that the ports can be reused next time the device is plugged in.

BZ#843473

With Red Hat Enterprise Linux 5.9, a patch that fixed IGMP reporting bug in a network bridge was backported to the bonding code from Red Hat Enterprise Linux 6. However, two other patches related to the problem were not included. This update backports these patches from Red Hat Enterprise Linux 6. Specifically, the first patch fixing a NULL pointer deference that could occur if

the master bond was not a network bridge. The patch adds a testing condition which prevents the code from dereferencing a NULL pointer. The second patch introduces a hook that allows to identify which bridge port is used for the master bridge interface and modifies the bonding code to use new functions to determine whether the used bond is a network bridge.

BZ#839839

Under certain circumstances, a race between certain asynchronous operations, such as "silly rename" and "silly delete", and the invalidate_inodes() function could occur when unmounting an NFS file system. Due to this race, the system could become unresponsive, or a kernel oops or data corruption could occur if an inode was removed from the list of inodes while the invalidate_inodes() function performed an iteration on the inode. This update modifies the NFS code to wait until the asynchronous operations are finished before performing inode clean-up. The race condition no longer occurs and an NFS file system is unmounted as expected.

BZ#839334

Previously on system boot, devices with associated Reserved Memory Region Reporting (RMRR) information had lost their RMRR information after they were removed from the static identity (SI) domain. Consequently, a system unexpectedly terminated in an endless loop due to unexpected NMIs triggered by DMA errors. This problem was observed on HP ProLiant Generation 7 (G7) and 8 (Gen8) systems. This update prevents non-USB devices that have RMRR information associated with them from being placed into the SI domain during system boot. HP ProLiant G7 and Gen8 systems that contain devices with the RMRR information now boot as expected.

BZ#831330

Previously, GFS2 did not properly free directory hash table memory from cache when the directory was removed from cache. If the same GFS2 inode was later reused as another directory, the stale directory hash table was reused instead of reading the correct information from the media. If the GFS2 hash table was not reused, a small amount of memory was lost until the next reboot. If the hash table was reused, the directory could become corrupt. Later, GFS2 could discover the file system inconsistency and withdraw from the file system, making it unavailable until the system was rebooted. This update applies a patch to the kernel that frees the directory hash table correctly from cache and prevents this file system corruption.

BZ#795550

The qla2xxx driver creates optrom and optrom_ctl files in sysfs which are used by some tools such as the scli command line tool from QLogic. However, the functions which implement these pseudo-files have race conditions. It will crash the kernel when multiple tools using these files at the same time. Users can work around this issue by making sure only 1 such process is running at a given point of time.

BZ#731531

Switching the FPU context was not properly handled in certain environments, such as systems with multi-core AMD processors using the 32-bit kernel. When running multiple instances of the applications using the FPU frequently, data corruption could occur because processes could often be restored with the context of another instance. This update applies series of patches that modifies the kernel's FPU behavior: the "lazy" FPU context switch is temporarily disabled after 5 consecutive context switches using the FPU, and restored again after the context is switched 256 times. The aforementioned data corruption problem no longer occurs.

BZ#595184

Previously, if a target sent multiple local port logout (LOGO) events, the fc_rport_work() function in the Fibre Channel library module (libfc) tried to process all of them, irrespective of the status of processing prior to the LOGO events. Consequently, fc_rport_work() terminated unexpectedly with

a stack trace. This update simplifies the remote port (rport) restart logic by making the decision to restart after deleting the transport rport. Now, all I/O operations run as expected and fc_rport_work() no longer crashes in the described scenario.

BZ#918952

Previously, the NFSv3 server incorrectly converted 64-bit cookies to 32-bit. Consequently, the cookies became invalid, which affected all file system operations depending on these cookies, such as the READDIR operation that is used to read entries from a directory. This led to various problems, such as exported directories being empty or displayed incorrectly, or an endless loop of the READDIRPLUS procedure which could potentially cause a buffer overflow. This update modifies knfsd code so that 64-bit cookies are now handled correctly and all file system operations work as expected.

Enhancements

BZ#796912

The ALSA HDA audio driver has been updated to support Creative Recon3D audio cards.

BZ#873514

The "unregister_lro_netdev" and "register_lro_netdev" kABI symbols have been added to the kernel. These symbols allow Large Receive Offload (LRO) to be disabled by the kernel stack.

BZ#918279

The Red Hat Enterprise Linux 5.10 kernel includes a new panic_on_io_nmi option (configured using the /proc/sys/kernel/panic_on_io_nmi file), which allows the kernel to panic when a non-maskable interrupt (NMI) occurs that is caused by an I/O error.

BZ#919633

The cciss driver has been updated to the latest version, which adds support for ProLiant servers with the latest HP SAS Smart Array controllers.

All Red Hat Enterprise Linux 5 users are advised to install these updated packages, which correct this issue, and fix the bugs and add the enhancements noted in the Red Hat Enterprise Linux 5.10 Release Notes and Technical Notes. The system must be rebooted for this update to take effect.

4.51.3. RHSA-2013:1292 — Moderate: kernel security and bug fix update

Updated kernel packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 5.

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

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2012-3511, Moderate

This update fixes the following security issues:

* A use-after-free flaw was found in the madvise() system call implementation in the Linux kernel. A local, unprivileged user could use this flaw to cause a denial of service or, potentially, escalate their privileges.

CVE-2013-4162, Moderate

A flaw was found in the way the Linux kernel's TCP/IP protocol suite implementation handled IPv6 sockets that used the UDP_CORK option. A local, unprivileged user could use this flaw to cause a denial of service.

CVE-2013-2141, Low

An information leak flaw in the Linux kernel could allow a local, unprivileged user to leak kernel memory to user-space.

Red Hat would like to thank Hannes Frederic Sowa for reporting CVE-2013-4162.

Bug Fixes

BZ#983864

A bug in the be2net driver prevented communication between NICs using be2net. This update applies a patch addressing this problem along with several other upstream patches that fix various other problems. Traffic between NICs using the be2net driver now proceeds as expected.

BZ#999819

A recent patch fixing a problem that prevented communication between NICs using the be2net driver caused the firmware of NICs to become unresponsive, and thus triggered a kernel panic. The problem was caused by unnecessary usage of a hardware workaround that allows skipping VLAN tag insertion. A patch has been applied and the workaround is now used only when the multi-channel configuration is enabled on the NIC. Note that the bug only affected the NICs with firmware version 4.2.xxxx.

BZ#1001488

A bug in the autofs4 mount expiration code could cause the autofs4 module to falsely report a busy tree of NFS mounts as "not in use". Consequently, automount attempted to unmount the tree and failed with a "failed to umount offset" error, leaving the mount tree to appear as empty directories. A patch has been applied to remove an incorrectly used autofs dentry mount check and the aforementioned problem no longer occurs.

BZ#1005239

A race condition in the be_open function in the be2net driver could trigger the BUG_ON() macro, which resulted in a kernel panic. A patch addressing this problem has been applied and the race condition is now avoided by enabling polling before enabling interrupts globally. The kernel no longer panics in this situation.

All kernel users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.51.4. RHSA-2013:0168 — Moderate: kernel security and bug fix update

Updated kernel packages that fix three security issues and several bugs are now available for Red Hat Enterprise Linux 5.

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

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2012-5515, Moderate

It was found that the Xen hypervisor implementation did not perform range checking on the guest provided values in multiple hypercalls. A privileged guest user could use this flaw to trigger long loops, leading to a denial of service (Xen hypervisor hang).

CVE-2012-1568, Low

It was found that when running a 32-bit binary that uses a large number of shared libraries, one of the libraries would always be loaded at a predictable address in memory. An attacker could use this flaw to bypass the Address Space Layout Randomization (ASLR) security feature.

CVE-2012-4444, Low

A flaw was found in the way the Linux kernel's IPv6 implementation handled overlapping, fragmented IPv6 packets. A remote attacker could potentially use this flaw to bypass protection mechanisms (such as a firewall or intrusion detection system (IDS)) when sending network packets to a target system.

Red Hat would like to thank the Xen project for reporting CVE-2012-5515, and Antonios Atlasis working with Beyond Security's SecuriTeam Secure Disclosure program and Loganaden Velvindron of AFRINIC for reporting CVE-2012-4444.

This update also fixes several bugs. Space precludes documenting all of these changes in this advisory. Documentation for these changes is available in the Red Hat Enterprise Linux 5.9 Technical Notes document.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.51.5. RHSA-2013:1166 — 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 5.

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

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2013-2206, Important

This update fixes the following security issues:

A flaw was found in the way the Linux kernel's Stream Control Transmission Protocol (SCTP) implementation handled duplicate cookies. If a local user queried SCTP connection information at the same time a remote attacker has initialized a crafted SCTP connection to the system, it could trigger a NULL pointer dereference, causing the system to crash.

CVE-2013-2224, Important

It was found that the fix for CVE-2012-3552 released via RHSA-2012:1540 introduced an invalid free flaw in the Linux kernel's TCP/IP protocol suite implementation. A local, unprivileged user could use this flaw to corrupt kernel memory via crafted sendmsg() calls, allowing them to cause a denial of service or, potentially, escalate their privileges on the system.

CVE-2013-2232, Moderate

An invalid pointer dereference flaw was found in the Linux kernel's TCP/IP protocol suite implementation. A local, unprivileged user could use this flaw to crash the system or, potentially, escalate their privileges on the system by using sendmsg() with an IPv6 socket connected to an IPv4 destination.

CVE-2013-2164, , Low, CVE-2013-2147, , Low, CVE-2013-2234, , Low, CVE-2013-2237, , Low

Information leak flaws in the Linux kernel could allow a privileged, local user to leak kernel memory to user-space.

This update also fixes several bugs. Documentation for these changes will be available shortly from the Technical Notes document linked to in the References section.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.51.6. RHSA-2013:0594 — Low: 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 5.

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

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix

CVE-2012-3400, Low

Buffer overflow flaws were found in the udf_load_logicalvol() function in the Universal Disk Format (UDF) file system implementation in the Linux kernel. An attacker with physical access to a system could use these flaws to cause a denial of service or escalate their privileges.

Bug Fixes

BZ#884704

Previously, race conditions could sometimes occur in interrupt handling on the Emulex BladeEngine 2 (BE2) controllers, causing the network adapter to become unresponsive. This update provides a series of patches for the be2net driver, which prevents the race from occurring. The network cards using BE2 chipsets no longer hang due to incorrectly handled interrupt events.

BZ#902683

A boot-time memory allocation pool (the DMI heap) is used to keep the list of Desktop Management Interface (DMI) devices during the system boot. Previously, the size of the DMI heap was only 2048 bytes on the AMD64 and Intel 64 architectures and the DMI heap space could become easily depleted on some systems, such as the IBM System x3500 M2. A subsequent OOM failure could,

under certain circumstances, lead to a NULL pointer entry being stored in the DMI device list. Consequently, scanning of such a corrupted DMI device list resulted in a kernel panic. The boot-time memory allocation pool for the AMD64 and Intel 64 architectures has been enlarged to 4096 bytes and the routines responsible for populating the DMI device list have been modified to skip entries if their name string is NULL. The kernel no longer panics in this scenario.

BZ#905829

The size of the buffer used to print the kernel taint output on kernel panic was too small, which resulted in the kernel taint output not being printed completely sometimes. With this update, the size of the buffer has been adjusted and the kernel taint output is now displayed properly.

BZ#885063

The code to print the kernel taint output contained a typographical error. Consequently, the kernel taint output, which is displayed on kernel panic, could not provide taint error messages for unsupported hardware. This update fixes the typo and the kernel taint output is now displayed correctly.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.51.7. RHSA-2013:1034 — Low: kernel security and bug fix update

Updated kernel packages that fix multiple security issues and various bugs are now available for Red Hat Enterprise Linux 5.

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

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2012-6544, , Low, CVE-2012-6545, , Low, CVE-2013-3222, , Low, CVE-2013-3224, , Low, CVE-2013-3231, , Low, CVE-2013-3235, , Low

Information leaks in the Linux kernel could allow a local, unprivileged user to leak kernel memory to user-space.

CVE-2013-0914, Low

An information leak was found in the Linux kernel's POSIX signals implementation. A local, unprivileged user could use this flaw to bypass the Address Space Layout Randomization (ASLR) security feature.

CVE-2013-1929, Low

A heap-based buffer overflow in the way the tg3 Ethernet driver parsed the vital product data (VPD) of devices could allow an attacker with physical access to a system to cause a denial of service or, potentially, escalate their privileges.

Bug Fixes

BZ#957606

Previously on system boot, devices with associated Reserved Memory Region Reporting (RMRR) information had lost their RMRR information after they were removed from the static identity (SI)

domain. Consequently, a system unexpectedly terminated in an endless loop due to unexpected NMIs triggered by DMA errors. This problem was observed on HP ProLiant Generation 7 (G7) and 8 (Gen8) systems. This update prevents non-USB devices that have RMRR information associated with them from being placed into the SI domain during system boot. HP ProLiant G7 and Gen8 systems that contain devices with the RMRR information now boot as expected.

BZ#958021

Previously, the kernel's futex wait code used timeouts that had granularity in milliseconds. Also, when passing these timeouts to system calls, the kernel converted the timeouts to "jiffies". Consequently, programs could time out inaccurately which could lead to significant latency problems in certain environments. This update modifies the futex wait code to use a high-resolution timer (hrtimer) so the timeout granularity is now in microseconds. Timeouts are no longer converted to "jiffies" when passed to system calls. Timeouts passed to programs are now accurate and the programs time out as expected.

BZ#966878

A recent change modified the size of the task_struct structure in the floating point unit (fpu) counter. However, on Intel Itanium systems, this change caused the kernel Application Binary Interface (kABI) to stop working properly when a previously compiled module was loaded, resulting in a kernel panic. With this update the change causing this bug has been reverted so the bug can no longer occur.

BZ#971872

The cxgb4 driver previously did not clear data structures used for firmware requests. Consequently, when initializing some Chelsio's Terminator 4 (T4) adapters, a probe request could fail because the request was incompatible with the adapter's firmware. This update modifies the cxgb4 driver to properly initialize firmware request structures before sending a request to the firmware and the problem no longer occurs.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.51.8. RHSA-2013:0847 — Moderate: kernel security and bug fix update

Updated kernel packages that fix one security issue and multiple bugs are now available for Red Hat Enterprise Linux 5.

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

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fix

CVE-2013-0153, Moderate

A flaw was found in the way the Xen hypervisor AMD IOMMU driver handled interrupt remapping entries. By default, a single interrupt remapping table is used, and old interrupt remapping entries are not cleared, potentially allowing a privileged guest user in a guest that has a passed-through, bus-mastering capable PCI device to inject interrupt entries into others guests, including the privileged management domain (Dom0), leading to a denial of service.

Red Hat would like to thank the Xen project for reporting the CVE-2013-0153 issue.

Bug Fixes

BZ#947736

When a process is opening a file over NFSv4, sometimes an OPEN call can succeed while the following GETATTR operation fails with an NFS4ERR_DELAY error. The NFSv4 code did not handle such a situation correctly and allowed an NFSv4 client to attempt to use the buffer that should contain the GETATTR information. However, the buffer did not contain the valid GETATTR information, which caused the client to return a "-ENOTDIR" error. Consequently, the process failed to open the requested file. This update backports a patch that adds a test condition verifying validity of the GETATTR information. If the GETATTR information is invalid, it is obtained later and the process opens the requested file as expected.

BZ#952098

Previously, the xdr routines in NFS version 2 and 3 conditionally updated the res->count variable. Read retry attempts after a short NFS read() call could fail to update the res->count variable, resulting in truncated read data being returned. With this update, the res->count variable is updated unconditionally so this bug can no longer occur.

BZ#953435

When handling requests from Intelligent Platform Management Interface (IPMI) clients, the IPMI driver previously used two different locks for an IPMI request. If two IPMI clients sent their requests at the same time, each request could receive one of the locks and then wait for the second lock to become available. This resulted in a deadlock situation and the system became unresponsive. The problem could occur more likely in environments with many IPMI clients. This update modifies the IPMI driver to handle the received messages using tasklets so the driver now uses a safe locking technique when handling IPMI requests and the mentioned deadlock can no longer occur.

BZ#954296

Incorrect locking around the cl_state_owners list could cause the NFSv4 state reclaimer thread to enter an infinite loop while holding the Big Kernel Lock (BLK). As a consequence, the NFSv4 client became unresponsive. With this update, safe list iteration is used, which prevents the NFSv4 client from hanging in this scenario.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.51.9. RHSA-2013:0747 — Moderate: kernel security and bug fix update

Updated kernel packages that fix several security issues and three bugs are now available for Red Hat Enterprise Linux 5.

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

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2013-0216, Moderate

A flaw was found in the Xen netback driver implementation in the Linux kernel. A privileged guest user with access to a para-virtualized network device could use this flaw to cause a long loop in netback, leading to a denial of service that could potentially affect the entire system.

CVE-2013-0231, Moderate

A flaw was found in the Xen PCI device back-end driver implementation in the Linux kernel. A privileged guest user in a guest that has a PCI passthrough device could use this flaw to cause a denial of service that could potentially affect the entire system.

CVE-2013-1826, Moderate

A NULL pointer dereference flaw was found in the IP packet transformation framework (XFRM) implementation in the Linux kernel. A local user who has the CAP_NET_ADMIN capability could use this flaw to cause a denial of service.

CVE-2012-6537, Low

Information leak flaws were found in the XFRM implementation in the Linux kernel. A local user who has the CAP_NET_ADMIN capability could use these flaws to leak kernel stack memory to user-space.

CVE-2012-6542, Low

An information leak flaw was found in the logical link control (LLC) implementation in the Linux kernel. A local, unprivileged user could use this flaw to leak kernel stack memory to user-space.

CVE-2012-6546, Low

Two information leak flaws were found in the Linux kernel's Asynchronous Transfer Mode (ATM) subsystem. A local, unprivileged user could use these flaws to leak kernel stack memory to user-space.

CVE-2012-6547, Low

An information leak flaw was found in the TUN/TAP device driver in the Linux kernel's networking implementation. A local user with access to a TUN/TAP virtual interface could use this flaw to leak kernel stack memory to user-space.

Red Hat would like to thank the Xen project for reporting the CVE-2013-0216 and CVE-2013-0231 issues.

Bug Fixes

BZ#923353

The IPv4 code did not correctly update the Maximum Transfer Unit (MTU) of the designed interface when receiving ICMP Fragmentation Needed packets. Consequently, a remote host did not respond correctly to ping attempts. With this update, the IPv4 code has been modified so the MTU of the designed interface is adjusted as expected in this situation. The ping command now provides the expected output.

BZ#923910

Previously, the be2net code expected the last word of an MCC completion message from the firmware to be transferred by direct memory access (DMA) at once. However, this is not always true, and could therefore cause the BUG_ON() macro to be triggered in the be_mcc_compl_is_new() function, consequently leading to a kernel panic. The BUG_ON() macro has been removed from be_mcc_compl_is_new(), and the kernel panic no longer occurs in this scenario.

BZ#924087

Previously, the NFSv3 server incorrectly converted 64-bit cookies to 32-bit. Consequently, the cookies became invalid, which affected all file system operations depending on these cookies, such

as the READDIR operation that is used to read entries from a directory. This led to various problems, such as exported directories being empty or displayed incorrectly, or an endless loop of the READDIRPLUS procedure which could potentially cause a buffer overflow. This update modifies knfsd code so that 64-bit cookies are now handled correctly and all file system operations work as expected.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.51.10. RHSA-2013:0621 — Important: kernel security update

Updated kernel packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

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

The kernel packages contain the Linux kernel, the core of any Linux operating system.

Security Fixes

CVE-2013-0268, Important

A flaw was found in the way file permission checks for the "/dev/cpu/[x]/msr" files were performed in restricted root environments (for example, when using a capability-based security model). A local user with the ability to write to these files could use this flaw to escalate their privileges to kernel level, for example, by writing to the SYSENTER_EIP_MSR register.

CVE-2013-0871, Important

A race condition was found in the way the Linux kernel's ptrace implementation handled PTRACE_SETREGS requests when the debuggee was woken due to a SIGKILL signal instead of being stopped. A local, unprivileged user could use this flaw to escalate their privileges.

Users should upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

4.52. kexec-tools

4.52.1. RHBA-2013:1321 — kexec-tools bug fix update

Updated kexec-tools packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

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#864011

The vmcore file is generated in the /proc file system. Prior to this update, the kdump (kernel crash collection) service failed to copy vmcore to the desired encrypted target partition. As a consequence, kdump failed to mount rootfs and dropped to a shell. With this update, the user is now notified to not dump to encrypted disks.

BZ#901620

A previous version of kexec-tools introduced a regression whereby kdump called findmodule for the ext[234] dump target. As ext2 is built into Red Hat Enterprise Linux 5 kernel, mkdumprd failed with the following error message: "No module ext2 found for kernel 2.6.18-238.5.1.el5, aborting.". To fix this bug, ext2 has been removed from the findmodule list and mkdumprd no longer fails.

BZ#919369

Due to incorrect computing of MEMSZ (amount of physical memory allocated to a resource pool or virtual machine), kdump failed to start on Red Hat Enterprise Linux 5 Xen Domain-0 if it had less than 4G RAM. The kdump service also asked for the /boot/vmlinuz-2.6.18-348.el5PAE Physical Address Extension (PAE) location. The kdump kernel service has been set to be non-PAE for systems with less than 4G RAM, thus fixing the bug. As a result, kdump starts as expected.

BZ#919962

The makedumpfile(8) manual pages have now been added to the Red Hat Enterprise Linux 5 documentation.

Users of kexec-tools are advised to upgrade to these updated packages, which fix these bugs.

4.52.2. RHBA-2013:0617 — kexec-tools bug fix update

Updated kexec-tools packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The kexec fastboot mechanism allows booting a Linux kernel from the context of an already running kernel. The kexec-tools package provides the /sbin/kexec binary and ancillary utilities that form the user-space component of the kernel's kexec feature.

Bug Fixes

BZ#915359

A previous version of kexec-tools introduced a regression whereby kdump called findmodule for the ext[234] dump target, but ext2 was built in the kernel. This caused the mkdumprd utility, which creates an initial RAM file system for use in conjunction with the booting of a kernel within the kdump framework for crash recovery, to fail with a "No module ext2 found" error message. This patch fixes this problem by removing ext2 from the findmodule list and these failures no longer occur.

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

4.53. krb5

4.53.1. RHSA-2013:0942 — Moderate: krb5 security update

Updated krb5 packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

Kerberos is a network authentication system which allows clients and servers to authenticate to each other using symmetric encryption and a trusted third-party, the Key Distribution Center (KDC).

Security Fix

CVE-2002-2443

It was found that kadmind's kpasswd service did not perform any validation on incoming network packets, causing it to reply to all requests. A remote attacker could use this flaw to send spoofed packets to a kpasswd service that appear to come from kadmind on a different server, causing the services to keep replying packets to each other, consuming network bandwidth and CPU.

All krb5 users should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, the krb5kdc and kadmind daemons will be restarted automatically

4.54. ksh

4.54.1. RHBA-2013:1351 — ksh bug fix update

Updated ksh packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

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#892206

Due to a bug in the ksh package, command substitutions containing the pipe ("|") character returned incorrect return codes. This bug has been fixed, and the pipe character can now be used inside command substitutions without complications.

BZ#910923

Previously, the ksh SIGTSTP signal handler could trigger another SIGTSTP signal. Consequently, ksh would enter an infinite loop. This updated version fixes the SIGTSTP signal processing and ksh now handles this signal without problems.

BZ#912443

In certain cases, ksh did not execute command substitution inside of "here" documents. Consequently, some content of a here document could be missing. With this update, the command substitution for here documents has been fixed. As a result, here documents include data from command substitutions as expected.

BZ#921138

Previously, when using arrays inside of ksh functions, memory leaks occurred. This bug has been fixed, and memory leaks no longer occur in the described scenario.

BZ#958195

Previously, ksh did not resize the file descriptor list every time it was necessary. Consequently, a memory corruption could occur when a large amount of file descriptors were used. With this update, ksh has been modified to resize the file descriptor list every time it is needed. As a result, memory corruption no longer occurs in the described scenario.

BZ#972732

Previously, ksh did not prevent modifications of variables of the read-only type. As a consequence, ksh terminated unexpectedly with a segmentation fault when such a variable had been modified. With this update, modification of read-only variables are not allowed, and ksh prints an error

With this update, modification of read-only variables are not allowed, and ksh prints an error message in this scenario.

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

4.55. kvm

4.55.1. RHSA-2013:0608 — Important: kvm security update

Updated kvm packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

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

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel.

Security Fix

CVE-2012-6075

A flaw was found in the way QEMU-KVM emulated the e1000 network interface card when the host was configured to accept jumbo network frames, and a guest using the e1000 emulated driver was not. A remote attacker could use this flaw to crash the guest or, potentially, execute arbitrary code with root privileges in the guest.

All users of kvm are advised to upgrade to these updated packages, which contain backported patches to correct this issue. Note that the procedure in the Solution section must be performed before this update will take effect.

4.55.2. RHSA-2013:0727 — Important: kvm security update

Updated kvm packages that fix three security issues are now available for Red Hat Enterprise Linux 5.

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

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel.

Security Fixes

CVE-2013-1796

A flaw was found in the way KVM handled guest time updates when the buffer the guest registered by writing to the MSR_KVM_SYSTEM_TIME machine state register (MSR) crossed a page boundary. A privileged guest user could use this flaw to crash the host or, potentially, escalate their privileges, allowing them to execute arbitrary code at the host kernel level.

CVE-2013-1797

A potential use-after-free flaw was found in the way KVM handled guest time updates when the GPA (guest physical address) the guest registered by writing to the MSR_KVM_SYSTEM_TIME machine state register (MSR) fell into a movable or removable memory region of the hosting user-space process (by default, QEMU-KVM) on the host. If that memory region is deregistered from

KVM using KVM_SET_USER_MEMORY_REGION and the allocated virtual memory reused, a privileged guest user could potentially use this flaw to escalate their privileges on the host.

CVE-2013-1798

A flaw was found in the way KVM emulated IOAPIC (I/O Advanced Programmable Interrupt Controller). A missing validation check in the ioapic_read_indirect() function could allow a privileged guest user to crash the host, or read a substantial portion of host kernel memory.

Red Hat would like to thank Andrew Honig of Google for reporting all of these issues.

All users of kvm are advised to upgrade to these updated packages, which contain backported patches to correct these issues. Note that the procedure in the Solution section must be performed before this update will take effect.

4.55.3. RHBA-2013:1008 — kvm bug fix update

Updated kvm packages that fix various bugs are now available for Red Hat Enterprise Linux 5.

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel.

Bug Fix

BZ#958359

Previously, tb_invalidate_phys_page_range() incurred a segmentation fault because it walked through an invalid chain of translation blocks. Thus, page_find() returned an incorrect pointer, which was subsequently used by tb_invalidate_phys_page_range() to find the head of the translation block chain. This update corrects the chain of translation blocks and crashes no longer occur.

Users of KVM are advised to upgrade to these updated packages, which fix these bugs. Note that the procedure in the Solution section must be performed before this update will take effect.

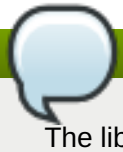
4.56. libtevent

4.56.1. RHBA-2013:1343 — libtevent bug fix and enhancement update

Updated libtevent packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The libtevent packages provide Tevent, an event system based on the talloc memory management library. Tevent supports many event types, including timers, signals, and the classic file descriptor events. Tevent also provides helpers to deal with asynchronous code represented by the tevent_req() (Tevent Request) functions.

This update also fixes the following bug:



Note

The libtevent package has been upgraded to upstream version 0.9.18, which provides a number of bug fixes and enhancements over the previous version. (BZ#951045)

This update also fixes the following bug:

Bug Fix

BZ#975488

Prior to this update, a condition in the poll backend copied a 64-bit variable into an unsigned integer variable, which was smaller than 64-bit on 32-bit architectures. Using that unsigned integer variable in a condition rendered that condition to be always false. The variable has been fixed to be of uint64_t format guaranteeing its width to be 64 bits on all architectures. As a result, the condition now yields expected results.

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

4.57. libvirt

4.57.1. RHBA-2013:0575 — libvirt bug fix update

Updated libvirt packages that fix one bug are now available for Red Hat Enterprise Linux 5.

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. The libvirt library also provides nwfilter support for fine-grained filtering of the network traffic reaching guests managed by libvirt.

Bug Fix

BZ#903600

If an LVM volume group contains a striped LVM volume, the output of the "device" field separates the multiple device paths using the comma separator. Previously, the libvirt library also used the lvs command with the comma separator, which caused regular expressions in the libvirt code to parse the output of lvs incorrectly when used on a striped LVM volume. Consequently, creation of a logical storage pool in libvirt failed if the used LVM volume group contained the striped LVM volume. Also, libvirt did not have the correct mechanism to generate multiple device XML elements for the multiple device paths of striped LVM volume. With this update, libvirt has been modified to use lvs with the "#" separator; also, the library can now parse the multiple device paths of striped LVM volumes and generate relevant XML code. Users can now create logical storage pools with striped LVM volumes and generate appropriate XML code as expected.

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

4.58. libxml2

4.58.1. RHBA-2013:0591 — libxml2 bug fix update

Updated libxml2 packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The libxml2 software library is used to manipulate XML files. It includes support to read, modify and write XML and HTML files. It is also the basis for the libxslt library which processes XSLT-1.0 stylesheets.

Bug Fixes

BZ#915350

Due to errors in the internal regular expression support, libxml2 sometimes failed when validating XMLs with certain XSD and Relax-NG files. Currently, the relaxng and xmlregexp codes are modified and libxml2 can now validate XMLs with those specific XSD and Relax-NG files.

BZ#915837

Previously, an internal routine xmlDOMWrapCloneNode would fail to preserve the namespace of an XML element being copied, which caused the namespace of the parameter node to be omitted from the copy. With this update, the problem no longer occurs.

Users of libxml2 parser are advised to upgrade to these updated packages, which fix these bugs.

4.58.2. RHSA-2013:0581 — Moderate: libxml2 security update

Updated libxml2 packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

The libxml2 library is a development toolbox providing the implementation of various XML standards.

Security Fix

CVE-2013-0338

A denial of service flaw was found in the way libxml2 performed string substitutions when entity values for entity references replacement was enabled. A remote attacker could provide a specially-crafted XML file that, when processed by an application linked against libxml2, would lead to excessive CPU consumption.

All users of libxml2 are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. The desktop must be restarted (log out, then log back in) for this update to take effect.

4.58.3. RHBA-2013:1123 — libxml2 bug fix update

Updated libxml2 packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The libxml2 software library is used to manipulate XML files. Among the operations allowed, it can validate XML files against XML Schematics.

Bug Fix

BZ#987321

This update fixes a regression that was introduced by the RHBA-2013:0591 advisory. This regression added a flaw in the XML schema compilation process. This flaw caused libxml2 to fail to compile some XML schemas, indicating that they had a non-deterministic content model. The broken code is now fixed, so libxml2 can compile those schemas and validate XMLs as expected.

Users of libxml2 are advised to upgrade to these updated packages, which fix this regression. The desktop must be restarted (log out, then log back in) for this update to take effect.

4.59. lmbench

4.59.1. RHBA-2013:1174 — lmbench bug fix update

An updated lmbench package that fixes several bugs is now available for Red Hat Enterprise Linux Hardware Certification.

lmbench is a series of micro benchmarks intended to measure basic operating system and hardware system metrics. The benchmarks fall into three general classes: bandwidth, latency, and "other".

Bug Fix

BZ#958448, BZ#958449

Previously, the lmbench package included unnecessary files which were not needed by the Red Hat Hardware Certification Test Suite and caused conflicts with other packages during installation. With this update, the unnecessary content has been removed.

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

4.60. ltrace

4.60.1. RHBA-2013:1317 — ltrace bug fix update

Updated ltrace packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

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#239057

On a system with the Itanium architecture, a SIGILL signal was occasionally delivered as a valid signal that informed the ltrace utility about events in a traced binary. However, ltrace misinterpreted the SIGILL signal as a signal delivered to the traced binary. With this update, ltrace handles SIGILL as expected.

BZ#526007

When tracing a process with many threads, the traced process was often killed as the threads ran into breakpoints that could not be handled by the ltrace utility. With this update, ltrace attaches to the newly created threads and carefully handles the breakpoints so that tracing events are not missed. Note that when ltrace attached to a running process, that process could have been detached from with the instruction pointer pointed to mid-instruction, or with pending events, which would kill the process. This update improves the detach logic so that the process is left in a consistent state before detaching.

BZ#639947

Due to a bug in the logic of tracing processes, the ltrace utility missed tracing events in forked processes on PowerPC systems. The logic of tracing processes that fork or clone has been improved and ltrace now works as expected.

BZ#754096

On PowerPC systems, the "-e" option did not work correctly. Consequently, when the option was given with a symbol name that did not match any of the symbols in the traced binary, the ltrace utility terminated unexpectedly. This update provides a patch to fix this bug and ltrace no longer crashes in the described scenario.

BZ#868281

Previously, the ltrace utility did not support PIE (Position Independent Executables) 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 PIE binaries and processes has been added and ltrace now handles the additional processing for the PIE binaries correctly.

BZ#890961

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.

4.61. lvm2

4.61.1. RHBA-2013:1352 — lvm2 bug fix update

Updated lvm2 packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The lvm2 packages provide support for Logical Volume Management (LVM).

Bug Fixes

BZ#711890

Previously, when the lvconvert command was used with the "--stripes" option, the required supplementary options, such as "--mirrors" or "--repair", were not enforced. Consequently, calling "lvconvert --stripes" without accompanying conversion instructions led to an incomplete conversion. With this update, a condition has been added to enforce the correct syntax. As a result, an error message is now displayed in the described scenario.

BZ#749883

A mirrored logical volume (LV) can itself have a mirrored log device. Previously, a simultaneous failure of both the mirrored leg and the mirror log was not handled correctly. Consequently, I/O errors occurred on the mirror LV. The described failure case is now handled correctly and I/O errors no longer occur.

BZ#773312

Due to a bug in the error condition, an attempt to up-convert an inactive mirror when there was insufficient allocatable extents led to the following error message:

Unable to allocate extents for mirror(s). ABORTING: Failed to remove temporary mirror layer inactive_mimagetmp_3. Manual cleanup with vgcfgrestore and dmsetup may be required.

The wording of this message was possibly misleading. The bug has been fixed, and a more accurate warning message is now displayed when not enough extents are available.

BZ#830993

Prior to this update, it was impossible to set the major and minor persistent numbers of a logical volume to a value outside of the range of 0-255 (8-bit). This limit has been changed, and the major number can now be set within the range of 0-4095 (12-bit), while the minor number within 0-1048575 (20-bit).

BZ#863112

Previously, the mpath filtering, which is enabled by the devices/multipath_component_detection=1 setting in the lvm.conf configuration file, did not check for partitions and failed when there were partitions on multipath components. Consequently, a message about duplicate physical volumes (PV) was issued as the LVM saw two PVs with the same UUID. With this update, mpath filtering has been modified to check for partitions properly and the aforementioned error no longer occurs.

BZ#908097

When there were missing physical volumes in a volume group (VG), most operations that alter the LVM meta data (such as the vgimport utility) were disallowed. Consequently, it was impossible to import and also to repair this VG. With this update, this behavior has been modified and it is now possible to use the "--force" option with vgimport to import VGs even with missing devices.

BZ#913664

Prior to this update, the lvconvert utility did not check for snapshot-merge support in the kernel before initializing the merge operation. After trying to merge a snapshot logical volume (LV) on a machine without this support, the origin LV failed to activate on the next boot. With this update, lvconvert has been modified not to start a snapshot-merge if there is no support for such operation in the kernel.

Users of lvm2 are advised to upgrade to these updated packages, which fix these bugs.

4.62. man-pages-overrides

4.62.1. RHBA-2013:1357 — man-pages-overrides bug fix update

An updated man-pages-overrides package that fixes several bugs is now available for Red Hat Enterprise Linux 5.

The man-pages-overrides package provides a collection of manual (man) pages to complement other packages or update those contained therein.

Bug Fixes

BZ#553440

Various manual pages from the poppler package contained an incorrect path to the configuration file and references to non-existent man pages. The invalid paths to the configuration file have been fixed and incorrect references removed form the man pages.

BZ#711765

Previously, the runcon(1) manual page did not specify the exact position of the "--" special argument. The position of the argument is now specified.

BZ#760101

The pam_limits PAM module has an off-by-one bug in calculation of the RLMIT_NICE priority. If the nice limit is set to -1, the real value set in the kernel will be equivalent to nice value 0. The

nice limit is set to -1, the real value set in the kernel will be equivalent to nice value 0. The limits.conf(5) manual page now describes the problem and provides a workaround.

BZ#896053

The missing BUGS section has been added to the times(2) manual page and describes a known bug that can occur in a small time window soon after the boot.

BZ#903550

Previously, the "max_childs" parameter was not documented in the udevd(8) manual page. This update adds documentation of that parameter.

BZ#949789

Previously, the shmop(2) manual page did not list the EIDRM error code in the Error section. The error code is now included in the manual page.

Users of man-pages-overrides are advised to upgrade to this updated package, which fixes these bugs.

4.63. mesa

4.63.1. RHSA-2013:0898 — Moderate: mesa security update

Updated mesa packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

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

Mesa provides a 3D graphics API that is compatible with Open Graphics Library (OpenGL). It also provides hardware-accelerated drivers for many popular graphics chips.

Security Fix

CVE-2013-1993

It was found that Mesa did not correctly validate messages from the X server. A malicious X server could cause an application using Mesa to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

All users of Mesa are advised to upgrade to these updated packages, which contain backported patches to correct these issues. All running applications linked against Mesa must be restarted for this update to take effect.

4.64. microcode_ctl

4.64.1. RHEA-2013:1340 — microcode_ctl enhancement update

Updated microcode_ctl packages that add one enhancement are now available for Red Hat Enterprise Linux 5.

The microcode_ctl packages provide microcode updates for Intel and AMD processors.

Enhancement

BZ#915898

The Intel CPU microcode file has been updated to version 20130808. 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 in order for these changes to take effect.

4.65. mkinitrd

4.65.1. RHBA-2013:0863 — mkinitrd bug fix update

Updated mkinitrd packages that fix one bug are now available Red Hat Enterprise Linux 5.

The mkinitrd packages provide a utility to create the initrd file system image. The initrd image is an initial RAM disk that is loaded by a boot loader before the Linux kernel is started.

Bug Fix

BZ#963559

Due to a bug in the libblkid library, the grubby utility could terminate unexpectedly with a segmentation fault when attempting to install multiple kernels in succession. This update uses the new version of libblkid and grubby now works as expected in the described scenario.

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

4.65.2. RHBA-2013:1288 — mkinitrd bug fix update

Updated mkinitrd packages that fix one bug are now available Red Hat Enterprise Linux 5.

The mkinitrd packages provide a utility to create the initrd file system image. The initrd image is an initial RAM disk that is loaded by a boot loader before the Linux kernel is started.

Bug Fix

BZ#1009239

After upgrading the nss package to version 3.14.3, systems with FIPS mode enabled did not boot, displaying the following message:

Error initializing NSS.

This was due to a missing library in the initrd image. This update adds the libsqlite3 library to the initrd image, and systems now boot correctly when FIPS mode is enabled.

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

4.66. module-init-tools

4.66.1. RHBA-2013:1359 — module-init-tools bug fix update

Updated module-init-tools packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The module-init-tools packages include various programs needed for automatic loading and unloading of modules under kernel versions 2.6 and later, as well as other module management programs. Device drivers and file systems are two examples of loaded and unloaded modules.

Bug Fix

BZ#708458

Updating kmod-kvm after a kernel update had been performed caused a broken symbolic link to the kvm.ko module due to the link pointing to the old kernel's kvm.ko module. Now, the new version of kmod-kvm is updated, and broken symbolic links no longer occur in the described scenario.

Users of module-init-tools are advised to upgrade to these updated packages, which fix this bug.

4.67. mysql

4.67.1. RHSA-2013:0180 — Important: mysql security update

Updated mysql packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

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

MySQL is a multi-user, multi-threaded SQL database server. It consists of the MySQL server daemon (mysqld) and many client programs and libraries.

Security Fixes

CVE-2012-5611

A stack-based buffer overflow flaw was found in the user permission checking code in MySQL. An authenticated database user could use this flaw to crash the mysqld daemon or, potentially, execute arbitrary code with the privileges of the user running the mysqld daemon.

CVE-2012-2749

A flaw was found in the way MySQL calculated the key length when creating a sort order index for certain queries. An authenticated database user could use this flaw to crash the mysqld daemon.

BZ#814605

This update also adds a patch for a potential flaw in the MySQL password checking function, which could allow an attacker to log into any MySQL account without knowing the correct password. This problem (CVE-2012-2122) only affected MySQL packages that use a certain compiler and C library optimization. It did not affect the mysql packages in Red Hat Enterprise Linux 5. The patch is being added as a preventive measure to ensure this problem cannot get exposed in future revisions of the mysql packages.

All MySQL users should upgrade to these updated packages, which correct these issues. After installing this update, the MySQL server daemon (mysqld) will be restarted automatically.

4.68. nfs-utils

4.68.1. RHBA-2013:1301 — nfs-utils bug fix update

Updated nfs-utils packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The nfs-utils packages provide a daemon for the kernel Network File System (NFS) server, and related tools such as the mount.nfs, umount.nfs, and showmount.

Bug Fixes

BZ#726472

Previously, during an NFS service start, users encountered the following rpc.idmapd message "dirscancb: open(/var/lib/nfs/rpc_pipefs/nfs/clnt6a): No such file or directory." This was because the daemon "rpc.idmapd" scanned the /var/lib/nfs/rpc_pipefs/nfs/ directory periodically looking for NFS client mounts to communicate to. The daemon tried to open communication with a client mount, but it disappeared in between looking for directory entries and opening them. NFS mount was umounted just before rpc.idmapd tried to communicate with it. This update requires Verbosity to be set to 1 or higher in order for the problem warning message to display. With the default Verbosity of 0, it is no longer logged, preventing it from clogging the logs with unhelpful messages.

BZ#873307

During system shutdown, the "umount" utility was called as part of a shutdown script, so the shutdown script failed to unmount the /var/ file system correctly. This was because the shutdown script searched for the /var/lock/subsys/nfs lock file, but could not find it because NFS service created the /var/lock/subsys/nfsd lock file. This update fixes the issue in the /etc/rc.d/rc script itself, so it tries to find nfsd and not the NFS lock file, and the shutdown script now successfully unmounts the file system.

BZ#892236

Previously, when the NFS service was started, messages that the RPC idmapd service was stopped and started were displayed. This occurred because in order to start NFS, the RPC idmapd service had to be restarted using the condrestart option (conditional restart), which starts RPC idmapd only if it is currently running. With this update, RPC idmapd messages are no longer displayed in the described scenario when the NFS service is started.

BZ#947552

Previously, the NFS version 3 of the MOUNT protocol was not fully supported. Therefore, the "showmount" utility did not work properly, and there were possible issues with the "umount" utility. Changes from the NFS version 2 protocol to the NFS version 3 protocol have required some adjustments to be made in the MOUNT protocol. To meet the needs of the NFS version 3 protocol, a new version of the MOUNT protocol has been defined. This new protocol satisfies the requirements of the NFS version 3 protocol, and addresses several other current market requirements. Thus, the "showmount" and "unmount" utilities now function as expected.

Users of nfs-utils are advised to upgrade to these updated packages, which fix these bugs. After installing this update, the nfs service will be restarted automatically.

4.69. nss

4.69.1. RHBA-2013:1318 — nss bug fix and enhancement update

Updated nss packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. Netscape Portable Runtime (NSPR) provides platform independence for non-GUI operating system facilities.

Bug Fixes

BZ#784676

A lack-of-robustness flaw caused the administration server for Red Hat Directory Server to terminate unexpectedly because the mod_nss module made nss calls before initializing nss as per the documented API. With this update, nss protects itself against being called before it has been properly initialized by the caller.

BZ#807419

Previously, output of the certutil -H command, which is a list of options and arguments used by the certutil tool, did not describe the -F option. This information has been added and the -F option is now properly described in the output of certutil -H.

BZ#855809

Due to a bug in the FreeBL library, the Openswan application could generate a Key Exchange payload that was one byte shorter than what was required by the Diffie Hellman (DH) protocol. Consequently, Openswan dropped connections during such payloads. With this update, the DH key derivation function in FreeBL has been fixed and connections are no longer dropped by Openswan.

BZ#975600

Previously, the remote-viewer utility failed to utilize a plugged-in smart card reader when a Spice client was running. Eventually, the client could terminate unexpectedly. Now, remote-viewer recognizes the reader and offers authentication once the card is inserted, and the crashes no longer occur.

BZ#987131

With this update, NSS has incorporated various GCM code fixes applied upstream since nss-3.14.3 was released.

Enhancement

BZ#960241

With this update, NSS's own internal cryptographic module now supports the NIST Suite B set of recommended algorithms for Elliptic Curve Cryptography.

Users of NSS and NSPR are advised to upgrade to these updated packages, which fix these issues and add this enhancement. After installing this update, applications using NSS or NSPR must be restarted for this update to take effect.

4.70. nss and nspr

4.70.1. RHSA-2013:1135 — Moderate: nss and nspr security, bug fix, and enhancement update

Updated nss and nspr packages that fix two security issues, various bugs, and add enhancements are now available for Red Hat Enterprise Linux 5.

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.

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. Netscape Portable Runtime (NSPR) provides platform independence for non-GUI operating system facilities.

Security Fixes

CVE-2013-1620

It was discovered that NSS leaked timing information when decrypting TLS/SSL and DTLS protocol encrypted records when CBC-mode cipher suites were used. A remote attacker could possibly use this flaw to retrieve plain text from the encrypted packets by using a TLS/SSL or DTLS server as a padding oracle.

CVE-2013-0791

An out-of-bounds memory read flaw was found in the way NSS decoded certain certificates. If an application using NSS decoded a malformed certificate, it could cause the application to crash.

Red Hat would like to thank the Mozilla project for reporting CVE-2013-0791. Upstream acknowledges Ambroz Bizjak as the original reporter of CVE-2013-0791.

Bug Fix

BZ#958023

A defect in the FreeBL library implementation of the Diffie-Hellman (DH) protocol previously caused Openswan to drop connections.

In addition, the nss package has been upgraded to upstream version 3.14.3, and the nspr package has been upgraded to upstream version 4.9.5. These updates provide a number of bug fixes and enhancements over the previous versions. (BZ#949845, BZ#924741)

Note that while upstream NSS version 3.14 prevents the use of certificates that have an MD5 signature, this erratum includes a patch that allows such certificates by default. To prevent the use of certificates that have an MD5 signature, set the "NSS_HASH_ALG_SUPPORT" environment variable to "-MD5".

Users of NSS and NSPR are advised to upgrade to these updated packages, which fix these issues and add these enhancements. After installing this update, applications using NSS or NSPR must be restarted for this update to take effect.

4.70.2. RHSA-2013:0214 — Important: nss and nspr security, bug fix, and enhancement update

Updated nss and nspr packages that fix one security issue, various bugs, and add enhancements are now available for Red Hat Enterprise Linux 5.

The Red Hat Security Response Team has rated this update as having important security impact.

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. Netscape Portable Runtime (NSPR) provides platform independence for non-GUI operating system facilities.

Bug Fix

BZ#890605

It was found that a Certificate Authority (CA) mis-issued two intermediate certificates to customers. These certificates could be used to launch man-in-the-middle attacks. This update renders those certificates as untrusted. This covers all uses of the certificates, including SSL, S/MIME, and code signing.

BZ#893371, BZ#893372

In addition, the nss package has been upgraded to upstream version 3.13.6, and the nspr package has been upgraded to upstream version 4.9.2. These updates provide a number of bug fixes and enhancements over the previous versions.

All NSS and NSPR users should upgrade to these updated packages, which correct these issues and add these enhancements. After installing the update, applications using NSS and NSPR must be restarted for the changes to take effect.

4.71. nss_ldap

4.71.1. RHBA-2013:0251 — nss_ldap bug fix update

Updated nss_ldap packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The nss_ldap packages contain the nss_ldap and pam_ldap modules. The nss_ldap module is a name service switch module, which allows applications to retrieve information about users and groups from a directory server. The pam_ldap module allows a directory server to be used by PAM-aware applications to verify user passwords.

Bug Fix

BZ#905908

Due to LDAP connectivity problems, the nss_ldap module returned error conditions but failed to clean them up. Consequently, nss_ldap started leaking file descriptors, namely sockets. A patch has been provided to address this bug and the socket leaks no longer occur in nss_ldap.

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

4.72. openmotif

4.72.1. RHBA-2013:1355 — openmotif bug fix update

Updated *openmotif* packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

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#492529

Attempting to use a keyboard accelerator such as Ctrl+S, failed to achieve the intended effect when the Caps Lock, Scroll Lock or NumLock keys were activated. This was caused by missing support for the X11R6 modifiers scheme. Support for the modifiers scheme has been implemented in this update so that keyboard accelerators can be used as expected even when modifiers, such as Caps Lock, Scroll Lock or NumLock, have been activated.

BZ#557453

Redisplaying a **`Label`** or the **`LabelGadget`** widget could have caused a **`BadDrawable X`** error and resulted in an invisible label. This update resolves the problem with unspecified pixmaps so that labels do not become invisible and **`BadDrawable`** errors are not incurred.

BZ#568730

Selecting an item in the **MultiList** widget resulted in that item becoming invisible due to the same color being used for both foreground and background colors. The same problem occurred with "insensitive" labels, buttons, icons and list entries. With this update, foreground and background colors in widgets have been differentiated so that the items do not become invisible during operation.

BZ#634094

Due to 32-bit time stamp problems, attempting to copy and paste on 64-bit architecture using the clipboard may have failed occasionally. With this update, the underlying source code has been modified to ensure the time stamp always contains a "CARD32" value, so that copy and paste on 64-bit architectures works as expected.

BZ#638553

Previously, a check that would limit removing a callback to valid windows while the focus is reset was missing in the code. Consequently, destroying a torn-off menu with a submenu mapped caused the application to terminate unexpectedly. With this update, the underlying source code has been modified to ensure that the focus is reset for valid windows only and destroying a torn-off menu with a submenu mapped now works as expected.

BZ#772937

The RHBA:2011-1451 advisory introduced a regression by specifying the **XmI.h** header file in the include directive of multiple files. However, if the file was not installed, compiling applications that used the **Label** and **LabelGadget** widgets failed with the following message:

```
/usr/include/Xm/LabelGP.h:48:17: error: XmI.h: No such file or
directory
```

With this update, the include directive containing "XmI.h" has been removed. Applications using the **Label** and **LabelGadget** widgets can now be compiled as expected.

BZ#818655

Previously, **OpenMotif** did not detect certain keystrokes, such as Home, Insert, Del, PgUp, PgDn on the keypad if the NumLock key was not engaged. This was caused by **Motif** overriding the existing keycode-to-keysym routine for its own virtual keysyms. As a result, the **XmTranslateKey()** function substituted the shifted keysym when it should not have. After this update, disengaging the NumLock key does not affect the detection of the aforementioned keystrokes.

BZ#864409

Previously, using the **XmList** widget in **Openmotif** to view log output from an application was obstructed by a very slow performance. This was due to the **XmListSetPos()** function, which is used to scroll to the end of the list, being too slow. With this update, a patch has been provided to fix the code and the performance problem has been resolved.

BZ#867792

Before this update, **OpenMotif** was missing certain strings on the Label Widget. This update adds the missing strings which are now displayed on the Label Widget.

BZ#880914

Previously, **OpenMotif** displayed its frame too large in size. After updating and counting children on the form, **OpenMotif** updated and repainted the form but it took extra space after replacing the children. With this update, the frame takes up only the required space.

BZ#980577

Previously, 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 scenario described.

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

4.73. openscap

4.73.1. RHEA-2013:1320 — openscap bug fix and enhancement update

Updated openscap packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5

OpenSCAP is an open source project, which enable integration of the SCAP line of standards. Security Content Automation Protocol (SCAP) is a line of standards managed by the National Institute of Standards and Technology (NIST). It was created to provide a standardized approach to maintaining the security of enterprise systems, such as automatically verifying presence of patches, checking system security configuration settings, and examining systems for signs of compromise.

Note

The openscap packages have been upgraded to upstream version 0.9.11, which provides a number of bug fixes and enhancements over the previous version. Among other changes, this update adds the following enhancement:

This update adds support for the National Institute of Standards and Technology's (NIST) SCAP 1.2 standard, so that all content, such as the following, is correctly supported: the Red Hat Enterprise Linux 5 Security Technical Implementation Guide (STIG); The United States Government Configuration Baseline (USGCB); and Red Hat Security Advisory content. (BZ#871120)

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

4.74. openssl

4.74.1. RHSA-2013:0587 — Moderate: openssl security update

Updated openssl packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having 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.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols, as well as a full-strength, general purpose cryptography library.

Security Fixes

CVE-2013-0169

It was discovered that OpenSSL leaked timing information when decrypting TLS/SSL and DTLS protocol encrypted records when CBC-mode cipher suites were used. A remote attacker could possibly use this flaw to retrieve plain text from the encrypted packets by using a TLS/SSL or DTLS server as a padding oracle.

CVE-2013-0166

A NULL pointer dereference flaw was found in the OCSP response verification in OpenSSL. A malicious OCSP server could use this flaw to crash applications performing OCSP verification by sending a specially-crafted response.

CVE-2012-4929

It was discovered that the TLS/SSL protocol could leak information about plain text when optional compression was used. An attacker able to control part of the plain text sent over an encrypted TLS/SSL connection could possibly use this flaw to recover other portions of the plain text.

Note: This update disables zlib compression, which was previously enabled in OpenSSL by default. Applications using OpenSSL now need to explicitly enable zlib compression to use it.

Bug Fix

BZ#839735

It was found that OpenSSL read certain environment variables even when used by a privileged (setuid or setgid) application. A local attacker could use this flaw to escalate their privileges. No application shipped with Red Hat Enterprise Linux 5 and 6 was affected by this problem. (BZ#839735)

All OpenSSL users should upgrade to these updated packages, which contain backported patches to resolve these issues. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

4.75. openswan

4.75.1. RHSA-2013:0827 — Important: openswan security update

Updated openswan packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

Openswan is a free implementation of Internet Protocol Security (IPsec) and Internet Key Exchange (IKE). IPsec uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. When using Opportunistic Encryption, Openswan's pluto IKE daemon requests DNS TXT records to obtain public RSA keys of itself and its peers.

Security Fix

CVE-2013-2053

A buffer overflow flaw was found in Openswan. If Opportunistic Encryption were enabled ("oe=yes" in "/etc/ipsec.conf") and an RSA key configured, an attacker able to cause a system to perform a DNS lookup for an attacker-controlled domain containing malicious records (such as by sending an email that triggers a DKIM or SPF DNS record lookup) could cause Openswan's pluto IKE daemon to crash or, potentially, execute arbitrary code with root privileges. With "oe=yes" but no RSA key configured, the issue can only be triggered by attackers on the local network who can control the reverse DNS entry of the target system. Opportunistic Encryption is disabled by default.

This issue was discovered by Florian Weimer of the Red Hat Product Security Team.

All users of openswan are advised to upgrade to these updated packages, which contain backported patches to correct this issue. After installing this update, the ipsec service will be restarted automatically.

4.76. Oracle Java SE 6

4.76.1. RHSA-2013:0570 — Low: Oracle Java SE 6 - notification of end of public updates

Oracle Java SE 6 will no longer receive updates after February 28, 2013. The java-1.6.0-sun packages on the Red Hat Enterprise Linux 5 and 6 Supplementary media and Supplementary Red Hat Network (RHN) channels are affected.

Oracle Java SE 6 will no longer receive updates after February 28, 2013. The Oracle Java SE 6 packages on the Red Hat Enterprise Linux 5 and 6 Supplementary media and Red Hat Network (RHN) channels will continue to be available after February 28, 2013.

Red Hat will continue to provide these packages only as a courtesy to customers. Red Hat will not provide updates to these packages after this date.

Red Hat recommends that customers using Oracle Java SE 6 choose one of the following alternative Java implementations:

- OpenJDK 6, which is available and supported in Red Hat Enterprise Linux 5 and 6.
- IBM's Java SE 6, which is available on the Red Hat Enterprise Linux 5 and 6 Supplementary media and Supplementary RHN channels through September 2017.
- OpenJDK 7, which is available and supported in Red Hat Enterprise Linux 5 and 6.
- IBM's Java SE 7, which is available on the Red Hat Enterprise Linux 5 and 6 Supplementary media and Supplementary RHN channels.
- Oracle Java SE 7, which is available today on the Red Hat Enterprise Linux 5 and 6 Supplementary media and Supplementary RHN channels.

In the near future, Red Hat will provide updated packages for these alternative Java implementations and detailed instructions describing how to configure a new default Java runtime environment.

4.76.2. RHSA-2013:0666 — Low: Oracle Java SE 6 - notification of end of public updates

Updates to the java-1.6.0-sun packages that disable the Java Web Browser Plug-in and Web Start included in these packages. As a result, customers who rely on Java-based browser applets may need to re-configure their browser to use one of the Java implementations listed in the Solution section below.

Oracle Java SE version 6 includes the Oracle Java Runtime Environment and the Oracle Java Software Development Kit.

Oracle Java SE 6 will not receive updates after February 28, 2013. The Oracle Java SE 6 packages on the Red Hat Enterprise Linux 5 and 6 Supplementary media and in Red Hat Network (RHN) channels will continue to be available.

Red Hat will continue to provide these packages only as a courtesy to customers. Red Hat will not provide updates to these packages after this date.

Once customers update their system by installing the packages associated with this advisory, the Oracle Java Web Plug-in will be disabled. As a result, customers who rely on Java-based browser applets may need to re-configure their browser to use one of the Java implementations listed in the Solution section below.

All users of java-1.6.0-sun are advised to upgrade to these updated packages.

Red Hat recommends that customers using Oracle Java SE 6 choose one of the following alternative Java implementations:

- OpenJDK 6, which is available and supported in Red Hat Enterprise Linux 5 and 6.
- IBM's Java SE 6, which is available on the Red Hat Enterprise Linux 5 and 6 Supplementary media and Supplementary RHN channels through September 2017.
- OpenJDK 7, which is available and supported in Red Hat Enterprise Linux 5 and 6.
- IBM's Java SE 7, which is available on the Red Hat Enterprise Linux 5 and 6 Supplementary media and Supplementary RHN channels.
- Oracle Java SE 7, which is available today on the Red Hat Enterprise Linux 5 and 6 Supplementary media and Supplementary RHN channels.

Please refer to Red Hat Knowledge solution 314713 for information on how to install and configure any of these Java implementations. This solution also describes how customers who rely on Java-based browser applets can re-configure their Java Web Plug-in.

4.77. pcre

4.77.1. RHBA-2013:1298 — pcre bug fix update

Updated pcre packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The pcre packages provide the Perl-compatible regular expression (PCRE) library.

Bug Fixes

BZ#669413

A previous update enabled Unicode properties to support \p{..}, \P{..}, and \X escape sequences. However, compiling certain regular expressions which contained extended classes under a non-UTF-8 PCRE mode failed due to the compilation entering an infinite loop. This has been fixed in this update so that compiling such regular expressions completes as expected.

BZ#859959

Using the pcregrep tool with -M (mutli-line match) and -v (inverse match) options caused the pcregrep tool to loop infinitely. With this update, the pcregrep multi-line loop logic has been fixed to advance in the input stream properly if inverted matching is requested, and it is now possible to use the "pcregrep -Mv" command.

BZ#866520

Previously, matching a regular expression with Unicode properties in a non-UTF-8 mode against a string with non-ASCII characters, caused an unexpected termination with a segmentation fault in the PCRE library. This update fixes back-tracking in non-UTF-8 mode, and the PCRE library no longer crashes in the aforementioned scenario.

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

4.78. perl

4.78.1. RHSA-2013:0685 — Moderate: perl security update

Updated perl packages that fix multiple security issues now available for Red Hat Enterprise Linux 5 and 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.

Perl is a high-level programming language commonly used for system administration utilities and web programming.

Security Fixes

CVE-2012-5195

A heap overflow flaw was found in Perl. If a Perl application allowed user input to control the count argument of the string repeat operator, an attacker could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2013-1667

A denial of service flaw was found in the way Perl's rehashing code implementation, responsible for recalculation of hash keys and redistribution of hash content, handled certain input. If an attacker supplied specially-crafted input to be used as hash keys by a Perl application, it could cause excessive memory consumption.

CVE-2012-5526

It was found that the Perl CGI module, used to handle Common Gateway Interface requests and responses, incorrectly sanitized the values for Set-Cookie and P3P headers. If a Perl application using the CGI module reused cookies values and accepted untrusted input from web browsers, a remote attacker could use this flaw to alter member items of the cookie or add new items.

CVE-2012-6329

It was found that the Perl Locale::Maketext module, used to localize Perl applications, did not properly handle backslashes or fully-qualified method names. An attacker could possibly use this flaw to execute arbitrary Perl code with the privileges of a Perl application that uses untrusted Locale::Maketext templates.

Red Hat would like to thank the Perl project for reporting CVE-2012-5195 and CVE-2013-1667. Upstream acknowledges Tim Brown as the original reporter of CVE-2012-5195 and Yves Orton as the original reporter of CVE-2013-1667.

All Perl users should upgrade to these updated packages, which contain backported patches to correct these issues. All running Perl programs must be restarted for this update to take effect.

4.78.2. RHBA-2013:1296 — perl bug fix update

Updated perl packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The perl packages provide the high-level programming language Perl, which is commonly used for system administration utilities and web programming.

Bug Fixes

BZ#800340

Previously, calling the POSIX::strftime() function resulted in a string longer than 64 bytes and, consequently, to a memory leak. This led to memory loss. With this update, memory allocation in the POSIX::strftime() function implementation has been changed to reallocate memory, which prevents memory loss from occurring.

BZ#848156

Previously, certain modules using Perl scripts, which use the overload() function in a specific way, were impacted by a performance regression. Consequently, users could observe slower operation of such scripts after an upgrade of the perl packages. A patch has been applied to prevent this bug.

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

4.79. php

4.79.1. RHSA-2013:1049 — Critical: php security update

Updated php packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fix

CVE-2013-4113

A buffer overflow flaw was found in the way PHP parsed deeply nested XML documents. If a PHP application used the xml_parse_into_struct() function to parse untrusted XML content, an attacker able to supply specially-crafted XML could use this flaw to crash the application or, possibly, execute arbitrary code with the privileges of the user running the PHP interpreter.

All php users should upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.80. php53

4.80.1. RHSA-2013:1307 — Moderate: php53 security, bug fix and enhancement update

Updated *php53* packages that fix several security issues, several bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

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.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fixes

CVE-2006-7243

It was found that PHP did not properly handle file names with a NULL character. A remote attacker could possibly use this flaw to make a PHP script access unexpected files and bypass intended file system access restrictions.

CVE-2011-1398

It was found that PHP did not check for carriage returns in HTTP headers, allowing intended HTTP response splitting protections to be bypassed. Depending on the web browser the victim is using, a remote attacker could use this flaw to perform HTTP response splitting attacks.

CVE-2013-4248

A flaw was found in PHP's SSL client's hostname identity check when handling certificates that contain hostnames with NULL bytes. If an attacker was able to get a carefully crafted certificate signed by a trusted Certificate Authority, the attacker could use the certificate to conduct man-in-the-middle attacks to spoof SSL servers.

CVE-2012-2688

An integer signedness issue, leading to a heap-based buffer underflow, was found in the PHP scandir() function. If a remote attacker could upload an excessively large number of files to a directory the scandir() function runs on, it could cause the PHP interpreter to crash or, possibly, execute arbitrary code.

CVE-2012-0831

It was found that PHP did not correctly handle the magic_quotes_gpc configuration directive. This could result in magic_quotes_gpc input escaping not being applied in all cases, possibly making it easier for a remote attacker to perform SQL injection attacks.

CVE-2013-1643

It was found that the PHP SOAP parser allowed the expansion of external XML entities during SOAP message parsing. A remote attacker could possibly use this flaw to read arbitrary files that are accessible to a PHP application using a SOAP extension.

Bug Fixes

BZ#864954

A PHP script that is using the Open Database Connectivity (ODBC) interfaces could enter a deadlock if the maximum execution time period expires while it is executing an SQL statement. This occurs because the execution timer uses a signal and the invoked ODBC functions are not reentrant. This update modifies the underlying code so the deadlock is less likely to occur.

BZ#869691

Previously, the **`setDate()`**, **`setISODate()`** and **`setTime()`** functions did not work correctly when the corresponding **`DateTime`** object was created from the timestamp. This bug has been fixed and the aforementioned functions now work properly.

BZ#869693

Previously, a segmentation fault occurred when PDOStatement was reused after failing due to the NOT NULL integrity constraint. This occurred when the **pdo_mysql** driver was in use. With this update, a patch has been introduced to fix this issue.

BZ#869694

Previously, the **`strcpy()`** function, called by the **`extract_sql_error_rec()`** function in the **unixODBC** API, overwrote a guard variable in the **`pdo_odbc_error()`** function. Consequently, a buffer overflow occurred. This bug has been fixed and the buffer overflow no longer occurs.

BZ#869697

Previously, the Fileinfo extension did not use the **`stat`** interface from the stream wrapper. Consequently, when used with a stream object, the Fileinfo extension failed with the following message:

```
file not found
```

With this update, the Fileinfo extension has been fixed to use the stream wrapper's stat interface. Note that only the **`file`** and **`phar`** stream wrappers support the stat interface in PHP 5.3.3.

BZ#892695

Under certain circumstances, the **`$this`** object became corrupted, and behaved as a non-object. A test with the **`is_object()`** function remained positive, but any attempt to access a member variable of **`$this`** resulted in the following warning:

```
Notice: Trying to get property of non-object
```

This behavior was caused by a bug in the **Zend garbage collector**. With this update, a patch has been introduced to fix garbage collection. As a result, **`$this`** no longer becomes corrupted.

BZ#951075

In certain cases, PHP incorrectly triggered the user **`error_handler()`** function. As a consequence, while evaluating this function, a segmentation fault occurred. With this update, **`error_handler()`** is triggered correctly. As a result, the segmentation fault no longer occurs.

BZ#951076

Previously, when the **`destroy_zend_class()`** terminated unexpectedly, a double free error occurred. With this update, the underlying source code has been modified to prevent the double free error.

BZ#951413

Previously, when the **copy()** function terminated unexpectedly, the resulting error was not reported. Consequently, data loss could occur. This bug has been fixed, and failed **copy()** is now acknowledged properly, which reduces the risk of data loss.

Enhancement

BZ#837044

With this update, a *php(language)* virtual provide for specifying the PHP language version has been added to the *php* package.

Users of PHP are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.80.2. RHSA-2013:1050 — Critical: php53 security update

Updated php53 packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

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

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fix

CVE-2013-4113

A buffer overflow flaw was found in the way PHP parsed deeply nested XML documents. If a PHP application used the xml_parse_into_struct() function to parse untrusted XML content, an attacker able to supply specially-crafted XML could use this flaw to crash the application or, possibly, execute arbitrary code with the privileges of the user running the PHP interpreter.

All php53 users should upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.81. pidgin

4.81.1. RHSA-2013:0646 — Moderate: pidgin security update

Updated pidgin packages that fix three security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having 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.

Pidgin is an instant messaging program which can log in to multiple accounts on multiple instant messaging networks simultaneously.

Security Fixes

CVE-2013-0272

A stack-based buffer overflow flaw was found in the Pidgin MXit protocol plug-in. A malicious server or a remote attacker could use this flaw to crash Pidgin by sending a specially-crafted

HTTP request.

CVE-2013-0273

A buffer overflow flaw was found in the Pidgin Sametime protocol plug-in. A malicious server or a remote attacker could use this flaw to crash Pidgin by sending a specially-crafted username.

CVE-2013-0274

A buffer overflow flaw was found in the way Pidgin processed certain UPnP responses. A remote attacker could send a specially-crafted UPnP response that, when processed, would crash Pidgin.

Red Hat would like to thank the Pidgin project for reporting the above issues. Upstream acknowledges Daniel Atallah as the original reporter of CVE-2013-0272.

All Pidgin users should upgrade to these updated packages, which contain backported patches to resolve these issues. Pidgin must be restarted for this update to take effect.

4.82. piranha

4.82.1. RHBA-2013:0262 — piranha bug fix update

Updated piranha packages are now available for Red Hat Enterprise Linux 5 Extended Update Support.

Piranha provides high-availability and load balancing services for Red Hat Enterprise Linux. The piranha packages contain various tools to administer and configure the Linux Virtual Server (LVS), as well as the heartbeat and failover components. LVS is a dynamically-adjusted kernel routing mechanism that provides load balancing, primarily for Web and FTP servers.

Bug Fix

BZ#911287

Previously, the pulse daemon did not correctly detect when the lvsd daemon had been terminated. As a result, the pulse daemon did not trigger a failover. With this update, the pulse daemon correctly detects when lvsd has been terminated and, if a backup director is configured and active, will result in a failover.

All users of piranha are advised to upgrade to these updated packages, which fixes this bug.

4.83. policycoreutils

4.83.1. RHBA-2013:1344 — policycoreutils bug fix update

Updated policycoreutils packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The policycoreutils packages contain essential utilities required for basic operation of SELinux.

Bug Fixes

BZ#949061

Due to unsupported locale, the semanage commands failed with the following traceback error message during the "add" and "delete" operations:

locale.Error: unsupported locale setting

This update corrects the code, and the semanage utility no longer fails in the described scenario.

BZ#723950

Due to missing support for the ext4 file system, the fixfiles utility did not work on such file systems. This update adds the support for ext4 and fixfiles now works properly in the described scenario.

BZ#805022

Prior to this update, the genhomedircon script created duplicate SELinux context template entries in the /etc/selinux/targeted/contexts/files/file_contexts.homedirs file, when /export/home/ was defined as the default home directory location for new users and /export/home/ existed on the file system. Consequently, error messages were returned to the /var/log/messages file. A patch has been provided to fix this bug and only one set of SELinux context template entries is now maintained in the /etc/selinux/targeted/contexts/files/file_contexts.homedirs file.

BZ#623708

Previously, the utmp utility never triggered a change on the first user who logged in to the system. Consequently, the restorecond daemon sometimes failed to update context on files when only one user was logged in. A patch has been provided to fix utmp and restorecond now works as expected in the described scenario.

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

4.83.2. RHBA-2013:0760 — policycoreutils bug fix update

Updated policycoreutils packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The policycoreutils packages contain the core utilities that are required for the basic operation of a Security-Enhanced Linux (SELinux) system and its policies. These utilities include load_policy to load policies, setfiles to label file systems, newrole to switch roles, and run_init to run /etc/init.d/ scripts in their proper context.

Bug Fix

BZ#953167

Previously, semanage commands failed with the following traceback error message during add and delete operations:

locale.Error: unsupported locale setting

This was due to an error in the source code of the semanage command. This update corrects the code, and semanage commands no longer fail in the described scenario.

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

4.84. poppler

4.84.1. RHBA-2013:1128 — poppler bug fix update

Updated poppler packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

Poppler is a Portable Document Format (PDF) rendering library, used by applications such as Evince.

This update fixes the following bugs:

* The addition of support for AES-encoded PDF documents introduced the following bug:

Bug Fixes

BZ#990096

The addition of support for AES-encoded PDF documents introduced the when exporting a password-protected PDF to Postscript using poppler, images were exported in their encoded form, making the resulting Postscript file unusable. This also affected printing of such PDFs as the same bug affected the printing logic. With this update, images in a password-protected PDF are properly decoded before the PDF is exported to Postscript, and printing of such PDFs no longer fails.

BZ#990097

Due to missing initialization of certain variables, previous versions of poppler functioned incorrectly when processing values of these uninitialized variables. With this update, the underlying source code has been modified to address this issue.

All users who require poppler are advised to upgrade to these updated packages, which fix these bugs.

4.85. procps

4.85.1. RHBA-2013:1338 — procps bug fix update

Updated procps packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

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#785169

In some cases, for example, with VMware ESX guests and C-states/CPU switched off, the sum of idle and non-idle ticks returned by the kernel might have been zero. Consequently, this could have caused arithmetic exceptions. With this update, the zero sum is evaluated as if there were idle cycles, and the arithmetic exceptions no longer appear.

BZ#869140

Previously, there was a misleading description of the SWAP field in the "top" tool. The Red Hat Enterprise Linux version 5 kernel does not export the VmSwap field in the /proc/#PID/status file, and therefore it was not possible to get the size of the swapped out portion of the task's address space. In the case of Red Hat Enterprise Linux 5, the SWAP field displayed by the "top" tool represented the non-resident portion of the task's address space instead. With this update, the SWAP description has been changed from "Swapped size" to "Non-resident size."

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

4.86. python-rhsm

4.86.1. RHBA-2013:1331 — python-rhsm bug fix and enhancement update

Updated python-rhsm packages that fix two bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The python-rhsm package is a library for communicating with the REST interface of the Red Hat Unified Entitlement Platform. It provides access to the Subscription Management tools which help users to determine which products are installed on their machines and the subscriptions their machines are receiving.

This update also fixes the following bugs:

Note

The python-rhsm package has been upgraded to upstream version 1.8.17, which provides a number of enhancements over the previous version. (BZ#922029)

This update also fixes the following bugs:

Bug Fixes

BZ#966936

Previously, the subscription-manager package depended on a version of the python-rhsm package that was not included in the previous version of Red Hat Enterprise Linux 5. As a consequence, the installation terminated with the following error:

Error: No module named rhsm.config

With this release, the python-rhsm package has been added to Red Hat Enterprise Linux 5 and dependencies are resolved successfully when installing the subscription-manager package.

BZ#988476

Previously, the user was allowed to set and remove parameters in all three sections of the rhsm.conf file even though the parameters are only used in one section. This confused the user and hindered them from setting the right parameters. This update removes the unnecessary configuration in the subscription-manager configuration module.

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

4.87. rdesktop

4.87.1. RHBA-2013:1367 — rdesktop bug fix update

Updated rdesktop packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The rdesktop packages provide a client for the Remote Desktop Server in Microsoft Windows. The rdesktop client uses the Remote Desktop Protocol (RDP) to remotely present a user's desktop.

Bug Fix

BZ#642554

Prior to this update, the rdesktop client did not handle Windows Server 2008 licenses correctly. As a consequence, rdesktop was not able to connect to Terminal Services on the second connection with the following error message:

"disconnect: Internal licensing error"

This update modifies the underlying code to handle the Windows Server 2008 licenses properly, and rdesktop now connects to Terminal Services as expected.

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

4.88. redhat-release

4.88.1. RHEA-2013:1311 — redhat-release enhancement update for Red Hat Enterprise Linux 5.10

Updated and enhanced redhat-release packages are now available for Red Hat Enterprise Linux 5.10.

The redhat-release packages contain licensing information regarding, and identifies the installed version of, Red Hat Enterprise Linux.

These updated redhat-release packages reflect changes made for the release of Red Hat Enterprise Linux 5.10.

Users of Red Hat Enterprise Linux 5 are advised to upgrade to these updated redhat-release packages.

4.89. redhat-release-notes

4.89.1. RHEA-2013:1341 — redhat-release-notes enhancement update

An updated redhat-release-notes package is now available for Red Hat Enterprise Linux 5.10 as part of ongoing support and maintenance of Red Hat Enterprise Linux 5.

Red Hat Enterprise Linux minor releases are an aggregation of individual enhancement, security and bug fix errata. The Red Hat Enterprise Linux 5.10 Release Notes document the major changes made to the Red Hat Enterprise Linux 5 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.

This package contains the Release Notes for Red Hat Enterprise Linux 5.10.

The online Red Hat Enterprise Linux 5.10 Release Notes, which are located online at https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/5/html/5.10_Release_Notes/index.html, are to be considered the definitive, up-to-date version. Customers with questions about the release are advised to consult the online Release Notes and Technical Notes for their version of Red Hat Enterprise Linux.

Users of Red Hat Enterprise Linux 5 are advised to upgrade to this updated redhat-release-notes package, which adds the updated Release Notes.

4.90. rgmanager

4.90.1. RHBA-2013:1316 — rgmanager bug fix and enhancement update

Updated *rgmanager* packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 5.

The *rgmanager* 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#865462

Previous attempts to use an IPv6 address in the cluster configuration with upper case letters returned an error message. Consequently, this caused attempts to start a cluster service in this manner to fail. With this update, the IP address is set independently of upper or lower case letters, and attempts to start the service with both cases functions as expected.

BZ#869705

Previously, SAP instances started by the SAPInstance cluster resource agent inherited limits on system resources, for example, the maximum number of open file descriptors for a root user. Those limits could not be applied by PAM due to the way that SAP processes were started by the cluster. With this update, SAPInstance resource agent takes limits configured in the /usr/sap/sapservices/ directory into account. If no limits are specified in the /usr/sap/sapservices/ directory, then safe default limits are applied.

BZ#879029

When a service was configured with a recoverable resource, such as nfsclient, a failure of that client correctly triggered the recovery function. However, even if the recovery was successful, rgmanager still stopped and recovered the service. This was caused because the do_status function recorded the rn_last_status function after the first failure, then ran recovery but did not record the new rn_last_status function. This update sets the rn_last_status function to 0 after the resource is recovered. Thus, rgmanager recovers the resource, and leaves the service running afterwards.

BZ#883860

Previously, certain man pages from the rgmanager packages had executable flags set and were installed with mode 0755, which was incorrect. Currently, the man pages are correctly installed with mode 0644, which corrects this issue.

BZ#889098

When the /etc/cluster/cluster.conf file was modified and distributed to the other nodes using the ccs_tool update, the file was changed on all the nodes, but the change was not applied in the cluster. This happened because a bug in the code caused a new configuration event to be queued when a configuration change was detected while processing configuration event, which caused even more events to be queued, possibly infinitely. Also, under certain circumstances, rgmanager issued a call to get cluster information without proper initialization of internal structures. With this update, the aforementioned problems has been fixed. Each configuration update event is queued only once and configuration changes are now applied in the cluster as expected.

BZ#907898

Due to an incorrect SELinux context in the /var/lib/nfs/statd/sm/ directory, the rpc.statd daemon was unable to start. This problem only happened if the cluster included NFS mounts, and therefore the /var/lib/nfs/statd/sm/ directory contained files. This update passes the "-Rdpf" instead of "-af" flags to the "cp" command when copying files to the /var/lib/nfs/statd/sm/ directory, so that the SELinux context is inherited from the target directory, and not preserved from the files being copied.

BZ#909459

Previously, in central processing mode, rgmanager did not handle certain inter-service dependencies correctly. If a service was dependent on another service that ran on the same cluster node, the dependent service became unresponsive during the service failover and remained in the recovering state. With this update, rgmanager has been modified to check a service state during

failover and stop the service if it is dependent on the service that is failing over. Resource Group Manager then attempts to start this dependent service on other nodes.

BZ#962376

When using High Availability Logical Volume Management agents (HA-LVM), failure of some of the physical volumes (PV) in the volume group (VG) resulted in the agent calling "vgreduce --removemissing --force [vg]", thus removing the missing PVs and any logical volumes (LV) that were on it. While this was helpful in the case of recovering from the loss of a mirror leg, when only using linear LVs, it is problematic, especially if another node is having no trouble accessing the storage. This update adds the "--mirrorsonly" option to the "vgreduce --removemissing" calls in the LVM agents, and HA-LVM only removes missing PVs on stop when they belong to mirrors.

BZ#968322

A general protection fault in the malloc_consolidate function caused rgmanager to terminate unexpectedly with a segmentation fault during a status check. This update fixes some instances where a very unlikely NULL pointer dereference could occur, and rgmanager no longer crashes in this situation.

Enhancements

BZ#670024

Previous versions of the Oracle Resource Agent were only tested against Oracle 10. With this update, support for the Oracle Database 11g has been added to the oracledb, orainstance, and oralistener resource agents.

BZ#841142

This update fixes a non-critical typing error in the ASEHAagent.sh resource agent.

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

4.90.2. RHBA-2013:0559 — rgmanager bug fix update

Updated rgmanager packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The rgmanager packages contain the Red Hat Resource Group Manager, which allows the ability to create and manage high-availability server applications in the event of system downtime.

Bug Fix

BZ#912625

Previously, in central processing mode, rgmanager did not handle certain inter-service dependencies correctly. If a service was dependent on another service that ran on the same cluster node, the dependent service became unresponsive during the service failover and remained in the recovering state. With this update, rgmanager has been modified to check a service state during failover and stop the service if it is dependent on the service that is failing over. Resource Group Manager then attempts to start this dependent service on other nodes.

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

4.90.3. RHBA-2013:0892 — rgmanager bug fix update

Updated rgmanager packages that fix a bug are now available for Red Hat Enterprise Linux 5.

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 Fix

BZ#967456

Previously, the NFS resource agents preserved SELinux context when copying files to the /var/lib/nfs/sm/ directory. As a result, files that were copied did not inherit the SELinux context of /var/lib/nfs/sm/, causing AVC denial messages to be returned. These messages prevented proper operation of the resource agents. This bug has been fixed and the NFS resource agents no longer preserve the SELinux context of files copied to /var/lib/nfs/sm/.

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

4.90.4. RHEA-2013:0852 — rgmanager enhancement update

Updated rgmanager packages that add one enhancement are now available for Red Hat Enterprise Linux 5.

The rgmanager packages contain the Red Hat Resource Group Manager, which allows users to create and manage high-availability server applications in the event of system downtime.

Enhancement

BZ#964991

With this update, support for Oracle Database 11g has been added to the oracledb, orainstance, and oralistener resource agents.

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

4.90.5. RHBA-2013:1267 — rgmanager bug fix update

Updated rgmanager packages that fix one bug are now available for Red Hat Enterprise Linux 5.

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 Fix

BZ#1004482

Previously, if a device failed in a non-redundant (i.e. not mirror or RAID) logical volume that was controlled by HA-LVM, the entire logical volume could be automatically deleted from the volume group. Now, if a non-redundant logical volume suffers a device failure, HA-LVM fails to start the service rather than forcing the removal of failed PVs from the volume group, thus fixing the bug.

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

4.90.6. RHBA-2013:1281 — rgmanager bug fix update

Updated rgmanager packages that fix one bug are now available for Red Hat Enterprise Linux 5.

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 Fix

BZ#1009245

Previously, the cluster services file system failed over from one node to another if the /tmp directory filled up. A patch has been provided to fix this bug and cluster services no longer fail over.

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

4.91. rhn-client-tools

4.91.1. RHBA-2013:1328 — rhn-client-tools bug fix and enhancement update

Updated rhn-client-tools packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

Red Hat Network Client Tools provide programs and libraries that allow the system to receive software updates from Red Hat Network (RHN).

Bug Fixes

BZ#873531

When registering a system using certain locales (for example, Simplified Chinese or Japanese), and the user entered an invalid username and password, the firstboot application displayed an erro message. However, missing line breaks caused the dialog box to become too large. This update adds line breaks in the error message, so that the dialog box is of reasonable size.

BZ#882933

Previously, when using the rhn_register tool in text user interface (TUI) mode, an invalid link was displayed on the "Setting up software updates" page. The link has been corrected and now points to the correct location.

BZ#886342

Previously, if the server's SSL certificate validation failed, attempting to register the system to RHN Classic failed with a traceback. With this update, a more useful error message is displayed instead of the traceback in the described scenario.

BZ#949645

Red Hat Network (RHN) Proxy did not work properly if separated from a parent by a slow network. Consequently, users who attempted to download larger repodata files and RPM packages experienced timeouts. This update changes both RHN Proxy and Red Hat Enterprise Linux RHN Client to allow all communications to honor a configured timeout value for connections.

Enhancement

BZ#949617

This update adds a function to get the number of physical CPU sockets in a managed system from Red Hat Network Satellite, the systems-management platform, via an API call.

Users of rhn-client-tools are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.92. rhnlib

4.92.1. RHBA-2013:1326 — rhnlib bug fix update

An updated rhnlib package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The rhnlib package consists of a collection of Python modules used by the Red Hat Network (RHN) software.

Bug Fix

BZ#951590

Red Hat Network (RHN) Proxy did not work properly if separated from a parent by a slow network. Consequently, users who attempted to download larger repodata files and RPM packages experienced timeouts. This update changes both RHN Proxy and Red Hat Enterprise Linux RHN Client to allow all communications to honor a configured timeout value for connections.

Users of rhnlib are advised to upgrade to this updated package, which fixes this bug.

4.93. rpm

4.93.1. RHBA-2013:1297 — rpm bug fix update

Updated rpm packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The RPM Package Manager (RPM) is a command-line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

Bug Fixes

BZ#648516

Previously, the package size was recorded incorrectly for packages built on big-endian platforms (PowerPC or IBM S/390), which would show up in Anaconda as packages having zero bytes. With this update, package sizes are correctly recorded on all platforms, but older packages built with the flawed versions of RPM still show incorrect sizes.

BZ#671194

Previously, when multiple packages failed to update correctly, the failed packages could get removed from the system entirely. With this update, the rpm and yum utilities can handle multiple failures during updates without unexpected package removals.

BZ#706935

Previously, attempts to install packages with a large number of files (approximately 80,000 or more), could have caused RPM to terminate unexpectedly with a segmentation fault due to the RPM header exceeding its upper limit. This update increases the header limit so RPM is able to handle larger package installs, and crashes no longer occur in the described scenario.

BZ#716853

A new size check recently added to rpmbuild caused rpmbuild to display an error message and exit if the contents of the RPM file exceeded 2GB in size. This size check was performed prior to the elimination of duplicate files, however, in some cases it was possible for rpmbuild to exit with a ">2GB" warning even if the contents of the RPM file were actually smaller than 2GB. With this update, the size check for rpmbuild is expanded, and it is possible to build RPM files larger than 2GB.

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

4.93.2. RHBA-2013:0558 — rpm bug fix update

Updated rpm packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The RPM Package Manager (RPM) is a command-line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages.

Bug Fix

BZ#906019

Previously, when updating packages with the rpm or yum utilities, users experienced multiple failures and the failed packages were removed from the system entirely. With this update, the rpm and yum utilities can handle multiple failures during updates without unexpected package removals.

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

4.94. ruby

4.94.1. RHSA-2013:1090 — Moderate: ruby security update

Updated ruby packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to do system management tasks.

Security Fix

CVE-2013-4073

A flaw was found in Ruby's SSL client's hostname identity check when handling certificates that contain hostnames with NULL bytes. An attacker could potentially exploit this flaw to conduct man-in-the-middle attacks to spoof SSL servers. Note that to exploit this issue, an attacker would need to obtain a carefully-crafted certificate signed by an authority that the client trusts.

All users of Ruby are advised to upgrade to these updated packages, which contain backported patches to resolve this issue.

4.94.2. RHSA-2013:0611 — Moderate: ruby security update

Updated ruby packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

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

Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to do system management tasks.

Security Fix

CVE-2013-1821

It was discovered that Ruby's REXML library did not properly restrict XML entity expansion. An attacker could use this flaw to cause a denial of service by tricking a Ruby application using REXML to read text nodes from specially-crafted XML content, which will result in REXML consuming large amounts of system memory.

All users of Ruby are advised to upgrade to these updated packages, which contain backported patches to resolve this issue.

4.95. s390utils

4.95.1. RHBA-2013:1335 — s390utils bug fix update

Updated *s390utils* packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The *s390utils* packages contain a set of user space utilities for Linux on IBM System z architecture.

Bug Fixes

BZ#783162

Prior to this update, in some cases, Initial Program Load (IPL) did not work after calling the **`zipl`** boot loader. Consequently, incorrect bootmap could be used during initialization and an incorrect kernel could be loaded. This update adds the fsync() function, which ensures that all correct and necessary data is written to disk.

BZ#787685

Previously, the **`qethconf`** tool for configuring network interfaces worked in the case-sensitive manner. Consequently, **`qethconf`** was searching for non-existent match of IPv6 addresses when these were written in capital letters. With this update, **`qethconf`** handles IPv6 addresses as expected and IPv6 searches are now case-insensitive.

BZ#809462

Due to an incomplete monitor record header for the stop record, unused monitor records of stopped processes were not halted correctly and continued to show up in the z/VM hypervisor monitor stream. The header data has been completed, thus preventing the stoppage of unused records.

BZ#820262

Prior to this update, the buffer used for writing error messages was too small. As a consequence, when trying to write changes to a read-only device using the **`fdasd`** program, the buffer overflew. This update adds **`fprintf()`** function, which writes directly to the **`stderr`** stream without the buffer. As a result, buffer overflows no longer occur.

BZ#820263

Previously, the lsdasd(8) manual page did not contain the **`-b`** option. In adddition, the **`lsdasd`** command returned "1" instead of "0" output, when the **`-h`** option was specified. The missing **`-b`** option has been added to the manual page and the outputs for the **`-h`** option have been correctly specified, thus fixing the bug.

BZ#857816

When the **`zipl`** boot loader was run on the Direct Access Storage Device with the Fixed Block Access format (FBA DASD), previously initialized Physical Volume (PV) on the partition could no longer be recognized by LVM. With this update, the cache for the disk and partition block devices

longer be recognized by LVM. With this update, the cache for the disk and partition block devices is flushed before installing the **IPL record**, thus fixing the bug.

BZ#837305

Previously, a Small Computer System Interface (SCSI) device was not available immediately after registration. As a consequence, the **lsluns** script failed to recognize the LUN0 and WLUN attachment with the following error message:

```
Cannot attach WLUN / LUN0 for scanning
```

To fix this bug, multiple checks for SCSI registration with the LUN0 and WLUN attached via the **unit_add** option have been added and SCSI mid layer now successfully completes the SCSI device registration.

BZ#906837

The **ziorep_config** configuration report is supposed to ignore SCSI disks that are not part of the **multipath** device mapper when creating the **multipath** mapper report. Previously , **ziorep_config** failed to correctly ignore SCSI disks which caused **get_line()** function to return **n/a** output if a **sysfs** attribute did not exist. This output is stored in the **mp_dev_mm** hash key so its value could not be used in a check for being undefined. With this update, the **mp_dev** hash field remains undefined, if no **multipath** device is found, thus fixing the bug.

BZ#828128

Previously, the **lsluns** script checked for sg kernel subsystem functionality before scanning available LUNs or showing attached LUNs. Consequently, **lsluns** failed to list available LUNs and to show attached LUNs with the **-a** option. Early kernel subsystem availability check has been removed to fix this bug.

BZ#851096

Previously, the **/etc/profile.d/s390.sh** script contained incorrect equation syntax. As a consequence, when the **zsh** shell on s390x architecture was started, the following error message appeared:

```
/etc/profile.d/s390.sh:4: = not found
```

The script has been fixed and no error messages are now returned.

Users of *s390utils* are advised to upgrade to these updated packages, which provide numerous bug fixes.

4.96. samba3x

4.96.1. RHSA-2013:1310 — Moderate: samba3x security and bug fix and update

Updated *samba3x* packages that fix several security issues and several bugs are now available for Red Hat Enterprise Linux 5.

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

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.

Security Fixes

CVE-2013-0213

It was discovered that the Samba Web Administration Tool (SWAT) did not protect against being opened in a web page frame. A remote attacker could possibly use this flaw to conduct a clickjacking attack against SWAT users or users with an active SWAT session.

CVE-2013-0214

A flaw was found in the Cross-Site Request Forgery (CSRF) protection mechanism implemented in SWAT. An attacker with the knowledge of a victim's password could use this flaw to bypass CSRF protections and conduct a CSRF attack against the victim SWAT user.

CVE-2013-4124

An integer overflow flaw was found in the way Samba handled an Extended Attribute (EA) list provided by a client. A malicious client could send a specially crafted EA list that triggered an overflow, causing the server to loop and reprocess the list using an excessive amount of memory.

Note

This issue does not affect the default configuration of samba server.

Red Hat would like to thank the Samba project for reporting CVE-2013-0213 and CVE-2013-0214. Upstream acknowledges Jann Horn as the original reporter of CVE-2013-0213 and CVE-2013-0214.

Bug Fixes

BZ#862872

When a domain controller (DC) was rebuilding the System Volume (Sysvol) directory, it disabled the Net Logon service. Even if another working DC was available, users were not able to log in until the rebuilding was finished and, as a consequence, error messages were returned. With this update, when an attempt to open the Net Logon connection fails two times, users are able to log in using another DC without any errors.

BZ#869295

Previously, when the **`Windbind`** daemon (**`windbindd`**) authenticated Active Directory (AD) users, it used 100% of the CPU and stopped the user authentication. This update provides a patch to fix this bug and **`windbindd`** now works as expected.

BZ#883861

When the **`Windbind`** daemon (**`windbindd`**) was not able to establish a Server Message Block (SMB) connection to a domain controller (DC), it retried three times in a row, waited for some time and tried to connect again. Because the socket that **`windbindd`** had opened to connect to DC was not closed, **`windbindd`** leaked three sockets each time it tried to establish the connection, which led to depletion of the available sockets. With this update, a patch has been provided to fix this bug and the sockets are now closed correctly so that **`windbindd`** no longer leaks sockets in the described scenario.

BZ#905071

Previously, guest users did not have the correct token allowing write operations on a writable guest share. Consequently, such users were not able to create or write to any files within the share. With

this update, a patch has been provided to fix this bug and the guest users are able to write to or create any files within the writable share as expected.

Note

The ***share*** parameter is obsolete and the security mode should be set to ***user***.

BZ#917564

The Samba service contains the user name mapping optimization that stores an unsuccessful mapping so that it is not necessary to traverse the whole mapping file every time. Due to a bug in the optimization, the user name mapping worked only once and then it was overwritten with the unsuccessful one. This update provides a patch to fix this bug and the successful user name mapping is no longer overwritten in the described scenario.

BZ#947999

Due to a bug in the authentication code that forwarded the NTLMv2 authentication challenge to the primary domain controller (PDC), an incorrect domain name was sent from a client. Consequently, the user was not able to log in, because when the domain name was hashed in the second NTLMv2 authentication challenge, the server could not verify the validity of the hash and the access was rejected. With this update, the correct domain name is set by the client to the PDC and the user is able to log in as expected.

BZ#982484

An attempt to execute the **wkssvc_NetWkstaEnumUsers** RPC command without a pointer to the resume handle caused the **smbd** daemon to terminate with a segmentation fault. Consequently, the client was disconnected. With this update, the underlying source code has been adapted to verify that the pointer is valid before attempting to dereference it. As a result, **smbd** no longer crashes in this situation.

All *samba3x* users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the smb service will be restarted automatically.

4.97. scl-utils

4.97.1. RHBA-2013:1303 — scl-utils bug fix update

Updated scl-utils packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The scl-utils packages provide a runtime utility and RPM packaging macros for packaging Software Collections. Software Collections allow users to concurrently install multiple versions of the same RPM packages on the system. Using the scl utility, users may enable specific versions of RPMs, which are installed into the /opt directory. The scl-utils packages provide support for Red Hat Developer Toolset 1.1 packages.

Bug Fixes

BZ#949994

Previously, detection of Software Collections that were specified to be enabled was done in a wrong place in the code. Thus, when attempting to enable multiple Software Collections with a single command, scl-utils enabled only the first given Collection. The updated package scans all the arguments, and all specified Software Collections are now enabled.

BZ#955668

When starting an inspection of the already-enabled Collections, a wrong variable was taken as source of information. Consequently, when running a shell in the scl_enabled environment, users could successfully enable the already-enabled Collection. This could lead to destruction of some parts of the original environment. This update accepts the correct variable as a source of information concerning the already-enabled collections, and the collections are no longer enabled multiple times.

BZ#957176

Previously, the python27 packages required a specific byte compiler. Consequently, the build of python27 using the wrong byte compiler collection failed. With this update, the python27 packages can be compiled successfully using a new functionality to override various rpm macros.

BZ#957752

If the PATH variable was not set as expected by scl-utils, executing the "scl enable" command led to a "command not found" error message. This was caused by the scl utility calling the scl_enabled command without the absolute PATH and relying on the PATH set by the user. With this update, scl-utils calls the scl_enabled helper script with the absolute PATH, and the aforementioned error messages no longer occur.

BZ#957765

Prior to this update, the ori_cmd variable was freed at the moment of displaying. Consequently, the scl utility could have failed with a segmentation fault. The fix has been provided for a double free or corruption error when reading commands from the standard input, and thus scl no longer fails.

BZ#964056

While enabling Software Collections, scl did not respect results of a test and always enabled Collections regardless of whether the respective Collection was already enabled or not. As a consequence, a Collection was enabled multiple times if the Collection was specified more than once in the command, which could result in undetermined behavior. This update runs the enable scriptlet only if the Collection has not been enabled before, and any attempts to enable a collection multiple times in one environment are now ignored.

Users of scl-utils are advised to upgrade to these updated packages, which fix these bugs.

4.98. selinux-policy

4.98.1. RHBA-2013:14802 — selinux-policy bug fix update

Updated *selinux-policy* packages that fix numerous bugs are now available for Red Hat Enterprise Linux 5.

The *selinux-policy* packages contain the rules that govern how confined processes run on the system.

Bug Fixes

BZ#746979

When the SSH daemon (**sshd**) was configured using the **rgmanager** utility as a service for clustering, **sshd** incorrectly ran in the **rgmanager_t** SELinux domain instead of the **sshd_t** SELinux domain. With this update, the relevant SELinux policy has been fixed and **sshd** runs in **sshd_t** as expected in the described scenario.

BZ#838702

With the SELinux strict policy enabled, when the user executed a locally developed application configured to use the **atd** daemon, the daemon ran in an incorrect SELinux domain due to the missing SELinux policy rules. Consequently, the following error message was logged in the **/var/log/message** file:

```
Not allowed to set exec context
```

With this update, the appropriate SELinux policy rules have been added so that **atd** runs in the correct domain and the error message is no longer returned.

BZ#906279

When SELinux was running in enforcing mode, it incorrectly prevented processes labeled with the **pptp_t** SELinux security context from accessing files labeled with the **proc_net_t** SELinux security context. This update fixes the relevant SELinux policy and **pptp_t** processes can access files with the **proc_net_t** context as expected.

BZ#921671

Previously, some patterns in the **/etc/selinux/targeted/contexts/files/file_contexts** file contained typographical errors. Some patterns matched the 32-bit path but the same pattern for the 64-bit path was missing. Consequently, different security contexts were assigned to these paths. With this update, the relevant file context specifications have been corrected so that there are no more differences between these paths.

BZ#923428, BZ#926028

Due to the incorrect SELinux policy rules for the **httpd_use_fusefs** and **allow_ftpd_use_fusefs** Booleans, the **httpd** and **ftpd** daemons were not able to access link files on a FUSE (Filesystem in Userspace) file system when SELinux was running in enforcing mode. The appropriate SELinux policy rules have been fixed and **httpd** and **ftpd** are now able to access link files on the FUSE file systems as expected.

BZ#953874

When SELinux was running in enforcing mode, an attempt to fetch a file using the Squid proxy caching server along with Kerberos authentication caused AVC denials to be returned. The relevant SELinux policy has been changed to allow Squid to connect to the tcp/133 port and the AVC denials are no longer returned in the described scenario.

BZ#958759, BZ#984583

Previously, the **mysqld_safe** script was unable to execute the Bourne shell (**/bin/sh**) with the **shell_exec_t** SELinux security context. Consequently, the *mysql55* and *mariadb55* Software Collection packages were not working correctly. With this update, SELinux policy rules have been updated and these packages now work as expected.

BZ#959171

When a Network Information Service (NIS) master with two NIS slaves was configured, executing the **yppasswdd --port 836** command proceeded up until it started rebuilding the **passwd.byname** and **passwd.byuid** databases. The databases were rebuilt successfully but they were not pushed to the NIS slaves due to missing SELinux policy rules. With this update, the relevant SELinux rule has been added to fix this bug and the **yppasswdd --port 836** command works as expected.

BZ#966929

Due to an incorrect SELinux policy, the **openvpn** service was not able to write or read the **/var/log/openvpn** file. Consequently, an attempt to start **openvpn** failed and AVC messages were logged to the **/var/log/audit/audit.log** file. With this update, the appropriate SELinux policy has been fixed so that the AVC messages are no longer returned and **openvpn** works as expected in the described scenario.

BZ#970707

When the **php-cgi** command-line interface was called by the **httpd** server, SELinux running in enforcing mode prevented access to the **/usr/share/snmp/mibs/.index** file. Consequently, the PHP SNMP (Simple Network Management Protocol) extension did not work correctly due to the missing Management Information Bases (MIBs). With this update, the relevant SELinux policy has been modified and SELinux no longer prevents access to MIBs in the described scenario.

BZ#978864

Previously, the **snmpd_t** SELinux domain was missing the **chown** capability. Consequently, the ***agentXperms*** directive in the **snmpd.conf** file did not work. This update provides an updated SELinux policy rule that allows processes running in the **snmpd_t** SELinux domain to use the **chown** capability, thus fixing this bug.

Users of *selinux-policy* are advised to upgrade to these updated packages, which fix these bugs.

4.99. sos

4.99.1. RHSA-2013:1121 — Low: sos security update

An updated sos package that fixes one security issue is now available for Red Hat Enterprise Linux 5.

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

The sos package contains a set of tools that gather information from system hardware, logs and configuration files. The information can then be used for diagnostic purposes and debugging.

Security Fix

CVE-2012-2664

The sosreport utility collected the Kickstart configuration file ("/root/anaconda-ks.cfg"), but did not remove the root user's password from it before adding the file to the resulting archive of debugging information. An attacker able to access the archive could possibly use this flaw to obtain the root user's password. "/root/anaconda-ks.cfg" usually only contains a hash of the password, not the plain text password.

Note: This issue affected all installations, not only systems installed via Kickstart. A "/root/anaconda-ks.cfg" file is created by all installation types.

The utility also collects yum repository information from "/etc/yum.repos.d" which in uncommon configurations may contain passwords. Any http_proxy password specified in these files will now be automatically removed. Passwords embedded within URLs in these files should be manually removed or the files excluded from the archive.

All users of sos are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

4.99.2. RHBA-2013:1356 — 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 5.

The *sos* package contains a set of tools that gather information from system hardware, logs and configuration files. The information can then be used for diagnostic purposes and debugging.

Bug Fixes

BZ#782218

When the *rhn-client-tools* package was not installed and the **__raisePlugins__** plug-in was enabled on the system, the **sosreport** utility failed to collect the **dmidecode** files and other hardware information. This update provides a patch to fix this bug and **sosreport** now works correctly in the described scenario.

BZ#782247

When the *audit* package was not installed and the **/var/log/audit** file did not exist on the system, the **auditd** plug-in failed with a traceback error. This bug has been fixed and **auditd** now properly handles the missing **/var/log/audit** file.

BZ#868008

When SELinux was disabled on the system, the **sosreport** utility did not collect the information located in the **sos_commands/selinux/** directory. This update provides a patch to fix this bug, and **sosreport** now correctly collects all the required information in the described scenario.

BZ#906071

Previous versions of the sos **psacct** (BSD Process Accounting) module collected all process accounting files present on the system, which could, under certain configurations, lead to a very large number of archived files in the process accounting directory. To fix this, **psacct** now collects only the most recent accounting file by default. The **all** option has been added to the module which allows the user to request the original behavior if required. As a result, reports generated on hosts with many archived accounting files no longer include this large set of additional data.

BZ#958346

Previously, the **sosreport** utility did not capture modules located in the **/etc/modules.*/** directory including module blacklisting. With this update, a patch has been provided to fix this bug and **sosreport** now captures the modules as expected.

BZ#976242

Previous versions of the **sos** utility did not sanitize special characters in system host names when using the name in file system paths. Consequently, inserting special characters in the system host name could cause **sos** to generate invalid file system paths and fail to generate a report. With this update, invalid characters are filtered out of system host names and **sos** now works correctly on systems having characters disallowed in file system paths present in the host name.

BZ#977187

When used on PowerPC systems, the **sosreport** utility took a copy of the **/boot/yaboot.conf**

file but not a copy of the **/etc/yaboot.conf** file. Consequently, **sosreport** could miss important information present in this file. This update applies a patch to fix this bug and the report from **sosreport** now contains information from **/etc/yaboot.conf** if present.

Enhancements

BZ#840981

Previous releases of **sos** captured only the **/proc/ioports** file detailing registered I/O port regions in use. The **/proc/iomem** file additionally describes regions of physical system memory and their use of memory, firmware data, and device I/O traffic. As this data can be important in debugging certain hardware and device-driver problems, both **ioports** and **iomem** data have beer made available within generated reports.

BZ#891325

Previously, the **sar** plug-in did not set a size restriction for collected data, which could cause the **sosreport** utility to fill up the directory for temporary files. This enhancement adds the ability to limit the maximum size of collected data for the **sar** plug-in.

BZ#907876

The ID mapping daemon (**idmapd**) controls identity mappings used by NFSv4 services and is important for diagnostic and troubleshooting efforts. This enhancement provides a new feature that allows the **sosreport** utility to analyze the **idmapd.conf** file on NFS client and server hosts.

Users of *sos* are advised to upgrade to this updated package, which fixes these bugs and adds these enhancements.

4.100. spamassassin

4.100.1. RHBA-2013:1336 — spamassassin bug fix update

Updated spamassassin packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

SpamAssassin provides a way to reduce unsolicited commercial email (spam) from incoming email.

Bug Fixes

BZ#892348

The rules using the "rawbody" test did not always return a match because SpamAssassin split the raw data into 1-2kB size parts. With this update, a note has been added to the Mail::SpamAssassin::Conf documentation, addressing the limitations resulting from this bug.

BZ#892350

Previously, a bug in the parser used the wrong data to detect URLs between HTML tags. As a consequence, SpamAssassin did not always detect HTTP(S) URL multiline mismatches in email messages. This bug is now fixed and SpamAssassin properly detects multiline mismatches.

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

4.101. sssd

4.101.1. RHSA-2013:1319 — Low: sssd security and bug fix update

Updated sssd packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 5.

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

SSSD (System Security Services Daemon) provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides NSS (Name Service Switch) and PAM (Pluggable Authentication Modules) interfaces toward the system and a pluggable back end system to connect to multiple different account sources.

Security Fix

CVE-2013-0219

A race condition was found in the way SSSD copied and removed user home directories. A local attacker who is able to write into the home directory of a different user who is being removed could use this flaw to perform symbolic link attacks, possibly allowing them to modify and delete arbitrary files with the privileges of the root user.

The CVE-2013-0219 issue war discovered by Florian Weimer of the Red Hat Product Security Team.

Bug Fixes

BZ#820908

After a paging control was used, memory in the sssd_be process was never freed which led to the growth of the sssd_be process memory usage over time. To fix this bug, the paging control was deallocated after use, and thus the memory usage of the sssd_be process no longer grows.

BZ#882414

If the sssd_be process was terminated and recreated while there were authentication requests pending, the sssd_pam process did not recover correctly and did not reconnect to the new sssd_be process. Consequently, the sssd_pam process was seemingly blocked and did not accept any new authentication requests. The sssd_pam process has been fixes so that it reconnects to the new instance of the sssd_be process after the original one terminated unexpectedly. Even after a crash and reconnect, the sssd_pam process now accepts new authentication requests.

BZ#886165

When the sssd_be process hung for a while, it was terminated and a new instance was created. If the old instance did not respond to the TERM signal and continued running, SSSD terminated unexpectedly. As a consequence, the user could not log in. SSSD now keeps track of sssd_be subprocesses more effectively, making the restarts of sssd_be more reliable in such scenarios. Users can now log in whenever the sssd_be is restarted and becomes unresponsive.

BZ#923813

In case the processing of an LDAP request took longer than the client timeout upon completing the request (60 seconds by default), the PAM client could have accessed memory that was previously freed due to the client timeout being reached. As a result, the sssd_pam process terminated unexpectedly with a segmentation fault. SSSD now ignores an LDAP request result when it detects that the set timeout of this request has been reached. The sssd_pam process no longer crashes in the aforementioned scenario.

BZ#805729

When there was a heavy load of users and groups to be saved in cache, SSSD experienced a timeout. Consequently, NSS did not start the backup process properly and it was impossible to log in. A patch has been provided to fix this bug. The SSSD daemon now remains responsive and the login continues as expected.

BZ#961680

SSSD kept the file descriptors to the log files open. Consequently, on occasions like moving the actual log file and restarting the back end, SSSD still kept the file descriptors open. SSSD now closes the file descriptor after the child process execution; after a successful back end start, the file descriptor to log files is closed.

BZ#979047

While performing access control in the Identity Management back end, SSSD erroneously downloaded the "member" attribute from the server and then attempted to use it in the cache verbatim. Consequently, the cache attempted to use the "member" attribute values as if they were pointing to the local cache which was CPU intensive. The member attribute when processing host groups is no longer downloaded and processed. Moreover, the login process is reasonably fast even with large host groups.

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

4.102. subscription-manager

4.102.1. RHBA-2013:1332 — subscription-manager bug fix and enhancement update

Updated subscription-manager packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The Subscription Manager tool allows users to understand the specific products which have been installed on their machines, and the specific subscriptions which their machines are consuming.

Note

The subscription-manager package has been upgraded to upstream version 1.8.22-1, which provides a number of bug fixes and enhancements over the previous version. Namely, this rebase addresses a number of usability issues, makes the client faster, and gives users a more consistent experience among Red Hat Enterprise Linux releases. (BZ#963413)

Bug Fixes

BZ#877331

Previously, several options were missing from the migration script which prevented the user from migrating from RHN Classic to certificate-based Subscription Management. To fix this bug, options have been added therein and the user can now migrate flawlessly.

BZ#916369

Prior to this update, the parameter-parsing code was constantly updating the configuration whenever the "--insecure" option was present. Consequently, the "--insecure" option would always overwrite the configuration value. The insecure value persistence has been modified to delay until after the command completes, thus fixing the bug.

BZ#906642

Previously, the repolist command did not accept the "--proxy" option, which hindered listing repositories using the HTTP proxy server. To fix this bug, the "--proxy" option has been added to the repolist command. The user can now list their repositories while also specifying their HTTP proxy server connection.

BZ#845622

Prior to this update, confusing error messages were displayed when the user's identity certificate expired. With this update, a proper message has been added. The users can now see when their identity certificates expire.

BZ#818978

Previously, a systemd script was missing which prevented the systemctl utility from starting the rhsmcertd daemon. Systemd-style initialization scripts for rhsmcertd have been added. As a result, rhsmcertd can now be started successfully using systemctl.

BZ#993202

Due to the incorrectly placed ca_cert_dir configuration entry in the /etc/rhsm/rhsm.conf file, interpolation problems occurred. To fix this bug, the ca_cert_dir configuration line has been moved from the [server] into [rhsm] section keeping the functionality as in previous versions.

BZ#997189

Previously, the firstboot utility displayed unnecessary and confusing error messages to the user. To fix this bug, the content of the messages has been changed to inform the user clearly and effectively.

Enhancements

BZ#905922

Subscription Manager can now be configured to not upload package profile data by setting the "report_package_profile = 1" configuration option in the /etc/rhsm/rhsm.conf file.

BZ#913118

The hasNow() function has been removed as it was deprecated and no longer useful for the users.

All users of subscription-manager are advised to upgrade to these updated packages, which provide these bug fixes and add these enhancements.

4.102.2. RHSA-2013:0788 — Moderate: subscription-manager security update

Updated subscription-manager packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

The subscription-manager packages provide programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat Entitlement platform.

Security Fix

CVE-2012-6137

It was discovered that the rhn-migrate-classic-to-rhsm tool did not verify the Red Hat Network Classic server's X.509 certificate when migrating system profiles registered with Red Hat Network Classic to Certificate-based Red Hat Network. An attacker could use this flaw to conduct man-in-the-middle attacks, allowing them to obtain the user's Red Hat Network credentials.

This issue was discovered by Florian Weimer of the Red Hat Product Security Team.

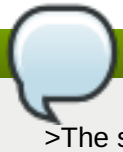
All users of subscription-manager are advised to upgrade to these updated packages, which contain a backported patch to fix this issue.

4.103. subscription-manager-migration-data

4.103.1. RHEA-2013:1333 — subscription-manager-migration-data enhancement update

An updated subscription-manager-migration-data package that adds various enhancements is now available for Red Hat Enterprise Linux 5.

The new Subscription Management tooling allows users to understand the specific products which have been installed on their machines, and the specific subscriptions which their machines consume.



Note

>The subscription-manager-migration-data package has been upgraded to upstream version 1.11.3.2, which provides a number of enhancements over the previous version. (BZ#961499)

Users of subscription-manager-migration-data are advised to upgrade to this updated package, which adds these enhancements.

4.104. subversion

4.104.1. RHSA-2013:0737 — Moderate: subversion security update

Updated subversion packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6.

The Red Hat Security Response Team has rated this update as having 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.

Subversion (SVN) is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes. The mod_dav_svn module is used with the Apache HTTP Server to allow access to Subversion repositories via HTTP.

Security Fixes

CVE-2013-1849

A NULL pointer dereference flaw was found in the way the mod_dav_svn module handled PROPFIND requests on activity URLs. A remote attacker could use this flaw to cause the httpd process serving the request to crash.

CVE-2013-1845

A flaw was found in the way the mod_dav_svn module handled large numbers of properties (such as those set with the "svn propset" command). A malicious, remote user could use this flaw to cause the httpd process serving the request to consume an excessive amount of system memory.

CVE-2013-1846, **CVE-2013-1847**

Two NULL pointer dereference flaws were found in the way the mod_dav_svn module handled LOCK requests on certain types of URLs. A malicious, remote user could use these flaws to cause the httpd process serving the request to crash.

Note: The CVE-2013-1849, CVE-2013-1846, and CVE-2013-1847 issues only caused a temporary denial of service, as the Apache HTTP Server started a new process to replace the crashed child process. When using prefork MPM, the crash only affected the attacker. When using worker (threaded) MPM, the connections of other users may have been interrupted.

Red Hat would like to thank the Apache Subversion project for reporting these issues. Upstream acknowledges Alexander Klink as the original reporter of CVE-2013-1845; Ben Reser as the original reporter of CVE-2013-1846; and Philip Martin and Ben Reser as the original reporters of CVE-2013-1847.

All subversion users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, you must restart the httpd daemon, if you are using mod_dav_svn, for the update to take effect.

4.105. sudo

4.105.1. RHSA-2013:1353 — Low: sudo security and bug fix update

An updated sudo package that fixes multiple security issues and several bugs is now available for Red Hat Enterprise Linux 5.

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

The sudo (superuser do) utility allows system administrators to give certain users the ability to run commands as root.

Security Fixes

CVE-2013-1775

A flaw was found in the way sudo handled time stamp files. An attacker able to run code as a local user and with the ability to control the system clock could possibly gain additional privileges by running commands that the victim user was allowed to run via sudo, without knowing the victim's password.

CVE-2013-1776, **CVE-2013-2776**

It was found that sudo did not properly validate the controlling terminal device when the tty_tickets option was enabled in the /etc/sudoers file. An attacker able to run code as a local user could possibly gain additional privileges by running commands that the victim user was allowed to run via sudo, without knowing the victim's password.

Bug Fixes

BZ#849679

Due to a bug in the cycle detection algorithm of the visudo utility, visudo incorrectly evaluated certain alias definitions in the /etc/sudoers file as cycles. Consequently, a warning message about undefined aliases appeared. This bug has been fixed, /etc/sudoers is now parsed correctly by visudo and the warning message no longer appears.

BZ#855836

Previously, the 'sudo -l' command did not parse the /etc/sudoers file correctly if it contained an Active Directory (AD) group. The file was parsed only up to the first AD group information and then the parsing failed with the following message:

sudo: unable to cache group ADDOM\admingroup, already exists

With this update, the underlying code has been modified and 'sudo -l' now parses /etc/sudoers containing AD groups correctly.

BZ#869287

Previously, the sudo utility did not escape the backslash characters contained in user names properly. Consequently, if a system used sudo integrated with LDAP or Active Directory (AD) as the primary authentication mechanism, users were not able to authenticate on that system. With this update, sudo has been modified to process LDAP and AD names correctly and the authentication process now works as expected.

BZ#905624

Prior to this update, the 'visudo -s (strict)' command incorrectly parsed certain alias definitions. Consequently, an error message was issued. The bug has been fixed, and parsing errors no longer occur when using 'visudo -s'.

All sudo users are advised to upgrade to this updated package, which contains backported patches to correct these issues.

4.105.2. RHBA-2013:0616 — sudo bug fix update

Updated sudo packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The sudo (superuser do) utility allows system administrators to give certain users the ability to run commands as root.

Bug Fixes

BZ#916220

The "sudo -l" command did not parse the /etc/sudoers file correctly if it contained an Active Directory (AD) group. The file was parsed only up to the first AD group information and the command then failed with the following error message:

```
sudo: unable to cache group ADDOM\admingroup, already exists
```

With this update, the underlying code has been modified so the "sudo -l" command now parses the /etc/sudoers file as it is supposed to and no longer displays this error message.

BZ#916232

Previously, sudo did not escape the backslash characters contained in user names properly. Consequently, if a system used sudo integrated with LDAP or Active Directory as the primary authentication mechanism, users were not able to authenticate on that system. This patch modifies sudo to process LDAP and AD names correctly and the authentication process now functions as expected.

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

4.106. system-config-cluster

4.106.1. RHBA-2013:1315 — system-config-cluster bug fix update

Updated system-config-cluster packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The system-config-cluster package contains system-config-cluster, a utility that allows you to graphically manage cluster configuration.

Bug Fixes

BZ#867022

Previously, the cluster.ng "nfsrestart" attribute was not defined as a file system attribute in system-config-cluster. As a consequence, when running the xmllint tool to validate the /etc/cluster/cluster.conf file, xmllint terminated with an error. With this update, the "nfsrestart" attribute has been added to the list of file system resources and validation of the /etc/cluster/cluster.conf file now works as expected.

BZ#875592

The "miss_count_const" parameter was missing from the cluster.ng schema and, as a consequence, when the user added the parameter to the /etc/cluster/cluster.conf file, the configuration file failed to validate. With this update, the parameter has been added to the cluster.ng schema and the /etc/cluster/cluster.conf file validates successfully with the aforementioned parameter.

BZ#903560

Previously, the "DRBD" resource was missing from the cluster.ng schema and, as a consequence, the /etc/cluster/cluster.conf file failed to validate with xmllint. With this update, the missing attribute has been added to the cluster.ng schema and the /etc/cluster/cluster.conf file now validates successfully with the aforementioned parameter.

Users of system-config-cluster are advised to upgrade to these updated packages, which fix these bugs.

4.107. system-config-kdump

4.107.1. RHBA-2013:0789 — system-config-kdump bug fix update

Updated system-config-kdump packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The system-config-kdump tool is a graphical utility used to configure kernel crash dumping via the kdump and kexec utilities.

Bug Fix

BZ#947938

Previously, the system-config-kdump utility did not allow users to configure the kdump utility to store kernel dumps as a file on the ext4 file system. This update provides the "ext4" option to the "Edit location -> Select location type" setting, thus fixing this bug.

Users of system-config-kdump are advised to upgrade to these updated packages, which fix this bug.

4.108. system-config-lvm

4.108.1. RHBA-2013:1347 — system-config-lvm bug fix update

Updated system-config-lvm packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The system-config-lvm packages contain a utility for configuring logical volumes (LVs) using a graphical user interface.

* Due to a limitation in the system-config-lvm application, it terminated unexpectedly when striped mirrored devices were found. With this update, system-config-lvm no longer crashes and users can fully interact with striped mirrored devices. However, such devices may not always render properly in the application. It is recommended to use the command line interface tools to interact with striped mirrored devices. (BZ#875148)

Bug Fix

BZ#875148

Due to a limitation in the system-config-lvm application, it terminated unexpectedly when striped mirrored devices were found. With this update, system-config-lvm no longer crashes and users can fully interact with striped mirrored devices. However, such devices may not always render properly in the application. It is recommended to use the command line interface tools to interact with striped mirrored devices.

Users of system-config-lvm are advised to upgrade to these updated packages, which fix this bug.

4.109. thunderbird

4.109.1. RHSA-2013:0697 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-0788

Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-0795

A flaw was found in the way Same Origin Wrappers were implemented in Thunderbird. Malicious content could use this flaw to bypass the same-origin policy and execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-0796

A flaw was found in the embedded WebGL library in Thunderbird. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird. Note: This issue only affected systems using the Intel Mesa graphics drivers.

CVE-2013-0800

An out-of-bounds write flaw was found in the embedded Cairo library in Thunderbird. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-0793

A flaw was found in the way Thunderbird handled the JavaScript history functions. Malicious content could cause a page to be displayed that has a baseURI pointing to a different site, allowing cross-site scripting (XSS) and phishing attacks.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Olli Pettay, Jesse Ruderman, Boris Zbarsky, Christian Holler, Milan Sreckovic, Joe Drew, Cody Crews, miaubiz, Abhishek Arya, and Mariusz Mlynski as the original reporters of these issues.

Note: All issues except CVE-2013-0800 cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 17.0.5 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.109.2. RHSA-2013:1269 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-1718, CVE-2013-1722, CVE-2013-1725, CVE-2013-1730, CVE-2013-1732, CVE-2013-1735, CVE-2013-1736

Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-1737

A flaw was found in the way Thunderbird handled certain DOM JavaScript objects. An attacker could use this flaw to make JavaScript client or add-on code make incorrect, security sensitive decisions.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges André Bargull, Scoobidiver, Bobby Holley, Reuben Morais, Abhishek Arya, Ms2ger, Sachin Shinde, Aki Helin, Nils, and Boris Zbarsky as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 17.0.9 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.109.3. RHSA-2013:1142 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-1701

Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-1710

A flaw was found in the way Thunderbird generated Certificate Request Message Format (CRMF) requests. An attacker could use this flaw to perform cross-site scripting (XSS) attacks or execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-1709

A flaw was found in the way Thunderbird handled the interaction between frames and browser history. An attacker could use this flaw to trick Thunderbird into treating malicious content as if it came from the browser history, allowing for XSS attacks.

CVE-2013-1713

It was found that the same-origin policy could be bypassed due to the way Uniform Resource Identifiers (URI) were checked in JavaScript. An attacker could use this flaw to perform XSS attacks, or install malicious add-ons from third-party pages.

CVE-2013-1714

It was found that web workers could bypass the same-origin policy. An attacker could use this flaw to perform XSS attacks.

CVE-2013-1717

It was found that, in certain circumstances, Thunderbird incorrectly handled Java applets. If a user launched an untrusted Java applet via Thunderbird, the applet could use this flaw to obtain read-only access to files on the user's local system.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Jeff Gilbert, Henrik Skupin, moz_bug_r_a4, Cody Crews, Federico Lanusse, and Georgi Guninski as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 17.0.8 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.109.4. RHSA-2013:0982 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-1682, CVE-2013-1684, CVE-2013-1685, CVE-2013-1686, CVE-2013-1687, CVE-2013-1690

Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-1692

It was found that Thunderbird allowed data to be sent in the body of XMLHttpRequest (XHR) HEAD requests. In some cases this could allow attackers to conduct Cross-Site Request Forgery (CSRF) attacks.

CVE-2013-1693

Timing differences in the way Thunderbird processed SVG image files could allow an attacker to read data across domains, potentially leading to information disclosure.

CVE-2013-1694, CVE-2013-1697

Two flaws were found in the way Thunderbird implemented some of its internal structures (called wrappers). An attacker could use these flaws to bypass some restrictions placed on them. This could lead to unexpected behavior or a potentially exploitable crash.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Gary Kwong, Jesse Ruderman, Andrew McCreight, Abhishek Arya, Mariusz Mlynski, Nils, Johnathan Kuskos, Paul Stone, Boris Zbarsky, and moz_bug_r_a4 as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 17.0.7 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.109.5. RHSA-2013:0627 — Important: thunderbird security update

An updated thunderbird package that fixes one security issue is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fix

CVE-2013-0787

A flaw was found in the processing of malformed content. Malicious content could cause Thunderbird to crash or execute arbitrary code with the privileges of the user running Thunderbird.

Red Hat would like to thank the Mozilla project for reporting this issue. Upstream acknowledges VUPEN Security via the TippingPoint Zero Day Initiative project as the original reporter.

Note: This issue cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. It could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which corrects this issue. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.109.6. RHSA-2013:0821 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-0801, CVE-2013-1674, CVE-2013-1675, CVE-2013-1676, CVE-2013-1677, CVE-2013-1678, CVE-2013-1679, CVE-2013-1680, CVE-2013-1681

Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-1670

A flaw was found in the way Thunderbird handled Content Level Constructors. Malicious content

A flaw was found in the way Thunderbird handled Content Level Constructors. Malicious content could use this flaw to perform cross-site scripting (XSS) attacks.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Christoph Diehl, Christian Holler, Jesse Ruderman, Timothy Nikkel, Jeff Walden, Nils, Ms2ger, Abhishek Arya, and Cody Crews as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 17.0.6 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.109.7. RHSA-2013:0272 — Critical: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-0775, CVE-2013-0780, CVE-2013-0782, CVE-2013-0783

Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-0776

It was found that, after canceling a proxy server's authentication prompt, the address bar continued to show the requested site's address. An attacker could use this flaw to conduct phishing attacks by tricking a user into believing they are viewing trusted content.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Nils, Abhishek Arya, Olli Pettay, Christoph Diehl, Gary Kwong, Jesse Ruderman, Andrew McCreight, Joe Drew, Wayne Mery, and Michal Zalewski as the original reporters of these issues.

Note: All issues cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

Important: This erratum upgrades Thunderbird to version 17.0.3 ESR. Thunderbird 17 is not completely backwards-compatible with all Mozilla add-ons and Thunderbird plug-ins that worked with Thunderbird 10.0. Thunderbird 17 checks compatibility on first-launch, and, depending on the individual configuration and the installed add-ons and plug-ins, may disable said Add-ons and plug-ins, or attempt to check for updates and upgrade them. Add-ons and plug-ins may have to be manually updated.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 17.0.3 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.110. tomcat5

4.110.1. RHSA-2013:0870 — Important: tomcat5 security update

Updated tomcat5 packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

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

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

Security Fix

CVE-2013-1976

A flaw was found in the way the tomcat5 init script handled the catalina.out log file. A malicious web application deployed on Tomcat could use this flaw to perform a symbolic link attack to change the ownership of an arbitrary system file to that of the tomcat user, allowing them to escalate their privileges to root.

Note: With this update, /var/log/tomcat5/catalina.out has been moved to the /var/log/tomcat5-initd.log file.

Red Hat would like to thank Simon Fayer of Imperial College London for reporting this issue.

Users of Tomcat are advised to upgrade to these updated packages, which correct this issue. Tomcat must be restarted for this update to take effect.

4.110.2. RHSA-2013:0640 — Important: tomcat5 security update

Updated tomcat5 packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

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

Apache Tomcat is a servlet container.

Security Fixes

CVE-2012-3546

It was found that when an application used FORM authentication, along with another component that calls request.setUserPrincipal() before the call to FormAuthenticator#authenticate() (such as the Single-Sign-On valve), it was possible to bypass the security constraint checks in the FORM authenticator by appending "/j_security_check" to the end of a URL. A remote attacker with an authenticated session on an affected application could use this flaw to circumvent authorization controls, and thereby access resources not permitted by the roles associated with their authenticated session.

CVE-2012-5885, CVE-2012-5886, CVE-2012-5887

Multiple weaknesses were found in the Tomcat DIGEST authentication implementation, effectively reducing the security normally provided by DIGEST authentication. A remote attacker could use these flaws to perform replay attacks in some circumstances.

Users of Tomcat should upgrade to these updated packages, which correct these issues. Tomcat must be restarted for this update to take effect.

4.111. tzdata

4.111.1. RHEA-2013:0674 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 3, 4, 5 and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#921173, BZ#921174, BZ#919628, BZ#921176

Time zone rules of tzdata have been modified to reflect the following changes:

The period of Daylight Saving Time (DST) in Paraguay will end on March 24 instead of April 14.

Haiti will use US daylight-saving rules in the year 2013.

Morocco does not observe DST during Ramadan. Therefore, Morocco is expected to switch to Western European Time (WET) on July 9 and resume again to Western European Summer Time (WEST) on August 8.

Also, the tzdata packages now provide rules for several new time zones: Asia/Khandyga, Asia/Ust-Nera, and Europe/Busingen.

All users of tzdata are advised to upgrade to these updated packages, which add this enhancement.

4.111.2. RHEA-2013:0880 — tzdata enhancement update

Updated tzdata packages that add various enhancements are now available for Red Hat Enterprise Linux 3, 4, 5, and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancements

BZ#928461, BZ#928462, BZ#928463, BZ#928464

The Gaza Strip and the West Bank entered Daylight Saving Time on March 28 at midnight local time.

Recent change to Daylight Saving rules in Paraguay appears to be perpetual. Transition times in years 2014 and later were updated accordingly.

The Macquarie Island was uninhabited between years 1919 and 1948. This update introduces a new time type with a "zzz" abbreviation, which distinguishes uninhabited regions from the inhabited ones.

The Macquarie Island belongs to Australia. This updated modifies the /usr/share/zoneinfo/zone.tab file accordingly.

All users of tzdata are advised to upgrade to these updated packages, which add these enhancements.

4.111.3. RHEA-2013:1025 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 3, 4, 5, and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#980805, BZ#980807, BZ#981019, BZ#981020

Morocco does not observe DST during Ramadan. Therefore, Morocco is expected to switch to Western European Time (WET) on July 7 and resume again to Western European Summer Time (WEST) on August 10. Also, the period of DST in Israel has been extended until the last Sunday in October from the year 2013 onwards.

All users of tzdata are advised to upgrade to these updated packages, which add this enhancement.

4.111.4. RHEA-2013:0182 — tzdata enhancement update

New tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 3, 4, 5, and 6.

The tzdata packages contain data files with rules for time zones.

Enhancement

BZ#894030, BZ#894044, BZ#894045, BZ#894046

On Nov 10, 2012, Libya changed to the time zone UTC+1. Therefore, starting from the year 2013 Libya will be switching to daylight saving time on the last Friday of March and back to the standard time on the last Friday of October. The time zone setting and the daylight saving time settings for the Africa/Tripoli time zone have been updated accordingly.

All users of tzdata are advised to upgrade to these updated packages, which add this enhancement.

4.111.5. RHEA-2013:0615 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 3, 4, 5 and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#912521, BZ#916272, BZ#916273, BZ#916274

The Chilean Government is extending the period of Daylight Saving Time (DST) in the year 2013 until April the 27th. Then, Chile Standard Time (CLT) and Easter Island Standard Time (EAST) will be in effect until September the 7th when switching again to DST. With this update, the rules used for Chile time zones have been adjusted accordingly.

All users of tzdata are advised to upgrade to these updated packages, which add this enhancement.

4.112. v7

4.112.1. RHBA-2013:0667 — v7 bug fix update

An updated v7 package that fixes one bug is now available for Red Hat Enterprise Linux Hardware Certification.

v7, the Red Hat Enterprise Linux hardware certification test suite, verifies the compatibility of hardware devices. Each v7 test run builds a results database for submission to Red Hat's hardware catalog as an RPM package. v7 replaces Red Hat Hardware Test Suite (HTS) for certifying hardware for use with Red Hat Enterprise Linux.

Bug Fix

BZ#919493

v7 did not have the complete GA kernel release information for Red Hat Enterprise Linux 5.9 in its local files. Consequently, if the System Under Test (SUT) could not reach the Red Hat Partner's File Transfer Protocol (FTP) site for an update, the info test failed. To fix this bug, the v7 1.5 R33 certification kit info test now includes an updated XML file with an entry for the GA kernel release included in Red Hat Enterprise Linux 5.9. As a result, the info test passes kernel verification.

Users of v7 are advised to upgrade to this updated package, which fixes this bug.

4.112.2. RHBA-2013:0222 — v7 bug fix and enhancement update

An updated v7 package that fixes several bugs and adds multiple enhancements is now available for Red Hat Enterprise Linux Hardware Certification.

v7, the Red Hat Enterprise Linux hardware certification test suite, verifies the compatibility of hardware devices. Each v7 test run builds a results database for submission to Red Hat's hardware catalog as an RPM package. v7 replaces Red Hat Hardware Test Suite (HTS) for certifying hardware for use with Red Hat Enterprise Linux.

This updated v7 package includes numerous bug fixes and enhancements. Space precludes documenting all of these changes in this advisory. Users are directed to the v7 Hardware Certification Test Suite 1 Technical Notes for information on the most significant of these changes:

https://access.redhat.com/site/documentation/en-US/v7_Hardware_Certification_Test_Suite/1/html/Technical_Notes/index.html

All users of v7 are advised to upgrade to this updated package, which provides numerous bug fixes and enhancements.

4.113. wpa_supplicant

4.113.1. RHEA-2013:1365 — wpa_supplicant enhancement update

Updated wpa_supplicant packages that add one enhancement are now available for Red Hat Enterprise Linux 5.

The wpa_supplicant packages contain an 802.1X Supplicant with support for WEP, WPA, WPA2 (IEEE 802.11i / RSN), and various EAP authentication methods. It implements key negotiation with a WPA Authenticator for client stations and controls the roaming and IEEE 802.11 authentication/association of the WLAN driver.

Enhancement

BZ#955153

It is now possible to store passwords in a hashed form in the wpa_supplicant.conf file rather than

only in plain text.

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

4.114. xen

4.114.1. RHBA-2013:0846 — xen bug fix update

Updated xen packages that fix one bug are now available for Red Hat Enterprise Linux 5.

Xen is a high-performance and secure open-source virtualization framework. The xen packages contain administration tools and the xend service for managing the kernel-xen kernel for virtualization on Red Hat Enterprise Linux.

Bug Fix

BZ#960013

Due to a lack of support for set affinity in systems with more than 64 CPU cores, it was not possible to use Xen with such systems as any excess CPUs were reported as idle. With this update, systems with large number of CPU cores are detected and Xen Hypervisor can handle them as expected.

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

4.114.2. RHSA-2013:0241 — Moderate: xen security update

Updated xen packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

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

The xen packages contain administration tools and the xend service for managing the kernel-xen kernel for virtualization on Red Hat Enterprise Linux.

Security Fix

CVE-2012-4544

A flaw was found in the way libxc, the Xen control library, handled excessively large kernel and ramdisk images when starting new guests. A privileged guest user in a para-virtualized guest (a DomU) could create a crafted kernel or ramdisk image that, when attempting to use it during guest start, could result in an out-of-memory condition in the privileged domain (the Dom0).

Red Hat would like to thank the Xen project for reporting this issue.

All users of xen are advised to upgrade to these updated packages, which correct this issue. After installing the updated packages, the xend service must be restarted for this update to take effect.

4.114.3. RHSA-2013:0599 — Important: xen security update

Updated xen packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

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

The xen packages contain administration tools and the xend service for managing the kernel-xen kernel for virtualization on Red Hat Enterprise Linux.

Security Fix

CVE-2012-6075

A flaw was found in the way QEMU emulated the e1000 network interface card when the host was configured to accept jumbo network frames, and a fully-virtualized guest using the e1000 emulated driver was not. A remote attacker could use this flaw to crash the guest or, potentially, execute arbitrary code with root privileges in the guest.

All users of xen are advised to upgrade to these updated packages, which correct this issue. After installing the updated packages, all running fully-virtualized guests must be restarted for this update to take effect.

4.115. xenpv-win

4.115.1. RHBA-2013:0740 — xenpv-win bug fix update

An updated xenpv-win package that fixes multiple bugs is now available for Red Hat Enterprise Linux 5.

The xenpv-win package contains installation images for para-virtualized drivers for guests running Microsoft Windows XP or later on Red Hat Enterprise Linux hosts. Para-virtualized drivers provide significant network and disk I/O performance improvements for fully virtualized guests over the same guests running with fully virtualized drivers.

Bug Fixes

BZ#770633

If a locked Windows 2003 guest with the xenpv-win driver installed was shut down or rebooted by executing the "xm shutdown" or "xm reboot" command, the commands became invalid when attempting to execute them again after the machine was unlocked. The underlying source code has been modified so that Windows 2003 guests can be shut down and rebooted repeatedly regardless of whether the guest has been locked or not.

BZ#805669

Due to a hard-coded 0 index in the code that manipulates the event channel pending mask, the xenpv-win driver could become unresponsive during boot on EC2 Large Instances. This problem has been fixed, and xenpv-win no longer hangs in this scenario.

BZ#844903

This version of xenpv-win has been certified through the Microsoft Server Virtualization Validation Platform (SVVP) program.

All users of are advised to upgrade to this updated package, which fixes these bugs.

4.116. xinetd

4.116.1. RHSA-2013:1302 — Low: xinetd security and bug fix update

An updated xinetd package that fixes one security issue and two bugs is now available for Red Hat Enterprise Linux 5.

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

The xinetd package provides a secure replacement for inetd, the Internet services daemon. xinetd provides access control for all services based on the address of the remote host and/or on time of access, and can prevent denial-of-access attacks.

Security Fix

CVE-2012-0862

When xinetd services are configured with the "TCPMUX" or "TCPMUXPLUS" type, and the tcpmux-server service is enabled, those services are accessible via port 1. It was found that enabling the tcpmux-server service (it is disabled by default) allowed every xinetd service, including those that are not configured with the "TCPMUX" or "TCPMUXPLUS" type, to be accessible via port 1. This could allow a remote attacker to bypass intended firewall restrictions.

Red Hat would like to thank Thomas Swan of FedEx for reporting this issue.

Bug Fixes

BZ#852274

Prior to this update, a file descriptor array in the service.c source file was not handled as expected. As a consequence, some of the descriptors remained open when xinetd was under heavy load. Additionally, the system log was filled with a large number of messages that took up a lot of disk space over time. This update modifies the xinetd code to handle the file descriptors correctly and messages no longer fill the system log.

BZ#811000

Prior to this update, services were disabled permanently when their CPS limit was reached. As a consequence, a failed bind operation could occur when xinetd attempted to restart the service. This update adds additional logic that attempts to restart the service. Now, the service is only disabled if xinetd cannot restart the service after 30 attempts.

All users of xinetd are advised to upgrade to this updated package, which contains backported patches to correct these issues.

4.117. xorg-x11-drv-ati

4.117.1. RHBA-2013:1360 — xorg-x11-drv-ati bug fix update

Updated xorg-x11-drv-ati packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The xorg-x11-drv-ati packages provide a driver for ATI graphics cards for the X.Org implementation of the X Window System.

Bug Fixes

BZ#274811

When connecting a digital monitor which supported a maximum 1600x1200 resolution, a Radeon

driver would set the 1600x1200@24bit mode for output. However, this mode was out of the ES1000 GPU's capacity, and, consequently, caused video corruption to occur. This update adds a clock range check to restrict output mode within the chip's capability, and video corruption no longer occurs in the described scenario.

BZ#703354

Prior to this update, there were issues with the ATI HD4xxx GPU series that in some cases prevented an Xserver from running. Consequently, the screen displayed a "load video device: ATI RV730 PRO Radeon HD 4650" error message, and users were left without graphics. With this update, Red Hat Enterprise Linux version 5.10 has graphics working properly on the HD4xxx GPU series, and error messages are no longer received.

Users of xorg-x11-drv-ati are advised to upgrade to these updated packages, which fix these bugs.

4.118. xorg-x11-server

4.118.1. RHBA-2013:1362 — xorg-x11-server bug fix update

Updated xorg-x11-server packages that fix one bug are now available for Red Hat Enterprise Linux 5.

X.Org is an open source implementation of the X Window System. It provides the basic low-level functionality that full-fledged graphical user interfaces are designed upon.

Bug Fix

BZ#960950

After booting the system in runlevel 5, if the user tried to the kill X.org process, it became unresponsive, displaying the following error:

Fatal server error: Caught signal 11. Server aborting

This bug occurred in several scenarios, including switching the runlevel, using the Ctrl+Alt+Backspace combination to terminate the X session, or after rebooting the system from the GUI. After this update, X.Org no longer crashes while being killed.

Users of xorg-x11-server are advised to upgrade to these updated packages, which fix this bug.

4.119. xulrunner

4.119.1. RHSA-2013:0614 — Critical: xulrunner security update

Updated xulrunner packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

XULRunner provides the XUL Runtime environment for applications using the Gecko layout engine.

Security Fix

CVE-2013-0787

A flaw was found in the way XULRunner handled malformed web content. A web page containing malicious content could cause an application linked against XULRunner (such as Mozilla Firefox) to crash or execute arbitrary code with the privileges of the user running the application.

Red Hat would like to thank the Mozilla project for reporting this issue. Upstream acknowledges VUPEN Security via the TippingPoint Zero Day Initiative project as the original reporter.

For technical details regarding this flaw, refer to the Mozilla security advisories.

All XULRunner users should upgrade to these updated packages, which correct this issue. After installing the update, applications using XULRunner must be restarted for the changes to take effect.

4.120. ypserv

4.120.1. RHBA-2013:0660 — ypserv bug fix update

Updated ypserv packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The ypserv packages provide the Network Information Service (NIS) server. NIS is a system that provides network information such as login names, passwords, home directories, and group information to all the machines on a network.

Bug Fix

BZ#920111

Previously, the ypserv utility allocated large amounts of virtual memory when parsing XDR requests, but failed to free that memory if the request was not parsed successfully. Consequently, memory leaks occurred. With this update, a patch has been provided to free the already allocated memory when the parsing of a request fails and, as a result, memory leaks no longer occur.

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

4.121. yum-rhn-plugin

4.121.1. RHBA-2013:1327 — yum-rhn-plugin bug fix update

An updated yum-rhn-plugin package that fixes three bugs is now available for Red Hat Enterprise Linux 5.

The yum-rhn-plugin package allows the Yum package manager to access content from Red Hat Network (RHN).

Bug Fixes

BZ#853799

Prior to this update, applying automatic updates with the yum-rhn-plugin utility on a Red Hat Enterprise Linux 5 system could fail with an "empty transaction" error message. This was because the cached version of yum-rhn-plugin metadata was not up-to-date. With this update, yum-rhn-plugin downloads new metadata if available, ensuring that all packages are available for download.

BZ#951592

Red Hat Network (RHN) Proxy did not work properly if separated from a parent by a slow network. Consequently, users who attempted to download larger repodata files and RPM packages experienced timeouts. This update changes both RHN Proxy and Red Hat Enterprise Linux RHN Client to allow all communications to honor a configured timeout value for connections.

BZ#845241

Scheduled package installation actions failed if the package was already installed. This caused dependent actions to fail to execute, such as configuration deployments, which in turn lead to the failure of automated installation using kickstart. This update ensures that a package installation action does not fail if the package is already installed.

Users of yum-rhn-plugin are advised to upgrade to this updated package, which fixes these bugs.

4.122. zsh

4.122.1. RHBA-2013:1337 — zsh bug fix update

Updated zsh packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The zsh shell is a command interpreter which can be used as an interactive login shell and as a shell script command processor. Zsh resembles the ksh shell (the Korn shell), but includes many enhancements. Zsh supports command line editing, built-in spelling correction, programmable command completion, shell functions (with autoloading), a history mechanism, and more.

Bug Fix

BZ#813219

Due to a missing error flag check, validating the syntax of a comparison expression (one that compares values with the less-than or greater-than signs) as the condition of a while loop did not exit and return a single error message as expected, but entered an infinite loop instead, returning a "bad math expression" error message at every iteration of the loop. With this update, in case an evaluated loop condition is not valid, the script that uses it exits after the first iteration of the loop with an error message and exit code 2.

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

Appendix A. Package Manifest

This document is a record of all package changes since the last minor update of &PROD; &PRODVER;.

A.1. Server

A.1.1. Added Packages

gcc-libraries-4.8.0-5.1.1.el5

- Group: System Environment/Libraries
- Summary: GCC runtime libraries
- Description: This package contains various GCC runtime libraries, such as libatomic, or libitm.

mysql51-1-9.el5

- Group: Applications/File
- Summary: Package that installs mysql51
- Description: This is the main package for mysql51 Software Collection, which installs necessary packages to use MySQL 5.1 server. Version 5.1 is needed to upgrade to MySQL 5.5 server but you should not use it in production environment. Software Collections allow to install more versions of the same package by using alternative directory structure. Install this package if you want to migrate to MySQL 5.5 server on your system.

mysql51-mysql-5.1.70-1.el5

- Group: Applications/Databases
- Summary: MySQL client programs and shared libraries
- Description: MySQL is a multi-user, multi-threaded SQL database server. MySQL is a client/server implementation consisting of a server daemon (mysqld) and many different client programs and libraries. The base package contains the standard MySQL client programs and generic MySQL files.

mysql55-1-12.el5

- Group: Applications/File
- Summary: Package that installs mysql55
- Description: This is the main package for mysql55 Software Collection, which installs necessary packages to use MySQL 5.5 server. Software Collections allow to install more versions of the same package by using alternative directory structure. Install this package if you want to use MySQL 5.5 server on your system.

mysql55-mysql-5.5.32-3.el5

- Group: Applications/Databases
- Summary: MySQL client programs and shared libraries

- Description: MySQL is a multi-user, multi-threaded SQL database server. MySQL is a client/server implementation consisting of a server daemon (mysqld) and many different client programs and libraries. The base package contains the standard MySQL client programs and generic MySQL files.

python-dateutil-1.2-3.el5

- Group: Development/Languages
- Summary: Powerful extensions to the standard datetime module
- Description: The dateutil module provides powerful extensions to the standard datetime module available in Python 2.3+.

python-kerberos-1.1-11.el5

- Group: System Environment/Libraries
- Summary: A high-level wrapper for Kerberos (GSSAPI) operations
- Description: This Python package is a high-level wrapper for Kerberos (GSSAPI) operations. The goal is to avoid having to build a module that wraps the entire Kerberos.framework, and instead offer a limited set of functions that do what is needed for client/serverKerberos authentication based on <http://www.ietf.org/rfc/rfc4559.txt>. Much of the C-code here is adapted from Apache's mod_auth_kerb-5.0rc7.

python-lxml-2.0.11-2.el5

- Group: Development/Libraries
- Summary: ElementTree-like Python bindings for libxml2 and libxslt
- Description: lxml provides a Python binding to the libxslt and libxml2 libraries. It follows the ElementTree API as much as possible in order to provide a more Pythonic interface to libxml2 and libxslt than the default bindings. In particular, lxml deals with Python Unicode strings rather than encoded UTF-8 and handles memory management automatically, unlike the default bindings.

redhat-support-lib-python-0.9.5-9.el5

- Group: Development/Libraries
- Summary: Red Hat Support Software Development Library
- Description: This package contains the Red Hat Support Software Development Library. Red Hat customers can use the library to easily integrate their help desk solutions, IT infrastructure, etc. with the services provided by the Red Hat Customer Portal. The library provided by this package is an abstraction layer that simplifies interactions with the Red Hat Customer Portal. Simply create an instance of the API by providing the necessary authorization credentials, then use the API object to interact with the Red Hat Customer Portal. Some of the interactions supported by this API include, but are not limited to, automatic diagnostic services on log files, knowledge base searching, support case creation, attach files to support cases, view the status of support cases, entitlement viewing, etc.

redhat-support-tool-0.9.5-8.el5

- Group: Development/Libraries
- Summary: Tool for console access to Red Hat subscriber services
- Description: This package contains the Red Hat Support Tool. The Red Hat Support Tool

provides console based access to Red Hat's subscriber services. These services include, but are not limited to, console based access to knowledge-base solutions, case management, automated diagnostic services, etc.

A.1.2. Dropped Packages

libitm-4.7.0-5.1.1.el5

- Group: System Environment/Libraries
- Summary: The GNU Transactional Memory library
- Description: This package contains the GNU Transactional Memory library which is a GCC transactional memory support runtime library.

A.1.3. Updated Packages

am-utils-6.1.5-4.1.el5 - am-utils-6.1.5-7.el5

- Group: System Environment/Daemons
- Summary: Automount utilities including an updated version of Amd.
- Description: Am-utils includes an updated version of Amd, the popular BSD automounter. An automounter is a program which maintains a cache of mounted filesystems. Filesystems are mounted when they are first referenced by the user and unmounted after a certain period of inactivity. Amd supports a variety of filesystems, including NFS, UFS, CD-ROMS and local drives. You should install am-utils if you need a program for automatically mounting and unmounting filesystems.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

anaconda-11.1.2.259-1 - anaconda-11.1.2.263-2

- Group: Applications/System
- Summary: Graphical system installer
- Description: The anaconda package contains the program which was used to install your system. These files are of little use on an already installed system.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

aspell-0.60.3-12 - aspell-0.60.3-13

- Group: Applications/Text
- Summary: A spelling checker.
- Description: GNU Aspell is a spell checker designed to eventually replace Ispell. It can either be used as a library or as an independent spell checker. Its main feature is that it does a much better job of coming up with possible suggestions than just about any other spell checker out there for the English language, including Ispell and Microsoft Word. It also has many other technical enhancements over Ispell such as using shared memory for dictionaries and intelligently handling personal dictionaries when more than one Aspell process is open at once.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

autofs-5.0.1-0.rc2.177.el5 - autofs-5.0.1-0.rc2.183.el5

- Group: System Environment/Daemons
- Summary: A tool for automatically mounting and unmounting filesystems.
- Description: autofs is a daemon which automatically mounts filesystems when you use them, and unmounts them later when you are not using them. This can include network filesystems, CD-ROMs, floppies, and so forth.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

axis-1.2.1-2jpp.6 - axis-1.2.1-2jpp.7.el5_9

- Group: Development/Libraries/Java
- Summary: A SOAP implementation in Java
- Description: Apache AXIS is an implementation of the SOAP ("Simple Object Access Protocol") submission to W3C. From the draft W3C specification: SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses. This project is a follow-on to the Apache SOAP project.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bash-3.2-32.el5 - bash-3.2-32.el5_9.1

- Group: System Environment/Shells
- Summary: The GNU Bourne Again shell (bash) version 3.2
- Description: The GNU Bourne Again shell (Bash) is a shell or command language interpreter that is compatible with the Bourne shell (sh). Bash incorporates useful features from the Korn shell (ksh) and the C shell (csh). Most sh scripts can be run by bash without modification. This package (bash) contains bash version 3.2, which improves POSIX compliance over previous versions.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bind-9.3.6-20.P1.el5_8.5 - bind-9.3.6-20.P1.el5_8.6

- Group: System Environment/Daemons
- Summary: The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server.
- Description: BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bind97-9.7.0-17.P2.el5 - bind97-9.7.0-17.P2.el5_9.2

- Group: System Environment/Daemons
- Summary: The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server
- Description: BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

binutils-2.17.50.0.6-20.el5_8.3 - binutils-2.17.50.0.6-26.el5

- Group: Development/Tools
- Summary: A GNU collection of binary utilities.
- Description: Binutils is a collection of binary utilities, including ar (for creating, modifying and extracting from archives), as (a family of GNU assemblers), gprof (for displaying call graph profile data), ld (the GNU linker), nm (for listing symbols from object files), objcopy (for copying and translating object files), objdump (for displaying information from object files), ranlib (for

generating an index for the contents of an archive), size (for listing the section sizes of an object or archive file), strings (for listing printable strings from files), strip (for discarding symbols), and addr2line (for converting addresses to file and line).

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

boost-1.33.1-15.el5 - boost-1.33.1-16.el5_9

- Group: System Environment/Libraries
- Summary: The Boost C++ Libraries
- Description: Boost provides free peer-reviewed portable C++ source libraries. The emphasis is on libraries which work well with the C++ Standard Library, in the hopes of establishing "existing practice" for extensions and providing reference implementations so that the Boost libraries are suitable for eventual standardization. (Some of the libraries have already been proposed for inclusion in the C++ Standards Committee's upcoming C++ Standard Library Technical Report.)
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ccid-1.3.8-1.el5 - ccid-1.3.8-2.el5

- Group: System Environment/Libraries
- Summary: Generic USB CCID smart card reader driver
- Description: Generic USB CCID (Chip/Smart Card Interface Devices) driver.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

clustermon-0.12.1-7.el5 - clustermon-0.12.1-10.el5

- Group: System Environment/Base
- Summary: Monitoring and management of Red Hat Enterprise Linux Cluster Suite
- Description: This package contains Red Hat Enterprise Linux Cluster Suite SNMP/CIM module/agent/provider.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cman-2.0.115-109.el5 - cman-2.0.115-118.el5

- Group: System Environment/Base
- Summary: cman - The Cluster Manager
- Description: cman - The Cluster Manager
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

conga-0.12.2-64.el5 - conga-0.12.2-68.el5

- Group: System Environment/Base

- Summary: Remote Management System
- Description: Conga is a project developing management system for remote stations. It consists of luci, https frontend, and ricci, secure daemon that dispatches incoming messages to underlying management modules.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

coolkey-1.1.0-15.el5 - coolkey-1.1.0-16.1.el5

- Group: System Environment/Libraries
- Summary: CoolKey PKCS #11 module
- Description: Linux Driver support for the CoolKey and CAC products.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cpio-2.6-25.el5 - cpio-2.6-26.el5

- Group: Applications/Archiving
- Summary: A GNU archiving program.
- Description: GNU cpio copies files into or out of a cpio or tar archive. Archives are files which contain a collection of other files plus information about them, such as their file name, owner, timestamps, and access permissions. The archive can be another file on the disk, a magnetic tape, or a pipe. GNU cpio supports the following archive formats: binary, old ASCII, new ASCII, crc, HPUX binary, HPUX old ASCII, old tar and POSIX.1 tar. By default, cpio creates binary format archives, so that they are compatible with older cpio programs. When it is extracting files from archives, cpio automatically recognizes which kind of archive it is reading and can read archives created on machines with a different byte-order. Install cpio if you need a program to manage file archives.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

crash-5.1.8-1.el5 - crash-5.1.8-2.el5_9

- Group: Development/Debuggers
- Summary: Kernel crash and live system analysis utility
- Description: The core analysis suite is a self-contained tool that can be used to investigate either live systems, kernel core dumps created from the netdump, diskdump and kdump packages from Red Hat Linux, the mcore kernel patch offered by Mission Critical Linux, or the LKCD kernel patch.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cups-1.3.7-30.el5 - cups-1.3.7-30.el5_9.3

- Group: System Environment/Daemons
- Summary: Common Unix Printing System
- Description: The Common UNIX Printing System provides a portable printing layer for UNIX® operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users. CUPS provides the System V and Berkeley command-line interfaces.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

curl-7.15.5-15.el5 - curl-7.15.5-17.el5_9

- Group: Applications/Internet
- Summary: A utility for getting files from remote servers (FTP, HTTP, and others).
- Description: cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and Dict servers, using any of the supported protocols. cURL is designed to work without user interaction or any kind of interactivity. cURL offers many useful capabilities, like proxy support, user authentication, FTP upload, HTTP post, and file transfer resume.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dbus-1.1.2-16.el5_7 - dbus-1.1.2-21.el5

- Group: System Environment/Libraries
- Summary: D-BUS message bus
- Description: D-BUS is a system for sending messages between applications. It is used both for the systemwide message bus service, and as a per-user-login-session messaging facility.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dbus-glib-0.73-10.el5_5 - dbus-glib-0.73-11.el5_9

- Group: System Environment/Libraries

- Summary: GLib bindings for D-Bus
- Description: D-Bus add-on library to integrate the standard D-Bus library with the GLib thread abstraction and main loop.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

devhelp-0.12-22.el5 - devhelp-0.12-23.el5_9

- Group: Development/Tools
- Summary: API document browser
- Description: An API document browser for GNOME 2.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

device-mapper-multipath-0.4.7-54.el5 - device-mapper-multipath-0.4.7-59.el5

- Group: System Environment/Base
- Summary: Tools to manage multipath devices using device-mapper.
- Description: device-mapper-multipath provides tools to manage multipath devices by instructing the device-mapper multipath kernel module what to do. The tools are : * multipath : Scan the system for multipath devices and assemble them. * multipathd : Detects when paths fail and execs multipath to update things.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dhcp-3.0.5-31.el5_8.1 - dhcp-3.0.5-33.el5_9

- Group: System Environment/Daemons
- Summary: DHCP (Dynamic Host Configuration Protocol) server and relay agent.
- Description: DHCP (Dynamic Host Configuration Protocol) is a protocol which allows individual devices on an IP network to get their own network configuration information (IP address, subnetmask, broadcast address, etc.) from a DHCP server. The overall purpose of DHCP is to make it easier to administer a large network. The dhcp package includes the ISC DHCP service and relay agent. To use DHCP on your network, install a DHCP service (or relay agent), and on clients run a DHCP client daemon. The dhcp package provides the ISC DHCP service and relay agent.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dovecot-1.0.7-7.el5_7.1 - dovecot-1.0.7-8.el5_9.1

- Group: System Environment/Daemons
- Summary: Dovecot Secure imap server
- Description: Dovecot is an IMAP server for Linux/UNIX-like systems, written with security primarily in mind. It also contains a small POP3 server. It supports mail in either of maildir or mbox formats.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

e2fsprogs-1.39-35.el5 - e2fsprogs-1.39-36.el5_9

- Group: System Environment/Base
- Summary: Utilities for managing the second and third extended (ext2/ext3) filesystems
- Description: The e2fsprogs package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in second and third extended (ext2/ext3) filesystems. E2fsprogs contains e2fsck (used to repair filesystem inconsistencies after an unclean shutdown), mke2fs (used to initialize a partition to contain an empty ext2 filesystem), debugfs (used to examine the internal structure of a filesystem, to manually repair a corrupted filesystem, or to create test cases for e2fsck), tune2fs (used to modify filesystem parameters), and most of the other core ext2fs filesystem utilities. You should install the e2fsprogs package if you need to manage the performance of an ext2 and/or ext3 filesystem.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

elinks-0.11.1-6.el5_4.1 - elinks-0.11.1-8.el5_9

- Group: Applications/Internet
- Summary: A text-mode Web browser.
- Description: Links is a text-based Web browser. Links does not display any images, but it does support frames, tables and most other HTML tags. Links' advantage over graphical browsers is its speed--Links starts and exits quickly and swiftly displays Web pages.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

esc-1.1.0-13.el5_8.2 - esc-1.1.0-14.el5_9.1

- Group: Applications/Internet
- Summary: Enterprise Security Client Smart Card Client
- Description: Enterprise Security Client allows the user to enroll and manage their cryptographic smartcards.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

firefox-10.0.11-1.el5_8 - firefox-17.0.8-1.el5_9

- Group: Applications/Internet
- Summary: Mozilla Firefox Web browser
- Description: Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.
- Added Dependencies:
  - python-devel
  - python-setuptools
  - sqlite-devel
  - xulrunner-devel >= 17.0.8
- Removed Dependencies:
  - xulrunner-devel >= 10.0.11-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

freetype-2.2.1-31.el5_8.1 - freetype-2.2.1-32.el5_9.1

- Group: System Environment/Libraries
- Summary: A free and portable font rendering engine

- Description: The FreeType engine is a free and portable font rendering engine, developed to provide advanced font support for a variety of platforms and environments. FreeType is a library which can open and manages font files as well as efficiently load, hint and render individual glyphs. FreeType is not a font server or a complete text-rendering library.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdm-2.16.0-59.el5 - gdm-2.16.0-59.el5_9.1

- Group: User Interface/X
- Summary: The GNOME Display Manager.
- Description: Gdm (the GNOME Display Manager) is a highly configurable reimplementation of xdm, the X Display Manager. Gdm allows you to log into your system with the X Window System running and supports running several different X sessions on your local machine at the same time.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gfs2-utils-0.1.62-35.el5 - gfs2-utils-0.1.62-39.el5

- Group: System Environment/Kernel
- Summary: Utilities for managing the global filesystem (GFS)
- Description: The gfs2-utils package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in GFS filesystems.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

glibc-2.5-107 - glibc-2.5-118

- Group: System Environment/Libraries
- Summary: The GNU libc libraries.
- Description: The glibc package contains standard libraries which are used by multiple programs on the system. In order to save disk space and memory, as well as to make upgrading easier, common system code is kept in one place and shared between programs. This particular package contains the most important sets of shared libraries: the standard C library and the standard math library. Without these two libraries, a Linux system will not function.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gnome-vfs2-2.16.2-10.el5 - gnome-vfs2-2.16.2-12.el5_9

- Group: System Environment/Libraries
- Summary: The GNOME virtual file-system libraries
- Description: GNOME VFS is the GNOME virtual file system. It is the foundation of the Nautilus file manager. It provides a modular architecture and ships with several modules that implement support for file systems, http, ftp, and others. It provides a URI-based API, backend supporting asynchronous file operations, a MIME type manipulation library, and other features.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

gnutls-1.4.1-10.el5 - gnutls-1.4.1-10.el5_9.2

- Group: System Environment/Libraries
- Summary: A TLS protocol implementation.
- Description: GnuTLS is a project that aims to develop a library which provides a secure layer, over a reliable transport layer. Currently the GnuTLS library implements the proposed standards by the IETF's TLS working group.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gtk2-2.10.4-29.el5 - gtk2-2.10.4-30.el5

- Group: System Environment/Libraries
- Summary: The GIMP ToolKit (GTK+), a library for creating GUIs for X
- Description: GTK+ is a multi-platform toolkit for creating graphical user interfaces. Offering a complete set of widgets, GTK+ is suitable for projects ranging from small one-off tools to complete application suites.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

httpd-2.2.3-74.el5 - httpd-2.2.3-82.el5_9

- Group: System Environment/Daemons
- Summary: Apache HTTP Server
- Description: The Apache HTTP Server is a powerful, efficient, and extensible web server.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hwdata-0.213.28-1.el5 - hwdata-0.213.28-3.el5

- Group: System Environment/Base
- Summary: Hardware identification and configuration data
- Description: hwdata contains various hardware identification and configuration data, such as the pci.ids database and MonitorsDb databases.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hypervkvpd-0-0.7.el5 - hypervkvpd-0-0.7.el5_9.3

- Group: System Environment/Daemons
- Summary: HyperV key value pair (KVP) daemon
- Description: Hypervkvpd is an implementation of HyperV key value pair (KVP) functionality for Linux.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

initscripts-8.45.42-1.el5_8.1 - initscripts-8.45.44-3.el5

- Group: System Environment/Base
- Summary: The inittab file and the /etc/init.d scripts.
- Description: The initscripts package contains the basic system scripts used to boot your Red Hat system, change runlevels, and shut the system down cleanly. Initscripts also contains the scripts that activate and deactivate most network interfaces.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ipa-client-2.1.3-4.el5 - ipa-client-2.1.3-7.el5

- Group: System Environment/Base
- Summary: IPA authentication for use on clients
- Description: IPA is an integrated solution to provide centrally managed Identity (machine, user, virtual machines, groups, authentication credentials), Policy (configuration settings, access control information) and Audit (events, logs, analysis thereof).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

jakarta-commons-httpclient-3.0-7jpp.1 - jakarta-commons-httpclient-3.0-7jpp.2

- Group: Development/Libraries/Java
- Summary: Jakarta Commons HTTPClient Package
- Description: The Hyper-Text Transfer Protocol (HTTP) is perhaps the most significant protocol

used on the Internet today. Web services, network-enabled appliances and the growth of network computing continue to expand the role of the HTTP protocol beyond user-driven web browsers, and increase the number of applications that may require HTTP support. Although the java.net package provides basic support for accessing resources via HTTP, it doesn't provide the full flexibility or functionality needed by many applications. The Jakarta Commons HTTP Client component seeks to fill this void by providing an efficient, up-to-date, and feature-rich package implementing the client side of the most recent HTTP standards and recommendations. Designed for extension while providing robust support for the base HTTP protocol, the HTTP Client component may be of interest to anyone building HTTP-aware client applications such as web browsers, web service clients, or systems that leverage or extend the HTTP protocol for distributed communication.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

java-1.6.0-openjdk-1.6.0.0-1.30.1.11.5.el5 - java-1.6.0-openjdk-1.6.0.0-1.41.1.11.11.90.el5_9

- Group: Development/Languages
- Summary: OpenJDK Runtime Environment
- Description: The OpenJDK runtime environment.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

java-1.7.0-openjdk-1.7.0.9-2.3.3.el5.1 - java-1.7.0-openjdk-1.7.0.25-2.3.10.5.el5_9

- Group: Development/Languages
- Summary: OpenJDK Runtime Environment
- Description: The OpenJDK runtime environment.
- Added Dependencies:

    - gcc-c++
    - java7-devel >= 1:1.7.0
    - zip
    - zlib > 1.2.3-6
  - Removed Dependencies:
    - ecj
    - freetype-devel
    - java-devel >= 1:1.6.0
    - xorg-x11-fonts-misc
    - xorg-x11-server-Xvfb
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

kernel-2.6.18-348.el5 - kernel-2.6.18-371.el5

  - Group: System Environment/Kernel
  - Summary: The Linux kernel (the core of the Linux operating system)
  - Description: The kernel package contains the Linux kernel (vmlinuz), the core of any Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.
  - No added dependencies
  - No removed dependencies
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

kexec-tools-1.102pre-161.el5 - kexec-tools-1.102pre-164.el5

  - Group: Applications/System
  - Summary: The kexec/kdump userspace component.

- Description: kexec-tools provides /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of the kernel's kexec feature.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

krb5-1.6.1-70.el5 - krb5-1.6.1-70.el5_9.2

- Group: System Environment/Libraries
- Summary: The Kerberos network authentication system.
- Description: Kerberos V5 is a trusted-third-party network authentication system, which can improve your network's security by eliminating the insecure practice of cleartext passwords.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ksh-20100621-12.el5 - ksh-20100621-18.el5

- Group: Applications/Shells
- Summary: The Original ATT Korn Shell
- Description: KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language, which is upward compatible with "sh" (the Bourne Shell).
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kvm-83-262.el5 - kvm-83-262.el5_9.4

- Group: Development/Tools
- Summary: Kernel-based Virtual Machine
- Description: KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware. Using KVM, one can run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, etc.
- Added Dependencies:
  - kernel-debug-devel = 2.6.18-348.6.1.el5
  - kernel-devel = 2.6.18-348.6.1.el5
- Removed Dependencies:
  - kernel-debug-devel = 2.6.18-339.el5
  - kernel-devel = 2.6.18-339.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libtevent-0.9.8-10.el5 - libtevent-0.9.18-2.el5

- Group: System Environment/Daemons
- Summary: Talloc-based, event-driven mainloop
- Description: Tevent is an event system based on the talloc memory management library. Tevent has support for many event types, including timers, signals, and the classic file descriptor events. Tevent also provide helpers to deal with asynchronous code providing the tevent_req (Tevent Request) functions.
- Added Dependencies:
  - docbook-style-xsl
  - doxygen

    - libxslt
    - pkgconfig
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libtiff-3.8.2-15.el5_8 - libtiff-3.8.2-18.el5_8

- Group: System Environment/Libraries
- Summary: Library of functions for manipulating TIFF format image files
- Description: The libtiff package contains a library of functions for manipulating TIFF (Tagged Image File Format) image format files. TIFF is a widely used file format for bitmapped images. TIFF files usually end in the .tif extension and they are often quite large. The libtiff package should be installed if you need to manipulate TIFF format image files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libvirt-0.8.2-29.el5 - libvirt-0.8.2-29.el5_9.1

- Group: Development/Libraries
- Summary: Library providing a simple API virtualization
- Description: Libvirt is a C toolkit to interact with the virtualization capabilities of recent versions of Linux (and other OSes).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

libxml2-2.6.26-2.1.15.el5_8.5 - libxml2-2.6.26-2.1.21.el5_9.3

- Group: Development/Libraries
- Summary: Library providing XML and HTML support
- Description: This library allows to manipulate XML files. It includes support to read, modify and write XML and HTML files. There is DTDs support this includes parsing and validation even with complex DtDs, either at parse time or later once the document has been modified. The output can be a simple SAX stream or and in-memory DOM like representations. In this case one can use the built-in XPath and XPointer implementation to select subnodes or ranges. A flexible Input/Output mechanism is available, with existing HTTP and FTP modules and combined to an URI library.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ltrace-0.5-13.45svn.el5_7.12 - ltrace-0.5-20.45svn.el5

- Group: Development/Debuggers
- Summary: Tracks runtime library calls from dynamically linked executables.
- Description: Ltrace is a debugging program which 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. Ltrace can also intercept and print system calls executed by the process. You should install ltrace if you need a sysadmin tool for tracking the execution of processes.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

lvm2-2.02.88-10.el5 - lvm2-2.02.88-12.el5

- Group: System Environment/Base
- Summary: Userland logical volume management tools
- Description: LVM2 includes all of the support for handling read/write operations on physical volumes (hard disks, RAID-Systems, magneto optical, etc., multiple devices (MD), see mdadd(8) or even loop devices, see losetup(8)), creating volume groups (kind of virtual disks) from one or more physical volumes and creating one or more logical volumes (kind of logical partitions) in volume groups.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

man-pages-overrides-5.9.2-2.el5 - man-pages-overrides-5.10.2-1.el5

- Group: Documentation
- Summary: Complementary and updated manual pages
- Description: A collection of manual ("man") pages to complement other packages or update those contained therein. Always have the latest version of this package installed.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mesa-6.5.1-7.10.el5 - mesa-6.5.1-7.11.el5_9

- Group: System Environment/Libraries
- Summary: Mesa graphics libraries
- Description: Mesa

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

microcode_ctl-1.17-3.el5 - microcode_ctl-1.17-5.el5

- Group: System Environment/Base
- Summary: Tool to update x86/x86-64 CPU microcode.
- Description: microcode_ctl - updates the microcode on Intel x86/x86-64 CPU's
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mkinitrd-5.1.19.6-79.el5 - mkinitrd-5.1.19.6-80.el5_9

- Group: System Environment/Base
- Summary: Creates an initial ramdisk image for preloading modules.
- Description: Mkinitrd creates filesystem images for use as initial ramdisk (initrd) images. These ramdisk images are often used to preload the block device modules (SCSI or RAID) needed to access the root filesystem. In other words, generic kernels can be built without drivers for any SCSI adapters which load the SCSI driver as a module. Since the kernel needs to read those modules, but in this case it isn't able to address the SCSI adapter, an initial ramdisk is used. The initial ramdisk is loaded by the operating system loader (normally LILO) and is available to the kernel as soon as the ramdisk is loaded. The ramdisk image loads the proper SCSI adapter and allows the kernel to mount the root filesystem. The mkinitrd program creates such a ramdisk using information found in the /etc/modules.conf file.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

module-init-tools-3.3-0.pre3.1.60.el5_5.1 - module-init-tools-3.3-0.pre3.1.63.el5

- Group: System Environment/Kernel
- Summary: Kernel module management utilities.
- Description: The modutils package includes various programs needed for automatic loading and unloading of modules under 2.6 and later kernels, as well as other module management programs. Device drivers and filesystems are two examples of loaded and unloaded modules.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mysql-5.0.95-3.el5 - mysql-5.0.95-5.el5_9

- Group: Applications/Databases
- Summary: MySQL client programs and shared libraries
- Description: MySQL is a multi-user, multi-threaded SQL database server. MySQL is a client/server implementation consisting of a server daemon (mysqld) and many different client programs and libraries. The base package contains the MySQL client programs, the client shared libraries, and generic MySQL files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nfs-utils-1.0.9-66.el5 - nfs-utils-1.0.9-70.el5

- Group: System Environment/Daemons
- Summary: NFS utilities and supporting clients and daemons for the kernel NFS server.
- Description: The nfs-utils package provides a daemon for the kernel NFS server and related tools, which provides a much higher level of performance than the traditional Linux NFS server used by most users. This package also contains the showmount program. Showmount queries the mount daemon on a remote host for information about the NFS (Network File System) server on the remote host. For example, showmount can display the clients which are mounted on that host. This package also contains the mount.nfs and umount.nfs program.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nspr-4.9.1-6.el5 - nspr-4.9.5-2.el5

- Group: System Environment/Libraries
- Summary: Netscape Portable Runtime
- Description: NSPR provides platform independence for non-GUI operating system facilities. These facilities include threads, thread synchronization, normal file and network I/O, interval timing and calendar time, basic memory management (malloc and free) and shared library linking.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nss-3.13.5-8.el5 - nss-3.14.3-18.el5

- Group: System Environment/Libraries
- Summary: Network Security Services

- Description: Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications. Applications built with NSS can support SSL v2 and v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/MIME, X.509 v3 certificates, and other security standards.
- Added Dependencies:
  - binutils220
  - nspr-devel >= 4.9.5
  - sqlite-devel
- Removed Dependencies:
  - nspr-devel >= 4.9.1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nss_ldap-253-51.el5 - nss_ldap-253-51.el5_9.1

- Group: System Environment/Base
- Summary: NSS library and PAM module for LDAP.
- Description: This package includes two LDAP access clients: nss_ldap and pam_ldap. Nss_ldap is a set of C library extensions that allow X.500 and LDAP directory servers to be used as a primary source of aliases, ethers, groups, hosts, networks, protocol, users, RPCs, services, and shadow passwords (instead of or in addition to using flat files or NIS). Pam_ldap is a module for Linux-PAM that supports password changes, V2 clients, Netscape's SSL, ypldapd, Netscape Directory Server password policies, access authorization, and crypted hashes.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openmotif-2.3.1-6.1.el5_8 - openmotif-2.3.1-7.2.el5

- Group: System Environment/Libraries

- Summary: Open Motif runtime libraries and executables.
- Description: This is the Open Motif 2.3.1 runtime environment. It includes the Motif shared libraries, needed to run applications which are dynamically linked against Motif, and the Motif Window Manager "mwm".
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openscap-0.8.0-1.el5 - openscap-0.9.11-1.el5

- Group: System Environment/Libraries
- Summary: Set of open source libraries enabling integration of the SCAP line of standards
- Description: OpenSCAP is a set of open source libraries providing an easier path for integration of the SCAP line of standards. SCAP is a line of standards managed by NIST with the goal of providing a standard language for the expression of Computer Network Defense related information.
- Added Dependencies:
  - curl-devel >= 7.12.0
  - libxml2-devel >= 2.6.26-2.1.21.el5_9.2
- Removed Dependencies:
  - libnl-devel
  - libxml2-devel
  - perl
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openssl-0.9.8e-22.el5_8.4 - openssl-0.9.8e-26.el5_9.1

- Group: System Environment/Libraries

- Summary: The OpenSSL toolkit
- Description: The OpenSSL toolkit provides support for secure communications between machines. OpenSSL includes a certificate management tool and shared libraries which provide various cryptographic algorithms and protocols.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openswan-2.6.32-4.el5 - openswan-2.6.32-5.el5_9

- Group: System Environment/Daemons
- Summary: IPSEC implementation with IKEv1 and IKEv2 keying protocols
- Description: Openswan is a free implementation of IPsec & IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the ipsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network or VPN. This package contains the daemons and userland tools for setting up Openswan. It supports the NETKEY/XFRM IPsec kernel stack that exists in the default Linux kernel. Openswan 2.6.x also supports IKEv2 (RFC4306)
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pcre-6.6-6.el5_6.1 - pcre-6.6-9.el5

- Group: System Environment/Libraries
- Summary: Perl-compatible regular expression library
- Description: Perl-compatible regular expression library. PCRE has its own native API, but a set of "wrapper" functions that are based on the POSIX API are also supplied in the library libpcreposix. Note that this just provides a POSIX calling interface to PCRE: the regular

expressions themselves still follow Perl syntax and semantics. The header file for the POSIX-style functions is called pcreposix.h.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perl-5.8.8-38.el5_8 - perl-5.8.8-41.el5

- Group: Development/Languages
- Summary: The Perl programming language
- Description: Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text. Perl's hallmarks are practicality and efficiency. While it is used to do a lot of different things, Perl's most common applications are system administration utilities and web programming. A large proportion of the CGI scripts on the web are written in Perl. You need the perl package installed on your system so that your system can handle Perl scripts. Install this package if you want to program in Perl or enable your system to handle Perl scripts.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perl-IO-Socket-SSL-1.01-1.fc6 - perl-IO-Socket-SSL-1.01-2.el5

- Group: Development/Libraries
- Summary: Perl library for transparent SSL
- Description: This module is a true drop-in replacement for IO::Socket::INET that uses SSL to encrypt data before it is transferred to a remote server or client. IO::Socket::SSL supports all the extra features that one needs to write a full-featured SSL client or server application: multiple SSL contexts, cipher selection, certificate verification, and SSL version selection. As an extra bonus, it works perfectly with mod_perl.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php-5.1.6-39.el5_8 - php-5.1.6-40.el5_9

- Group: Development/Languages
- Summary: The PHP HTML-embedded scripting language. (PHP: Hypertext Preprocessor)
- Description: PHP is an HTML-embedded scripting language that allows developers to write dynamically generated web pages. PHP is ideal for writing database-enabled websites, with built-in integration for several commercial and non-commercial database management systems. PHP is often used as a replacement for CGI scripts. The php package contains a module that adds support for the PHP language to the Apache HTTP Server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php53-5.3.3-13.el5_8 - php53-5.3.3-21.el5

- Group: Development/Languages
- Summary: PHP scripting language for creating dynamic web sites
- Description: PHP is an HTML-embedded scripting language. PHP attempts to make it easy for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP coding is probably as a replacement for CGI scripts. The php package contains the module which adds support for the PHP language to Apache HTTP Server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

piranha-0.8.4-25.el5 - piranha-0.8.4-25.el5_9.1

- Group: System Environment/Base
- Summary: Cluster administation tools
- Description: Various tools to administer and configure the Linux Virtual Server as well as heartbeating and failover components. The LVS is a dynamically adjusted kernel routing mechanism that provides load balancing primarily for web and ftp servers though other services are supported.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

policycoreutils-1.33.12-14.8.el5 - policycoreutils-1.33.12-14.13.el5

- Group: System Environment/Base
- Summary: SELinux policy core utilities.
- Description: Security-enhanced Linux is a feature of the Linux® kernel and a number of utilities with enhanced security functionality designed to add mandatory access controls to Linux. The Security-enhanced Linux kernel contains new architectural components originally developed to improve the security of the Flask operating system. These architectural components provide general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement®, Role-based Access Control, and Multi-level Security. policycoreutils contains the policy core utilities that are required for basic operation of a SELinux system. These utilities include load_policy to load policies, setfiles to label filesystems, newrole to switch roles, and run_init to run /etc/init.d scripts in the proper context.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

poppler-0.5.4-19.el5 - poppler-0.5.4-19.el5_9.2

- Group: Development/Libraries
- Summary: PDF rendering library
- Description: Poppler, a PDF rendering library, it's a fork of the xpdf PDF viewer developed by Derek Noonburg of Glyph and Cog, LLC.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

procps-3.2.7-22.el5 - procps-3.2.7-26.el5

- Group: Applications/System
- Summary: System and process monitoring utilities.
- Description: The procps package contains a set of system utilities that provide system information. Procps includes ps, free, skill, pkill, pgrep, snice, tload, top, uptime, vmstat, w, watch and pdwx. The ps command displays a snapshot of running processes. The top command provides a repetitive update of the statuses of running processes. The free command displays the amounts of free and used memory on your system. The skill command sends a terminate command (or another specified signal) to a specified set of processes. The snice command is used to change the scheduling priority of specified processes. The tload command prints a graph of the current system load average to a specified tty. The uptime command displays the current time, how long the system has been running, how many users are logged on, and system load averages for the past one, five, and fifteen minutes. The w command displays a list of the users who are currently logged on and what they are running. The watch program watches a running program. The vmstat command displays virtual memory statistics about processes, memory, paging, block I/O, traps, and CPU activity. The pwdx command reports the current working directory of a process or processes.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

python-rhsm-1.0.10-1.el5 - python-rhsm-1.8.17-1.el5

- Group: Development/Libraries
- Summary: A Python library to communicate with a Red Hat Unified Entitlement Platform
- Description: A small library for communicating with the REST interface of a Red Hat Unified Entitlement Platform. This interface is used for the management of system entitlements, certificates, and access to content.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rdesktop-1.6.0-7 - rdesktop-1.6.0-8

- Group: User Interface/Desktops
- Summary: X client for remote desktop into Windows Terminal Server
- Description: rdesktop is an open source client for Windows NT Terminal Server and Windows 2000 & 2003 Terminal Services, capable of natively speaking Remote Desktop Protocol (RDP) in order to present the user's NT desktop. Unlike Citrix ICA, no server extensions are required.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-release-5Server-5.9.0.2 - redhat-release-5Server-5.10.0.4

- Group: System Environment/Base
- Summary: Red Hat Enterprise Linux release file

- Description: Red Hat Enterprise Linux release files
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-release-notes-5Server-46 - redhat-release-notes-5Server-48

- Group: System Environment/Base
- Summary: Red Hat Enterprise Linux release notes files
- Description: Red Hat Enterprise Linux release notes files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rgmanager-2.0.52-37.el5 - rgmanager-2.0.52-47.el5

- Group: System Environment/Base
- Summary: Open Source HA Resource Group Failover for Red Hat Enterprise Linux
- Description: Red Hat Resource Group Manager provides high availability of critical server applications in the event of planned or unplanned system downtime.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

rhn-client-tools-0.4.20-86.el5 - rhn-client-tools-0.4.20.1-6.el5

- Group: System Environment/Base
- Summary: Support programs and libraries for Red Hat Network
- Description: Red Hat Network Client Tools provides programs and libraries to allow your system to receive software updates from Red Hat Network.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhnlib-2.5.22-7.el5 - rhnlib-2.5.22.1-6.el5

- Group: Development/Libraries
- Summary: Python libraries for the RHN project
- Description: rhnlib is a collection of python modules used by the Red Hat Network (http://rhn.redhat.com) software.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rpm-4.4.2.3-31.el5 - rpm-4.4.2.3-34.el5

- Group: System Environment/Base
- Summary: The RPM package management system
- Description: The RPM Package Manager (RPM) is a powerful command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages. Each software package consists of an archive of files along with

information about the package like its version, a description, etc.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ruby-1.8.5-27.el5 - ruby-1.8.5-31.el5_9

- Group: Development/Languages
- Summary: An interpreter of object-oriented scripting language
- Description: Ruby is the interpreted scripting language for quick and easy object-oriented programming. It has many features to process text files and to do system management tasks (as in Perl). It is simple, straight-forward, and extensible.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

s390utils-1.8.1-17.el5 - s390utils-1.8.1-18.el5

- Group: System Environment/Base
- Summary: Linux/390 specific utilities
- Description: This package contains utilities related to Linux for S/390. The most important programs contained in this package are: - The cmstools suite to list, check, copy and cat files from a CMS volume. - chccwdev, a script to generically change attributes of a ccw device. - dasdfmt, which is used to low-level format eckd-dasds with either the classic linux disk layout or the new z/OS compatible disk layout. - dasdview, which displays DASD and VTOC information and dumps the content of a DASD to the console. - fdasd, which is used to create or modify partitions on eckd-dasds formatted with the z/OS compatible disk layout. - osasnmpd, a subagent for net-snmp to access the OSA hardware. - qetharp to query and purge address data in the OSA and HiperSockets hardware - qethconf to configure IBM QETH function IPA, VIPA and Proxy ARP. - src_vipa.sh to start applications using VIPA capabilities - tunedasd, a tool to adjust tunable parameters on DASD devices - vmconvert, a tool to convert vm dumps to lkcd

compatible dumps. - vmcp, a tool to send CP commands from a Linux guest to the VM. - vmur, a tool to work with z/VM spool file queues (reader, punch, printer). - zipl, which is used to make either dasds or tapes bootable for system IPL or system dump. - zdump, which is used to retrieve system dumps from either tapes or dasds. - ziomon tools to collect data for zfcp performance analysis and report. - iucvterm, a z/VM IUCV terminal applications. - cpuplugd, a daemon that manages CPU and memory resources based on a set of rules. - dumpconf, the dump device used for system dump in case a kernel panic occurs. - mon_statd, pair of Linux - z/VM monitoring daemons. - ipl_tools, tool set to configure and list reipl and shutdown actions. - cpi, a service to set the system and sysplex names from the Linux guest to the HMC/SE using the Control Program Identification feature.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

samba3x-3.6.6-0.129.el5 - samba3x-3.6.6-0.136.el5

- Group: System Environment/Daemons
- Summary: Server and Client software to interoperate with Windows machines
- Description: Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB/CIFS server that can be used to provide network services to SMB/CIFS clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.
- Added Dependencies:
  - libtevent-devel >= 0.9.18
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

scl-utils-20120927-2.el5 - scl-utils-20120927-8.el5

- Group: Applications/File
- Summary: Utilities for alternative packaging
- Description: Run-time utility for alternative packaging.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

selinux-policy-2.4.6-338.el5 - selinux-policy-2.4.6-346.el5

- Group: System Environment/Base
- Summary: SELinux policy configuration
- Description: SELinux Reference Policy - modular.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sos-1.7-9.62.el5 - sos-1.7-9.66.el5

- Group: Development/Libraries
- Summary: A set of tools to gather troubleshooting information from a system
- Description: Sos is a set of tools that gathers information about system hardware and configuration. The information can then be used for diagnostic purposes and debugging. Sos is commonly used to help support technicians and developers.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

spamassassin-3.3.1-2.el5 - spamassassin-3.3.1-4.el5

- Group: Applications/Internet
- Summary: Spam filter for email which can be invoked from mail delivery agents.
- Description: SpamAssassin provides you with a way to reduce if not completely eliminate Unsolicited Commercial Email (SPAM) from your incoming email. It can be invoked by a MDA such as sendmail or postfix, or can be called from a procmail script, .forward file, etc. It uses a genetic-algorithm evolved scoring system to identify messages which look spammy, then adds headers to the message so they can be filtered by the user's mail reading software. This distribution includes the spamd/spamc components which create a server that considerably speeds processing of mail. To enable spamassassin, if you are receiving mail locally, simply add this line to your ~/.procmailrc: INCLUDERC=/etc/mail/spamassassin/spamassassin-default.rc To filter spam for all users, add that line to /etc/procmailrc (creating if necessary).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sqlite-3.3.6-6 - sqlite-3.3.6-7

- Group: Applications/Databases
- Summary: Library that implements an embeddable SQL database engine
- Description: SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete database is stored in a single disk file. The API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and flexibility of an SQL database without the administrative hassles of supporting a separate database server. Version 2 and version 3 binaries are named to permit each to be installed on a single host
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sssd-1.5.1-58.el5 - sssd-1.5.1-70.el5

- Group: Applications/System
- Summary: System Security Services Daemon
- Description: Provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable backend system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

subscription-manager-1.0.24-1.el5 - subscription-manager-1.8.22-1.el5

- Group: System Environment/Base
- Summary: Tools and libraries for subscription and repository management
- Description: The Subscription Manager package provides programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat entitlement platform.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

subscription-manager-migration-data-1.11.2.7-1.el5 - subscription-manager-migration-data-1.11.3.2-1.el5

- Group: System Environment/Base
- Summary: RHN Classic to RHSM migration data
- Description: This package provides certificates for migrating a system from RHN Classic to RHSM.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

subversion-1.6.11-10.el5_8 - subversion-1.6.11-11.el5_9

- Group: Development/Tools
- Summary: Modern Version Control System designed to replace CVS
- Description: Subversion is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes. Subversion only stores the differences between versions, instead of every complete file. Subversion is intended to be a compelling replacement for CVS.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sudo-1.7.2p1-22.el5 - sudo-1.7.2p1-28.el5

- Group: Applications/System
- Summary: Allows restricted root access for specified users.
- Description: Sudo (superuser do) allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root while logging all commands and arguments. Sudo operates on a per-command basis. It is not a replacement for the shell. Features include: the ability to restrict what commands a user may run on a per-host basis,

copious logging of each command (providing a clear audit trail of who did what), a configurable timeout of the sudo command, and the ability to use the same configuration file (sudoers) on many different machines.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-cluster-1.0.57-16 - system-config-cluster-1.0.57-17

- Group: Applications/System
- Summary: system-config-cluster is a utility which allows you to manage cluster configuration in a graphical setting.
- Description: system-config-cluster is a utility which allows you to manage cluster configuuration in a graphical setting.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-kdump-1.0.14-4.el5 - system-config-kdump-1.0.14-5.el5_9

- Group: System Environment/Base
- Summary: A graphical interface for configuring kernel crash dumping
- Description: system-config-kdump is a graphical tool for configuring kernel crash dumping via kdump and kexec.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-lvm-1.1.5-13.el5 - system-config-lvm-1.1.5-14.el5

- Group: Applications/System
- Summary: A utility for graphically configuring Logical Volumes
- Description: system-config-lvm is a utility for graphically configuring Logical Volumes
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tomcat5-5.5.23-0jpp.37.el5 - tomcat5-5.5.23-0jpp.40.el5_9

- Group: Networking/Daemons
- Summary: Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API
- Description: Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Tomcat is developed in an open and participatory environment and released under the Apache Software License. Tomcat is intended to be a collaboration of the best-of-breed developers from around the world. We invite you to participate in this open development project. To learn more about getting involved, click here.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tzdata-2012i-2.el5 - tzdata-2013c-2.el5

- Group: System Environment/Base
- Summary: Timezone data
- Description: This package contains data files with rules for various time zones around the world.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

wpa_supplicant-0.5.10-9.el5 - wpa_supplicant-0.5.10-10.el5

- Group: System Environment/Base
- Summary: WPA/WPA2/IEEE 802.1X Supplicant
- Description: wpa_supplicant is a WPA Supplicant for Linux, BSD and Windows with support for WPA and WPA2 (IEEE 802.11i / RSN). Supplicant is the IEEE 802.1X/WPA component that is used in the client stations. It implements key negotiation with a WPA Authenticator and it controls the roaming and IEEE 802.11 authentication/association of the wlan driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xen-3.0.3-142.el5 - xen-3.0.3-142.el5_9.3

- Group: Development/Libraries
- Summary: Xen is a virtual machine monitor
- Description: This package contains the Xen tools and management daemons needed to run virtual machines on x86, x86_64, and ia64 systems. Information on how to use Xen can be found at the Xen project pages. The Xen system also requires the Xen hypervisor and domain-0 kernel, which can be found in the kernel-xen* package. Virtualization can be used to run

multiple operating systems on one physical system, for purposes of hardware consolidation, hardware abstraction, or to test untrusted applications in a sandboxed environment.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xinetd-2.3.14-17.el5 - xinetd-2.3.14-19.el5

- Group: System Environment/Daemons
- Summary: A secure replacement for inetd.
- Description: Xinetd is a secure replacement for inetd, the Internet services daemon. Xinetd provides access control for all services based on the address of the remote host and/or on time of access and can prevent denial-of-access attacks. Xinetd provides extensive logging, has no limit on the number of server arguments, and lets you bind specific services to specific IP addresses on your host machine. Each service has its own specific configuration file for Xinetd; the files are located in the /etc/xinetd.d directory.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-ati-6.6.3-3.33.el5 - xorg-x11-drv-ati-6.6.3-3.35.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 ati video driver
- Description: X.Org X11 ati video driver.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-server-1.1.1-48.100.el5 - xorg-x11-server-1.1.1-48.101.el5

- Group: User Interface/X
- Summary: X.Org X11 X server
- Description: X.Org X11 X server
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xulrunner-10.0.11-1.el5_8 - xulrunner-17.0.8-3.el5_9

- Group: Applications/Internet
- Summary: XUL Runtime for Gecko Applications
- Description: XULRunner is a Mozilla runtime package that can be used to bootstrap XUL+XPCOM applications that are as rich as Firefox and Thunderbird. It provides mechanisms for installing, upgrading, and uninstalling these applications. XULRunner also provides libxul, a solution which allows the embedding of Mozilla technologies in other projects and products.
- Added Dependencies:
  - nspr-devel >= 4.9.2
  - nss-devel >= 3.13.6
  - python-devel
  - python-setuptools
  - sqlite-devel
- Removed Dependencies:
  - nspr-devel >= 4.8.9
  - nss-devel >= 3.13.1

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yelp-2.16.0-29.el5 - yelp-2.16.0-30.el5_9

- Group: Applications/System
- Summary: A system documentation reader from the Gnome project
- Description: Yelp is the Gnome 2 help/documentation browser. It is designed to help you browse all the documentation on your system in one central tool.
- Added Dependencies:
  - gecko-devel-unstable >= 17.0
- Removed Dependencies:
  - gecko-devel-unstable >= 10.0
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ypserv-2.19-9.el5_8.1 - ypserv-2.19-10.el5_9.1

- Group: System Environment/Daemons
- Summary: The NIS (Network Information Service) server.
- Description: The Network Information Service (NIS) is a system that provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can allow users to log in on any machine on the network, as long as the machine has the NIS client programs running and the user's password is recorded in the NIS passwd database. NIS was formerly known as Sun Yellow Pages (YP). This package provides the NIS server, which will need to be running on your network. NIS clients do not need to be running the server. Install ypserv if you need an NIS server for your network. You also need to install the yp-tools and ypbind packages on any NIS client machines.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yum-rhn-plugin-0.5.4-29.el5 - yum-rhn-plugin-0.5.4.1-7.el5

- Group: System Environment/Base
- Summary: RHN support for yum
- Description: This yum plugin provides support for yum to access a Red Hat Network server for software updates.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

zsh-4.2.6-8.el5 - zsh-4.2.6-9.el5

- Group: System Environment/Shells
- Summary: A powerful interactive shell
- Description: The zsh shell is a command interpreter usable as an interactive login shell and as a shell script command processor. Zsh resembles the ksh shell (the Korn shell), but includes many enhancements. Zsh supports command line editing, built-in spelling correction, programmable command completion, shell functions (with autoloading), a history mechanism, and more.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

A.2. Client

A.2.1. Added Packages

gcc-libraries-4.8.0-5.1.1.el5

- Group: System Environment/Libraries
- Summary: GCC runtime libraries
- Description: This package contains various GCC runtime libraries, such as libatomic, or libitm.

mysql51-1-9.el5

- Group: Applications/File
- Summary: Package that installs mysql51
- Description: This is the main package for mysql51 Software Collection, which installs necessary packages to use MySQL 5.1 server. Version 5.1 is needed to upgrade to MySQL 5.5 server but you should not use it in production environment. Software Collections allow to install more versions of the same package by using alternative directory structure. Install this package if you want to migrate to MySQL 5.5 server on your system.

mysql51-mysql-5.1.70-1.el5

- Group: Applications/Databases
- Summary: MySQL client programs and shared libraries
- Description: MySQL is a multi-user, multi-threaded SQL database server. MySQL is a client/server implementation consisting of a server daemon (mysqld) and many different client programs and libraries. The base package contains the standard MySQL client programs and generic MySQL files.

mysql55-1-12.el5

- Group: Applications/File
- Summary: Package that installs mysql55
- Description: This is the main package for mysql55 Software Collection, which installs necessary packages to use MySQL 5.5 server. Software Collections allow to install more versions of the same package by using alternative directory structure. Install this package if you want to use MySQL 5.5 server on your system.

mysql55-mysql-5.5.32-3.el5

- Group: Applications/Databases
- Summary: MySQL client programs and shared libraries
- Description: MySQL is a multi-user, multi-threaded SQL database server. MySQL is a client/server implementation consisting of a server daemon (mysqld) and many different client programs and libraries. The base package contains the standard MySQL client programs and generic MySQL files.

python-dateutil-1.2-3.el5

- Group: Development/Languages

- Summary: Powerful extensions to the standard datetime module
- Description: The dateutil module provides powerful extensions to the standard datetime module available in Python 2.3+.

python-kerberos-1.1-11.el5

- Group: System Environment/Libraries
- Summary: A high-level wrapper for Kerberos (GSSAPI) operations
- Description: This Python package is a high-level wrapper for Kerberos (GSSAPI) operations. The goal is to avoid having to build a module that wraps the entire Kerberos.framework, and instead offer a limited set of functions that do what is needed for client/serverKerberos authentication based on <http://www.ietf.org/rfc/rfc4559.txt>. Much of the C-code here is adapted from Apache's mod_auth_kerb-5.0rc7.

python-lxml-2.0.11-2.el5

- Group: Development/Libraries
- Summary: ElementTree-like Python bindings for libxml2 and libxslt
- Description: lxml provides a Python binding to the libxslt and libxml2 libraries. It follows the ElementTree API as much as possible in order to provide a more Pythonic interface to libxml2 and libxslt than the default bindings. In particular, lxml deals with Python Unicode strings rather than encoded UTF-8 and handles memory management automatically, unlike the default bindings.

redhat-support-lib-python-0.9.5-9.el5

- Group: Development/Libraries
- Summary: Red Hat Support Software Development Library
- Description: This package contains the Red Hat Support Software Development Library. Red Hat customers can use the library to easily integrate their help desk solutions, IT infrastructure, etc. with the services provided by the Red Hat Customer Portal. The library provided by this package is an abstraction layer that simplifies interactions with the Red Hat Customer Portal. Simply create an instance of the API by providing the necessary authorization credentials, then use the API object to interact with the Red Hat Customer Portal. Some of the interactions supported by this API include, but are not limited to, automatic diagnostic services on log files, knowledge base searching, support case creation, attach files to support cases, view the status of support cases, entitlement viewing, etc.

redhat-support-tool-0.9.5-8.el5

- Group: Development/Libraries
- Summary: Tool for console access to Red Hat subscriber services
- Description: This package contains the Red Hat Support Tool. The Red Hat Support Tool provides console based access to Red Hat's subscriber services. These services include, but are not limited to, console based access to knowledge-base solutions, case management, automated diagnostic services, etc.

A.2.2. Dropped Packages

libitm-4.7.0-5.1.1.el5

- Group: System Environment/Libraries
- Summary: The GNU Transactional Memory library
- Description: This package contains the GNU Transactional Memory library which is a GCC transactional memory support runtime library.

A.2.3. Updated Packages

am-utils-6.1.5-4.1.el5 - am-utils-6.1.5-7.el5

- Group: System Environment/Daemons
- Summary: Automount utilities including an updated version of Amd.
- Description: Am-utils includes an updated version of Amd, the popular BSD automounter. An automounter is a program which maintains a cache of mounted filesystems. Filesystems are mounted when they are first referenced by the user and unmounted after a certain period of inactivity. Amd supports a variety of filesystems, including NFS, UFS, CD-ROMS and local drives. You should install am-utils if you need a program for automatically mounting and unmounting filesystems.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

anaconda-11.1.2.259-1 - anaconda-11.1.2.263-2

- Group: Applications/System
- Summary: Graphical system installer
- Description: The anaconda package contains the program which was used to install your system. These files are of little use on an already installed system.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

aspell-0.60.3-12 - aspell-0.60.3-13

- Group: Applications/Text
- Summary: A spelling checker.
- Description: GNU Aspell is a spell checker designed to eventually replace Ispell. It can either be used as a library or as an independent spell checker. Its main feature is that it does a much better job of coming up with possible suggestions than just about any other spell checker out there for the English language, including Ispell and Microsoft Word. It also has many other technical enhancements over Ispell such as using shared memory for dictionaries and intelligently handling personal dictionaries when more than one Aspell process is open at once.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

autofs-5.0.1-0.rc2.177.el5 - autofs-5.0.1-0.rc2.183.el5

- Group: System Environment/Daemons
- Summary: A tool for automatically mounting and unmounting filesystems.
- Description: autofs is a daemon which automatically mounts filesystems when you use them, and unmounts them later when you are not using them. This can include network filesystems, CD-ROMs, floppies, and so forth.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

axis-1.2.1-2jpp.6 - axis-1.2.1-2jpp.7.el5_9

- Group: Development/Libraries/Java
- Summary: A SOAP implementation in Java

- Description: Apache AXIS is an implementation of the SOAP ("Simple Object Access Protocol") submission to W3C. From the draft W3C specification: SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses. This project is a follow-on to the Apache SOAP project.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bash-3.2-32.el5 - bash-3.2-32.el5_9.1

- Group: System Environment/Shells
- Summary: The GNU Bourne Again shell (bash) version 3.2
- Description: The GNU Bourne Again shell (Bash) is a shell or command language interpreter that is compatible with the Bourne shell (sh). Bash incorporates useful features from the Korn shell (ksh) and the C shell (csh). Most sh scripts can be run by bash without modification. This package (bash) contains bash version 3.2, which improves POSIX compliance over previous versions.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bind-9.3.6-20.P1.el5_8.5 - bind-9.3.6-20.P1.el5_8.6

- Group: System Environment/Daemons
- Summary: The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server.

- Description: BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

bind97-9.7.0-17.P2.el5 - bind97-9.7.0-17.P2.el5_9.2

- Group: System Environment/Daemons
- Summary: The Berkeley Internet Name Domain (BIND) DNS (Domain Name System) server
- Description: BIND (Berkeley Internet Name Domain) is an implementation of the DNS (Domain Name System) protocols. BIND includes a DNS server (named), which resolves host names to IP addresses; a resolver library (routines for applications to use when interfacing with DNS); and tools for verifying that the DNS server is operating properly.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

binutils-2.17.50.0.6-20.el5_8.3 - binutils-2.17.50.0.6-26.el5

- Group: Development/Tools
- Summary: A GNU collection of binary utilities.
- Description: Binutils is a collection of binary utilities, including ar (for creating, modifying and extracting from archives), as (a family of GNU assemblers), gprof (for displaying call graph profile data), ld (the GNU linker), nm (for listing symbols from object files), objcopy (for copying and translating object files), objdump (for displaying information from object files), ranlib (for generating an index for the contents of an archive), size (for listing the section sizes of an object or archive file), strings (for listing printable strings from files), strip (for discarding symbols), and addr2line (for converting addresses to file and line).

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

boost-1.33.1-15.el5 - boost-1.33.1-16.el5_9

- Group: System Environment/Libraries
- Summary: The Boost C++ Libraries
- Description: Boost provides free peer-reviewed portable C++ source libraries. The emphasis is on libraries which work well with the C++ Standard Library, in the hopes of establishing "existing practice" for extensions and providing reference implementations so that the Boost libraries are suitable for eventual standardization. (Some of the libraries have already been proposed for inclusion in the C++ Standards Committee's upcoming C++ Standard Library Technical Report.)
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ccid-1.3.8-1.el5 - ccid-1.3.8-2.el5

- Group: System Environment/Libraries
- Summary: Generic USB CCID smart card reader driver
- Description: Generic USB CCID (Chip/Smart Card Interface Devices) driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

cman-2.0.115-109.el5 - cman-2.0.115-118.el5

- Group: System Environment/Base
- Summary: cman - The Cluster Manager
- Description: cman - The Cluster Manager
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

coolkey-1.1.0-15.el5 - coolkey-1.1.0-16.1.el5

- Group: System Environment/Libraries
- Summary: CoolKey PKCS #11 module
- Description: Linux Driver support for the CoolKey and CAC products.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cpio-2.6-25.el5 - cpio-2.6-26.el5

- Group: Applications/Archiving
- Summary: A GNU archiving program.
- Description: GNU cpio copies files into or out of a cpio or tar archive. Archives are files which contain a collection of other files plus information about them, such as their file name, owner, timestamps, and access permissions. The archive can be another file on the disk, a magnetic

tape, or a pipe. GNU cpio supports the following archive formats: binary, old ASCII, new ASCII, crc, HPUX binary, HPUX old ASCII, old tar and POSIX.1 tar. By default, cpio creates binary format archives, so that they are compatible with older cpio programs. When it is extracting files from archives, cpio automatically recognizes which kind of archive it is reading and can read archives created on machines with a different byte-order. Install cpio if you need a program to manage file archives.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

crash-5.1.8-1.el5 - crash-5.1.8-2.el5_9

- Group: Development/Debuggers
- Summary: Kernel crash and live system analysis utility
- Description: The core analysis suite is a self-contained tool that can be used to investigate either live systems, kernel core dumps created from the netdump, diskdump and kdump packages from Red Hat Linux, the mcore kernel patch offered by Mission Critical Linux, or the LKCD kernel patch.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cups-1.3.7-30.el5 - cups-1.3.7-30.el5_9.3

- Group: System Environment/Daemons
- Summary: Common Unix Printing System
- Description: The Common UNIX Printing System provides a portable printing layer for UNIX® operating systems. It has been developed by Easy Software Products to promote a standard printing solution for all UNIX vendors and users. CUPS provides the System V and Berkeley command-line interfaces.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

curl-7.15.5-15.el5 - curl-7.15.5-17.el5_9

- Group: Applications/Internet
- Summary: A utility for getting files from remote servers (FTP, HTTP, and others).
- Description: cURL is a tool for getting files from FTP, HTTP, Gopher, Telnet, and Dict servers, using any of the supported protocols. cURL is designed to work without user interaction or any kind of interactivity. cURL offers many useful capabilities, like proxy support, user authentication, FTP upload, HTTP post, and file transfer resume.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dbus-1.1.2-16.el5_7 - dbus-1.1.2-21.el5

- Group: System Environment/Libraries
- Summary: D-BUS message bus
- Description: D-BUS is a system for sending messages between applications. It is used both for the systemwide message bus service, and as a per-user-login-session messaging facility.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

dbus-glib-0.73-10.el5_5 - dbus-glib-0.73-11.el5_9

- Group: System Environment/Libraries
- Summary: GLib bindings for D-Bus
- Description: D-Bus add-on library to integrate the standard D-Bus library with the GLib thread abstraction and main loop.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

devhelp-0.12-22.el5 - devhelp-0.12-23.el5_9

- Group: Development/Tools
- Summary: API document browser
- Description: An API document browser for GNOME 2.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

device-mapper-multipath-0.4.7-54.el5 - device-mapper-multipath-0.4.7-59.el5

- Group: System Environment/Base
- Summary: Tools to manage multipath devices using device-mapper.
- Description: device-mapper-multipath provides tools to manage multipath devices by instructing the device-mapper multipath kernel module what to do. The tools are : * multipath : Scan the system for multipath devices and assemble them. * multipathd : Detects when paths fail and execs multipath to update things.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dhcp-3.0.5-31.el5_8.1 - dhcp-3.0.5-33.el5_9

- Group: System Environment/Daemons
- Summary: DHCP (Dynamic Host Configuration Protocol) server and relay agent.
- Description: DHCP (Dynamic Host Configuration Protocol) is a protocol which allows individual devices on an IP network to get their own network configuration information (IP address, subnetmask, broadcast address, etc.) from a DHCP server. The overall purpose of DHCP is to make it easier to administer a large network. The dhcp package includes the ISC DHCP service and relay agent. To use DHCP on your network, install a DHCP service (or relay agent), and on clients run a DHCP client daemon. The dhcp package provides the ISC DHCP service and relay agent.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

dovecot-1.0.7-7.el5_7.1 - dovecot-1.0.7-8.el5_9.1

- Group: System Environment/Daemons
- Summary: Dovecot Secure imap server
- Description: Dovecot is an IMAP server for Linux/UNIX-like systems, written with security primarily in mind. It also contains a small POP3 server. It supports mail in either of maildir or mbox formats.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

e2fsprogs-1.39-35.el5 - e2fsprogs-1.39-36.el5_9

- Group: System Environment/Base
- Summary: Utilities for managing the second and third extended (ext2/ext3) filesystems
- Description: The e2fsprogs package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in second and third extended (ext2/ext3) filesystems. E2fsprogs contains e2fsck (used to repair filesystem inconsistencies after an unclean shutdown), mke2fs (used to initialize a partition to contain an empty ext2 filesystem), debugfs (used to examine the internal structure of a filesystem, to manually repair a corrupted filesystem, or to create test cases for e2fsck), tune2fs (used to modify filesystem parameters), and most of the other core ext2fs filesystem utilities. You should install the e2fsprogs package if you need to manage the performance of an ext2 and/or ext3 filesystem.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

elinks-0.11.1-6.el5_4.1 - elinks-0.11.1-8.el5_9

- Group: Applications/Internet
- Summary: A text-mode Web browser.
- Description: Links is a text-based Web browser. Links does not display any images, but it does support frames, tables and most other HTML tags. Links' advantage over graphical browsers is its speed--Links starts and exits quickly and swiftly displays Web pages.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

esc-1.1.0-13.el5_8.2 - esc-1.1.0-14.el5_9.1

- Group: Applications/Internet
- Summary: Enterprise Security Client Smart Card Client
- Description: Enterprise Security Client allows the user to enroll and manage their cryptographic smartcards.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

firefox-10.0.11-1.el5_8 - firefox-17.0.8-1.el5_9

- Group: Applications/Internet
- Summary: Mozilla Firefox Web browser
- Description: Mozilla Firefox is an open-source web browser, designed for standards compliance, performance and portability.
- Added Dependencies:
  - python-devel
  - python-setuptools
  - sqlite-devel
  - xulrunner-devel >= 17.0.8
- Removed Dependencies:
  - xulrunner-devel >= 10.0.11-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

freetype-2.2.1-31.el5_8.1 - freetype-2.2.1-32.el5_9.1

- Group: System Environment/Libraries
- Summary: A free and portable font rendering engine
- Description: The FreeType engine is a free and portable font rendering engine, developed to provide advanced font support for a variety of platforms and environments. FreeType is a library which can open and manages font files as well as efficiently load, hint and render individual glyphs. FreeType is not a font server or a complete text-rendering library.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdm-2.16.0-59.el5 - gdm-2.16.0-59.el5_9.1

- Group: User Interface/X
- Summary: The GNOME Display Manager.
- Description: Gdm (the GNOME Display Manager) is a highly configurable reimplementation of xdm, the X Display Manager. Gdm allows you to log into your system with the X Window System running and supports running several different X sessions on your local machine at the same time.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gfs2-utils-0.1.62-35.el5 - gfs2-utils-0.1.62-39.el5

- Group: System Environment/Kernel
- Summary: Utilities for managing the global filesystem (GFS)
- Description: The gfs2-utils package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in GFS filesystems.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

glibc-2.5-107 - glibc-2.5-118

- Group: System Environment/Libraries
- Summary: The GNU libc libraries.
- Description: The glibc package contains standard libraries which are used by multiple programs on the system. In order to save disk space and memory, as well as to make upgrading easier, common system code is kept in one place and shared between programs. This particular package contains the most important sets of shared libraries: the standard C library and the standard math library. Without these two libraries, a Linux system will not function.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gnome-vfs2-2.16.2-10.el5 - gnome-vfs2-2.16.2-12.el5_9

- Group: System Environment/Libraries
- Summary: The GNOME virtual file-system libraries
- Description: GNOME VFS is the GNOME virtual file system. It is the foundation of the Nautilus file manager. It provides a modular architecture and ships with several modules that implement support for file systems, http, ftp, and others. It provides a URI-based API, backend supporting asynchronous file operations, a MIME type manipulation library, and other features.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gnutls-1.4.1-10.el5 - gnutls-1.4.1-10.el5_9.2

- Group: System Environment/Libraries
- Summary: A TLS protocol implementation.
- Description: GnuTLS is a project that aims to develop a library which provides a secure layer, over a reliable transport layer. Currently the GnuTLS library implements the proposed standards by the IETF's TLS working group.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gtk2-2.10.4-29.el5 - gtk2-2.10.4-30.el5

- Group: System Environment/Libraries
- Summary: The GIMP ToolKit (GTK+), a library for creating GUIs for X
- Description: GTK+ is a multi-platform toolkit for creating graphical user interfaces. Offering a complete set of widgets, GTK+ is suitable for projects ranging from small one-off tools to complete application suites.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

httpd-2.2.3-74.el5 - httpd-2.2.3-82.el5_9

- Group: System Environment/Daemons
- Summary: Apache HTTP Server
- Description: The Apache HTTP Server is a powerful, efficient, and extensible web server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hwdata-0.213.28-1.el5 - hwdata-0.213.28-3.el5

- Group: System Environment/Base
- Summary: Hardware identification and configuration data
- Description: hwdata contains various hardware identification and configuration data, such as the pci.ids database and MonitorsDb databases.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hypervkvpd-0-0.7.el5 - hypervkvpd-0-0.7.el5_9.3

- Group: System Environment/Daemons
- Summary: HyperV key value pair (KVP) daemon
- Description: Hypervkvpd is an implementation of HyperV key value pair (KVP) functionality for Linux.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

initscripts-8.45.42-1.el5_8.1 - initscripts-8.45.44-3.el5

- Group: System Environment/Base
- Summary: The inittab file and the /etc/init.d scripts.
- Description: The initscripts package contains the basic system scripts used to boot your Red Hat system, change runlevels, and shut the system down cleanly. Initscripts also contains the scripts that activate and deactivate most network interfaces.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ipa-client-2.1.3-4.el5 - ipa-client-2.1.3-7.el5

- Group: System Environment/Base
- Summary: IPA authentication for use on clients
- Description: IPA is an integrated solution to provide centrally managed Identity (machine, user, virtual machines, groups, authentication credentials), Policy (configuration settings, access control information) and Audit (events, logs, analysis thereof).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

jakarta-commons-httpclient-3.0-7jpp.1 - jakarta-commons-httpclient-3.0-7jpp.2

- Group: Development/Libraries/Java
- Summary: Jakarta Commons HTTPClient Package
- Description: The Hyper-Text Transfer Protocol (HTTP) is perhaps the most significant protocol used on the Internet today. Web services, network-enabled appliances and the growth of network computing continue to expand the role of the HTTP protocol beyond user-driven web browsers, and increase the number of applications that may require HTTP support. Although the java.net package provides basic support for accessing resources via HTTP, it doesn't provide the full flexibility or functionality needed by many applications. The Jakarta Commons HTTP Client component seeks to fill this void by providing an efficient, up-to-date, and feature-rich package implementing the client side of the most recent HTTP standards and recommendations. Designed for extension while providing robust support for the base HTTP protocol, the HTTP Client component may be of interest to anyone building HTTP-aware client applications such as web browsers, web service clients, or systems that leverage or extend the HTTP protocol for distributed communication.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

java-1.6.0-openjdk-1.6.0.0-1.30.1.11.5.el5 - java-1.6.0-openjdk-1.6.0.0-1.41.1.11.11.90.el5_9

- Group: Development/Languages
- Summary: OpenJDK Runtime Environment
- Description: The OpenJDK runtime environment.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

java-1.7.0-openjdk-1.7.0.9-2.3.3.el5.1 - java-1.7.0-openjdk-1.7.0.25-2.3.10.5.el5_9

- Group: Development/Languages

- Summary: OpenJDK Runtime Environment
- Description: The OpenJDK runtime environment.
- Added Dependencies:
  - gcc-c++
  - java7-devel >= 1:1.7.0
  - zip
  - zlib > 1.2.3-6
- Removed Dependencies:
  - ecj
  - freetype-devel
  - java-devel >= 1:1.6.0
  - xorg-x11-fonts-misc
  - xorg-x11-server-Xvfb
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kernel-2.6.18-348.el5 - kernel-2.6.18-371.el5

- Group: System Environment/Kernel
- Summary: The Linux kernel (the core of the Linux operating system)
- Description: The kernel package contains the Linux kernel (vmlinuz), the core of any Linux operating system. The kernel handles the basic functions of the operating system: memory allocation, process allocation, device input and output, etc.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kexec-tools-1.102pre-161.el5 - kexec-tools-1.102pre-164.el5

- Group: Applications/System
- Summary: The kexec/kdump userspace component.
- Description: kexec-tools provides /sbin/kexec binary that facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. This package contains the /sbin/kexec binary and ancillary utilities that together form the userspace component of the kernel's kexec feature.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

krb5-1.6.1-70.el5 - krb5-1.6.1-70.el5_9.2

- Group: System Environment/Libraries
- Summary: The Kerberos network authentication system.
- Description: Kerberos V5 is a trusted-third-party network authentication system, which can improve your network's security by eliminating the insecure practice of cleartext passwords.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ksh-20100621-12.el5 - ksh-20100621-18.el5

- Group: Applications/Shells
- Summary: The Original ATT Korn Shell
- Description: KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language, which is upward compatible with "sh" (the Bourne Shell).

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kvm-83-262.el5 - kvm-83-262.el5_9.4

- Group: Development/Tools
- Summary: Kernel-based Virtual Machine
- Description: KVM (for Kernel-based Virtual Machine) is a full virtualization solution for Linux on x86 hardware. Using KVM, one can run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, etc.
- Added Dependencies:
  - kernel-debug-devel = 2.6.18-348.6.1.el5
  - kernel-devel = 2.6.18-348.6.1.el5
- Removed Dependencies:
  - kernel-debug-devel = 2.6.18-339.el5
  - kernel-devel = 2.6.18-339.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libtevent-0.9.8-10.el5 - libtevent-0.9.18-2.el5

- Group: System Environment/Daemons
- Summary: Talloc-based, event-driven mainloop
- Description: Tevent is an event system based on the talloc memory management library. Tevent has support for many event types, including timers, signals, and the classic file descriptor events. Tevent also provide helpers to deal with asynchronous code providing the tevent_req (Tevent Request) functions.

- Added Dependencies:
  - docbook-style-xsl
  - doxygen
  - libxslt
  - pkgconfig
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libtiff-3.8.2-15.el5_8 - libtiff-3.8.2-18.el5_8

- Group: System Environment/Libraries
- Summary: Library of functions for manipulating TIFF format image files
- Description: The libtiff package contains a library of functions for manipulating TIFF (Tagged Image File Format) image format files. TIFF is a widely used file format for bitmapped images. TIFF files usually end in the .tif extension and they are often quite large. The libtiff package should be installed if you need to manipulate TIFF format image files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libvirt-0.8.2-29.el5 - libvirt-0.8.2-29.el5_9.1

- Group: Development/Libraries
- Summary: Library providing a simple API virtualization
- Description: Libvirt is a C toolkit to interact with the virtualization capabilities of recent versions of Linux (and other OSes).
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libxml2-2.6.26-2.1.15.el5_8.6 - libxml2-2.6.26-2.1.21.el5_9.3

- Group: Development/Libraries
- Summary: Library providing XML and HTML support
- Description: This library allows to manipulate XML files. It includes support to read, modify and write XML and HTML files. There is DTDs support this includes parsing and validation even with complex DtDs, either at parse time or later once the document has been modified. The output can be a simple SAX stream or and in-memory DOM like representations. In this case one can use the built-in XPath and XPointer implementation to select subnodes or ranges. A flexible Input/Output mechanism is available, with existing HTTP and FTP modules and combined to an URI library.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ltrace-0.5-13.45svn.el5_7.12 - ltrace-0.5-20.45svn.el5

- Group: Development/Debuggers
- Summary: Tracks runtime library calls from dynamically linked executables.
- Description: Ltrace is a debugging program which 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. Ltrace can also intercept and print system calls executed by the process. You should install ltrace if you need a sysadmin tool for tracking the execution of processes.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lvm2-2.02.88-10.el5 - lvm2-2.02.88-12.el5

- Group: System Environment/Base
- Summary: Userland logical volume management tools
- Description: LVM2 includes all of the support for handling read/write operations on physical volumes (hard disks, RAID-Systems, magneto optical, etc., multiple devices (MD), see mdadd(8) or even loop devices, see losetup(8)), creating volume groups (kind of virtual disks) from one or more physical volumes and creating one or more logical volumes (kind of logical partitions) in volume groups.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

man-pages-overrides-5.9.2-2.el5 - man-pages-overrides-5.10.2-1.el5

- Group: Documentation
- Summary: Complementary and updated manual pages
- Description: A collection of manual ("man") pages to complement other packages or update those contained therein. Always have the latest version of this package installed.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mesa-6.5.1-7.10.el5 - mesa-6.5.1-7.11.el5_9

- Group: System Environment/Libraries
- Summary: Mesa graphics libraries
- Description: Mesa
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

microcode_ctl-1.17-3.el5 - microcode_ctl-1.17-5.el5

- Group: System Environment/Base
- Summary: Tool to update x86/x86-64 CPU microcode.
- Description: microcode_ctl - updates the microcode on Intel x86/x86-64 CPU's
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mkinitrd-5.1.19.6-79.el5 - mkinitrd-5.1.19.6-80.el5_9

- Group: System Environment/Base
- Summary: Creates an initial ramdisk image for preloading modules.
- Description: Mkinitrd creates filesystem images for use as initial ramdisk (initrd) images. These ramdisk images are often used to preload the block device modules (SCSI or RAID) needed to access the root filesystem. In other words, generic kernels can be built without drivers for any SCSI adapters which load the SCSI driver as a module. Since the kernel needs to read those modules, but in this case it isn't able to address the SCSI adapter, an initial ramdisk is used. The initial ramdisk is loaded by the operating system loader (normally LILO) and is available to the kernel as soon as the ramdisk is loaded. The ramdisk image loads the proper SCSI adapter and allows the kernel to mount the root filesystem. The mkinitrd program creates such a ramdisk using information found in the /etc/modules.conf file.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

module-init-tools-3.3-0.pre3.1.60.el5_5.1 - module-init-tools-3.3-0.pre3.1.63.el5

- Group: System Environment/Kernel
- Summary: Kernel module management utilities.
- Description: The modutils package includes various programs needed for automatic loading and unloading of modules under 2.6 and later kernels, as well as other module management programs. Device drivers and filesystems are two examples of loaded and unloaded modules.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mysql-5.0.95-3.el5 - mysql-5.0.95-5.el5_9

- Group: Applications/Databases
- Summary: MySQL client programs and shared libraries
- Description: MySQL is a multi-user, multi-threaded SQL database server. MySQL is a client/server implementation consisting of a server daemon (mysqld) and many different client programs and libraries. The base package contains the MySQL client programs, the client shared libraries, and generic MySQL files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

nfs-utils-1.0.9-66.el5 - nfs-utils-1.0.9-70.el5

- Group: System Environment/Daemons
- Summary: NFS utilities and supporting clients and daemons for the kernel NFS server.
- Description: The nfs-utils package provides a daemon for the kernel NFS server and related tools, which provides a much higher level of performance than the traditional Linux NFS server used by most users. This package also contains the showmount program. Showmount queries the mount daemon on a remote host for information about the NFS (Network File System) server on the remote host. For example, showmount can display the clients which are mounted on that host. This package also contains the mount.nfs and umount.nfs program.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nspr-4.9.1-6.el5 - nspr-4.9.5-2.el5

- Group: System Environment/Libraries
- Summary: Netscape Portable Runtime
- Description: NSPR provides platform independence for non-GUI operating system facilities. These facilities include threads, thread synchronization, normal file and network I/O, interval timing and calendar time, basic memory management (malloc and free) and shared library linking.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nss-3.13.5-8.el5 - nss-3.14.3-18.el5

- Group: System Environment/Libraries
- Summary: Network Security Services
- Description: Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications. Applications built with NSS can support SSL v2 and v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/MIME, X.509 v3 certificates, and other security standards.
- Added Dependencies:
  - binutils220
  - nspr-devel >= 4.9.5
  - sqlite-devel
- Removed Dependencies:
  - nspr-devel >= 4.9.1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nss_ldap-253-51.el5 - nss_ldap-253-51.el5_9.1

- Group: System Environment/Base
- Summary: NSS library and PAM module for LDAP.
- Description: This package includes two LDAP access clients: nss_ldap and pam_ldap. Nss_ldap is a set of C library extensions that allow X.500 and LDAP directory servers to be used as a primary source of aliases, ethers, groups, hosts, networks, protocol, users, RPCs, services, and shadow passwords (instead of or in addition to using flat files or NIS). Pam_ldap is a module for Linux-PAM that supports password changes, V2 clients, Netscape's SSL, ypldapd, Netscape Directory Server password policies, access authorization, and crypted hashes.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

openmotif-2.3.1-6.1.el5_8 - openmotif-2.3.1-7.2.el5

- Group: System Environment/Libraries
- Summary: Open Motif runtime libraries and executables.
- Description: This is the Open Motif 2.3.1 runtime environment. It includes the Motif shared libraries, needed to run applications which are dynamically linked against Motif, and the Motif Window Manager "mwm".
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openscap-0.8.0-1.el5 - openscap-0.9.11-1.el5

- Group: System Environment/Libraries
- Summary: Set of open source libraries enabling integration of the SCAP line of standards
- Description: OpenSCAP is a set of open source libraries providing an easier path for integration of the SCAP line of standards. SCAP is a line of standards managed by NIST with the goal of providing a standard language for the expression of Computer Network Defense related information.
- Added Dependencies:
  - curl-devel >= 7.12.0
  - libxml2-devel >= 2.6.26-2.1.21.el5_9.2
- Removed Dependencies:
  - libnl-devel
  - libxml2-devel
  - perl
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

openssl-0.9.8e-22.el5_8.4 - openssl-0.9.8e-26.el5_9.1

- Group: System Environment/Libraries
- Summary: The OpenSSL toolkit
- Description: The OpenSSL toolkit provides support for secure communications between machines. OpenSSL includes a certificate management tool and shared libraries which provide various cryptographic algorithms and protocols.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openswan-2.6.32-4.el5 - openswan-2.6.32-5.el5_9

- Group: System Environment/Daemons
- Summary: IPSEC implementation with IKEv1 and IKEv2 keying protocols
- Description: Openswan is a free implementation of IPsec & IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks. Everything passing through the untrusted net is encrypted by the ipsec gateway machine and decrypted by the gateway at the other end of the tunnel. The resulting tunnel is a virtual private network or VPN. This package contains the daemons and userland tools for setting up Openswan. It supports the NETKEY/XFRM IPsec kernel stack that exists in the default Linux kernel. Openswan 2.6.x also supports IKEv2 (RFC4306)
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pcre-6.6-6.el5_6.1 - pcre-6.6-9.el5

- Group: System Environment/Libraries

- Summary: Perl-compatible regular expression library
- Description: Perl-compatible regular expression library. PCRE has its own native API, but a set of "wrapper" functions that are based on the POSIX API are also supplied in the library libpcreposix. Note that this just provides a POSIX calling interface to PCRE: the regular expressions themselves still follow Perl syntax and semantics. The header file for the POSIX-style functions is called pcreposix.h.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perl-5.8.8-38.el5_8 - perl-5.8.8-41.el5

- Group: Development/Languages
- Summary: The Perl programming language
- Description: Perl is a high-level programming language with roots in C, sed, awk and shell scripting. Perl is good at handling processes and files, and is especially good at handling text. Perl's hallmarks are practicality and efficiency. While it is used to do a lot of different things, Perl's most common applications are system administration utilities and web programming. A large proportion of the CGI scripts on the web are written in Perl. You need the perl package installed on your system so that your system can handle Perl scripts. Install this package if you want to program in Perl or enable your system to handle Perl scripts.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perl-IO-Socket-SSL-1.01-1.fc6 - perl-IO-Socket-SSL-1.01-2.el5

- Group: Development/Libraries
- Summary: Perl library for transparent SSL
- Description: This module is a true drop-in replacement for IO::Socket::INET that uses SSL to encrypt data before it is transferred to a remote server or client. IO::Socket::SSL supports all

the extra features that one needs to write a full-featured SSL client or server application: multiple SSL contexts, cipher selection, certificate verification, and SSL version selection. As an extra bonus, it works perfectly with mod_perl.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php-5.1.6-39.el5_8 - php-5.1.6-40.el5_9

- Group: Development/Languages
- Summary: The PHP HTML-embedded scripting language. (PHP: Hypertext Preprocessor)
- Description: PHP is an HTML-embedded scripting language that allows developers to write dynamically generated web pages. PHP is ideal for writing database-enabled websites, with built-in integration for several commercial and non-commercial database management systems. PHP is often used as a replacement for CGI scripts. The php package contains a module that adds support for the PHP language to the Apache HTTP Server.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

php53-5.3.3-13.el5_8 - php53-5.3.3-21.el5

- Group: Development/Languages
- Summary: PHP scripting language for creating dynamic web sites
- Description: PHP is an HTML-embedded scripting language. PHP attempts to make it easy for developers to write dynamically generated webpages. PHP also offers built-in database integration for several commercial and non-commercial database management systems, so writing a database-enabled webpage with PHP is fairly simple. The most common use of PHP coding is probably as a replacement for CGI scripts. The php package contains the module which adds support for the PHP language to Apache HTTP Server.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pidgin-2.6.6-11.el5.4 - pidgin-2.6.6-17.el5_9.1

- Group: Applications/Internet
- Summary: A Gtk+ based multiprotocol instant messaging client
- Description: Pidgin allows you to talk to anyone using a variety of messaging protocols including AIM, MSN, Yahoo!, Jabber, Bonjour, Gadu-Gadu, ICQ, IRC, Novell Groupwise, QQ, Lotus Sametime, SILC, Simple and Zephyr. These protocols are implemented using a modular, easy to use design. To use a protocol, just add an account using the account editor. Pidgin supports many common features of other clients, as well as many unique features, such as perl scripting, TCL scripting and C plugins. Pidgin is not affiliated with or endorsed by America Online, Inc., Microsoft Corporation, Yahoo! Inc., or ICQ Inc.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

policycoreutils-1.33.12-14.8.el5 - policycoreutils-1.33.12-14.13.el5

- Group: System Environment/Base
- Summary: SELinux policy core utilities.
- Description: Security-enhanced Linux is a feature of the Linux® kernel and a number of utilities with enhanced security functionality designed to add mandatory access controls to Linux. The Security-enhanced Linux kernel contains new architectural components originally developed to improve the security of the Flask operating system. These architectural components provide general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement®, Role-based Access Control, and Multi-level Security. policycoreutils contains the policy core utilities that are required for basic operation of a SELinux system. These utilities include load_policy to load policies, setfiles to label filesystems, newrole to switch roles, and run_init to run /etc/init.d scripts in the proper context.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

poppler-0.5.4-19.el5 - poppler-0.5.4-19.el5_9.2

- Group: Development/Libraries
- Summary: PDF rendering library
- Description: Poppler, a PDF rendering library, it's a fork of the xpdf PDF viewer developed by Derek Noonburg of Glyph and Cog, LLC.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

procps-3.2.7-22.el5 - procps-3.2.7-26.el5

- Group: Applications/System
- Summary: System and process monitoring utilities.
- Description: The procps package contains a set of system utilities that provide system information. Procps includes ps, free, skill, pkill, pgrep, snice, tload, top, uptime, vmstat, w, watch and pdwx. The ps command displays a snapshot of running processes. The top command provides a repetitive update of the statuses of running processes. The free command displays the amounts of free and used memory on your system. The skill command sends a terminate command (or another specified signal) to a specified set of processes. The snice command is used to change the scheduling priority of specified processes. The tload command prints a graph of the current system load average to a specified tty. The uptime command displays the current time, how long the system has been running, how many users are logged on, and system load averages for the past one, five, and fifteen minutes. The w command displays a list of the users who are currently logged on and what they are running. The watch program watches a running program. The vmstat command displays virtual memory statistics about processes, memory, paging, block I/O, traps, and CPU activity. The pwdx command reports the current working directory of a process or processes.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

python-rhsm-1.0.10-1.el5 - python-rhsm-1.8.17-1.el5

- Group: Development/Libraries
- Summary: A Python library to communicate with a Red Hat Unified Entitlement Platform
- Description: A small library for communicating with the REST interface of a Red Hat Unified Entitlement Platform. This interface is used for the management of system entitlements, certificates, and access to content.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rdesktop-1.6.0-7 - rdesktop-1.6.0-8

- Group: User Interface/Desktops
- Summary: X client for remote desktop into Windows Terminal Server
- Description: rdesktop is an open source client for Windows NT Terminal Server and Windows 2000 & 2003 Terminal Services, capable of natively speaking Remote Desktop Protocol (RDP) in order to present the user's NT desktop. Unlike Citrix ICA, no server extensions are required.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

redhat-release-5Client-5.9.0.2 - redhat-release-5Client-5.10.0.4

- Group: System Environment/Base
- Summary: Red Hat Enterprise Linux release file
- Description: Red Hat Enterprise Linux release files
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

redhat-release-notes-5Client-46 - redhat-release-notes-5Client-48

- Group: System Environment/Base
- Summary: Red Hat Enterprise Linux release notes files
- Description: Red Hat Enterprise Linux release notes files.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhn-client-tools-0.4.20-86.el5 - rhn-client-tools-0.4.20.1-6.el5

- Group: System Environment/Base
- Summary: Support programs and libraries for Red Hat Network
- Description: Red Hat Network Client Tools provides programs and libraries to allow your system to receive software updates from Red Hat Network.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rhnlib-2.5.22-7.el5 - rhnlib-2.5.22.1-6.el5

- Group: Development/Libraries
- Summary: Python libraries for the RHN project
- Description: rhnlib is a collection of python modules used by the Red Hat Network (http://rhn.redhat.com) software.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rpm-4.4.2.3-31.el5 - rpm-4.4.2.3-34.el5

- Group: System Environment/Base
- Summary: The RPM package management system
- Description: The RPM Package Manager (RPM) is a powerful command line driven package management system capable of installing, uninstalling, verifying, querying, and updating software packages. Each software package consists of an archive of files along with information about the package like its version, a description, etc.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

ruby-1.8.5-27.el5 - ruby-1.8.5-31.el5_9

- Group: Development/Languages
- Summary: An interpreter of object-oriented scripting language
- Description: Ruby is the interpreted scripting language for quick and easy object-oriented programming. It has many features to process text files and to do system management tasks (as in Perl). It is simple, straight-forward, and extensible.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

samba3x-3.6.6-0.129.el5 - samba3x-3.6.6-0.136.el5

- Group: System Environment/Daemons
- Summary: Server and Client software to interoperate with Windows machines
- Description: Samba is the suite of programs by which a lot of PC-related machines share files, printers, and other information (such as lists of available files and printers). The Windows NT, OS/2, and Linux operating systems support this natively, and add-on packages can enable the same thing for DOS, Windows, VMS, UNIX of all kinds, MVS, and more. This package provides an SMB/CIFS server that can be used to provide network services to SMB/CIFS clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.
- Added Dependencies:
  - libtevent-devel >= 0.9.18
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

scl-utils-20120927-2.el5 - scl-utils-20120927-8.el5

- Group: Applications/File
- Summary: Utilities for alternative packaging
- Description: Run-time utility for alternative packaging.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

selinux-policy-2.4.6-338.el5 - selinux-policy-2.4.6-346.el5

- Group: System Environment/Base
- Summary: SELinux policy configuration
- Description: SELinux Reference Policy - modular.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sos-1.7-9.62.el5 - sos-1.7-9.66.el5

- Group: Development/Libraries
- Summary: A set of tools to gather troubleshooting information from a system
- Description: Sos is a set of tools that gathers information about system hardware and configuration. The information can then be used for diagnostic purposes and debugging. Sos is commonly used to help support technicians and developers.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

spamassassin-3.3.1-2.el5 - spamassassin-3.3.1-4.el5

- Group: Applications/Internet
- Summary: Spam filter for email which can be invoked from mail delivery agents.
- Description: SpamAssassin provides you with a way to reduce if not completely eliminate Unsolicited Commercial Email (SPAM) from your incoming email. It can be invoked by a MDA such as sendmail or postfix, or can be called from a procmail script, .forward file, etc. It uses a genetic-algorithm evolved scoring system to identify messages which look spammy, then adds headers to the message so they can be filtered by the user's mail reading software. This distribution includes the spamd/spamc components which create a server that considerably speeds processing of mail. To enable spamassassin, if you are receiving mail locally, simply add this line to your ~/.procmailrc: INCLUDERC=/etc/mail/spamassassin/spamassassin-default.rc To filter spam for all users, add that line to /etc/procmailrc (creating if necessary).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sqlite-3.3.6-6 - sqlite-3.3.6-7

- Group: Applications/Databases
- Summary: Library that implements an embeddable SQL database engine
- Description: SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete database is stored in a single disk file. The API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and flexibility of an SQL database without the administrative hassles of supporting a separate database server. Version 2 and version 3 binaries are named to permit each to be installed on a single host
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sssd-1.5.1-58.el5 - sssd-1.5.1-70.el5

- Group: Applications/System
- Summary: System Security Services Daemon
- Description: Provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides an NSS and PAM interface toward the system and a pluggable backend system to connect to multiple different account sources. It is also the basis to provide client auditing and policy services for projects like FreeIPA.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

subscription-manager-1.0.24-1.el5 - subscription-manager-1.8.22-1.el5

- Group: System Environment/Base
- Summary: Tools and libraries for subscription and repository management
- Description: The Subscription Manager package provides programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat entitlement platform.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

subscription-manager-migration-data-1.11.2.7-1.el5 - subscription-manager-migration-data-1.11.3.2-1.el5

- Group: System Environment/Base
- Summary: RHN Classic to RHSM migration data
- Description: This package provides certificates for migrating a system from RHN Classic to RHSM.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

subversion-1.6.11-10.el5_8 - subversion-1.6.11-11.el5_9

- Group: Development/Tools
- Summary: Modern Version Control System designed to replace CVS
- Description: Subversion is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes. Subversion only stores the differences between versions, instead of every complete file. Subversion is intended to be a compelling replacement for CVS.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sudo-1.7.2p1-22.el5 - sudo-1.7.2p1-28.el5

- Group: Applications/System
- Summary: Allows restricted root access for specified users.
- Description: Sudo (superuser do) allows a system administrator to give certain users (or groups of users) the ability to run some (or all) commands as root while logging all commands and arguments. Sudo operates on a per-command basis. It is not a replacement for the shell. Features include: the ability to restrict what commands a user may run on a per-host basis,

copious logging of each command (providing a clear audit trail of who did what), a configurable timeout of the sudo command, and the ability to use the same configuration file (sudoers) on many different machines.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-kdump-1.0.14-4.el5 - system-config-kdump-1.0.14-5.el5_9

- Group: System Environment/Base
- Summary: A graphical interface for configuring kernel crash dumping
- Description: system-config-kdump is a graphical tool for configuring kernel crash dumping via kdump and kexec.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

system-config-lvm-1.1.5-13.el5 - system-config-lvm-1.1.5-14.el5

- Group: Applications/System
- Summary: A utility for graphically configuring Logical Volumes
- Description: system-config-lvm is a utility for graphically configuring Logical Volumes
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

thunderbird-10.0.11-1.el5_8 - thunderbird-17.0.8-5.el5_9

- Group: Applications/Internet
- Summary: Mozilla Thunderbird mail/newsgroup client
- Description: Mozilla Thunderbird is a standalone mail and newsgroup client.
- Added Dependencies:
  - nspr-devel >= 4.9.2
  - python-devel
  - python-setuptools
  - sqlite-devel
- Removed Dependencies:
  - autoconf213
  - nspr-devel >= 4.8.9
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tomcat5-5.5.23-0jpp.37.el5 - tomcat5-5.5.23-0jpp.40.el5_9

- Group: Networking/Daemons
- Summary: Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API
- Description: Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Tomcat is developed in an open and participatory environment and released under the Apache Software License. Tomcat is intended to be a collaboration of the best-of-breed developers from around the world. We invite you to participate in this open development project. To learn more about getting involved, click here.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tzdata-2012i-2.el5 - tzdata-2013c-2.el5

- Group: System Environment/Base
- Summary: Timezone data
- Description: This package contains data files with rules for various time zones around the world.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

wpa_supplicant-0.5.10-9.el5 - wpa_supplicant-0.5.10-10.el5

- Group: System Environment/Base
- Summary: WPA/WPA2/IEEE 802.1X Supplicant
- Description: wpa_supplicant is a WPA Supplicant for Linux, BSD and Windows with support for WPA and WPA2 (IEEE 802.11i / RSN). Supplicant is the IEEE 802.1X/WPA component that is used in the client stations. It implements key negotiation with a WPA Authenticator and it controls the roaming and IEEE 802.11 authentication/association of the wlan driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xen-3.0.3-142.el5 - xen-3.0.3-142.el5_9.3

- Group: Development/Libraries
- Summary: Xen is a virtual machine monitor
- Description: This package contains the Xen tools and management daemons needed to run virtual machines on x86, x86_64, and ia64 systems. Information on how to use Xen can be found at the Xen project pages. The Xen system also requires the Xen hypervisor and domain-0 kernel, which can be found in the kernel-xen* package. Virtualization can be used to run multiple operating systems on one physical system, for purposes of hardware consolidation, hardware abstraction, or to test untrusted applications in a sandboxed environment.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xinetd-2.3.14-17.el5 - xinetd-2.3.14-19.el5

- Group: System Environment/Daemons
- Summary: A secure replacement for inetd.
- Description: Xinetd is a secure replacement for inetd, the Internet services daemon. Xinetd provides access control for all services based on the address of the remote host and/or on time of access and can prevent denial-of-access attacks. Xinetd provides extensive logging, has no limit on the number of server arguments, and lets you bind specific services to specific IP addresses on your host machine. Each service has its own specific configuration file for Xinetd; the files are located in the /etc/xinetd.d directory.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-drv-ati-6.6.3-3.33.el5 - xorg-x11-drv-ati-6.6.3-3.35.el5

- Group: User Interface/X Hardware Support
- Summary: Xorg X11 ati video driver

- Description: X.Org X11 ati video driver.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xorg-x11-server-1.1.1-48.100.el5 - xorg-x11-server-1.1.1-48.101.el5

- Group: User Interface/X
- Summary: X.Org X11 X server
- Description: X.Org X11 X server
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

xulrunner-10.0.11-1.el5_8 - xulrunner-17.0.8-3.el5_9

- Group: Applications/Internet
- Summary: XUL Runtime for Gecko Applications
- Description: XULRunner is a Mozilla runtime package that can be used to bootstrap XUL+XPCOM applications that are as rich as Firefox and Thunderbird. It provides mechanisms for installing, upgrading, and uninstalling these applications. XULRunner also provides libxul, a solution which allows the embedding of Mozilla technologies in other projects and products.
- Added Dependencies:
  - nspr-devel >= 4.9.2
  - nss-devel >= 3.13.6
  - python-devel
  - python-setuptools

    - sqlite-devel
  - Removed Dependencies:
    - nspr-devel >= 4.8.9
    - nss-devel >= 3.13.1
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

yelp-2.16.0-29.el5 - yelp-2.16.0-30.el5_9

  - Group: Applications/System
  - Summary: A system documentation reader from the Gnome project
  - Description: Yelp is the Gnome 2 help/documentation browser. It is designed to help you browse all the documentation on your system in one central tool.
  - Added Dependencies:
    - gecko-devel-unstable >= 17.0
  - Removed Dependencies:
    - gecko-devel-unstable >= 10.0
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

ypserv-2.19-9.el5_8.1 - ypserv-2.19-10.el5_9.1

  - Group: System Environment/Daemons
  - Summary: The NIS (Network Information Service) server.
  - Description: The Network Information Service (NIS) is a system that provides network information (login names, passwords, home directories, group information) to all of the machines on a network. NIS can allow users to log in on any machine on the network, as long as the machine has the NIS client programs running and the user's password is recorded in the

NIS passwd database. NIS was formerly known as Sun Yellow Pages (YP). This package provides the NIS server, which will need to be running on your network. NIS clients do not need to be running the server. Install ypserv if you need an NIS server for your network. You also need to install the yp-tools and ypbind packages on any NIS client machines.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yum-rhn-plugin-0.5.4-29.el5 - yum-rhn-plugin-0.5.4.1-7.el5

- Group: System Environment/Base
- Summary: RHN support for yum
- Description: This yum plugin provides support for yum to access a Red Hat Network server for software updates.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

zsh-4.2.6-8.el5 - zsh-4.2.6-9.el5

- Group: System Environment/Shells
- Summary: A powerful interactive shell
- Description: The zsh shell is a command interpreter usable as an interactive login shell and as a shell script command processor. Zsh resembles the ksh shell (the Korn shell), but includes many enhancements. Zsh supports command line editing, built-in spelling correction, programmable command completion, shell functions (with autoloading), a history mechanism, and more.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

Appendix B. Revision History

Revision 1-0.15	**Wed Mar 12 2014**	**Miroslav Svoboda**

Republished to include the latest kernel advisory, RHSA-2014:0285.

Revision 1-0.14	**Tue 21 Jan 2014**	**Eliška Slobodová**

Fixed a typo.

Revision 1-0.12	**Tue 01 Oct 2013**	**Eliška Slobodová**

Release of the Red Hat Enterprise Linux 5.10 Technical Notes.

Revision 1-0.1	**Tue Jul 16 2013**	**Eliška Slobodová**

Release of the Red Hat Enterprise Linux 5.10 Beta Technical Notes.