Red Hat Enterprise Linux 5
5.9 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 5.9
Edition 9

Red Hat Engineering Content Services

Red Hat Enterprise Linux 5 5.9 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 5.9
Edition 9

Red Hat Engineering Content Services

Legal Notice

Abstract

The Red Hat Enterprise Linux 5.9 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 5.8 and minor release Red Hat Enterprise Linux 5.9.

Table of Contents

Preface

The *Red Hat Enterprise Linux 5.9 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 5.9.

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

For every user, the *Red Hat Enterprise Linux 5.9 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-2.6.18-348*

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-2.6.18-348*

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

In 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 http://ecryptfs.sourceforge.net/README and http://ecryptfs.sourceforge.net/ecryptfs-faq.html 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.

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-2.6.18-348*

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-2.6.18-348*

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 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-2.6.18-348*

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*, other above-mentioned system-specific packages

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-2.0.115-109*

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-2.5-107*

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 to install the operating system software.

- 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/knowledge/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. 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)

2.6. 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)

2.7. 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
```

2.8. 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*

2.9. 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.

2.10. 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.

2.11. 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)

2.12. 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.

2.13. 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
```

2.14. 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*.

2.15. 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)

2.16. 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)

2.17. 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)
- iSCSI iface binding is not supported during install or boot. The initiator only supports the ability to log into target portals using the default behavior where the initiator uses the network routing table to decide which NIC to use.

  To work around this limitation, booting or installation can be done using the default behavior. After the iscs and iscsid services start, the iscsi service can log into the target using iSCSI iface binding. This however, will leave an extra session using the default behavior, and it has to be manually logged out using the following command:

  ```
  iscsiadm -m node -T target -p ip -I default -u
  ```

(BZ#500273)

2.18. 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.

2.19. kernel

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

- 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.

- 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. As a consequence, a kernel panic occurs when multiple tools use these files at the same time. To work around this problem, make sure only one such process is running at a given point of time.

- 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)
- Throughput across machines using IPv6 addresses and with bnx2x interfaces set up can be degraded.
- 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)

2.20. 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)

2.21. 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 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

2.22. less

The less utility is a text file browser that resembles more, but with more capabilities ("less is more"). The less utility allows users to move backwards in the file as well as forwards. Because less need not read the entire input file before it starts, less starts up more quickly than text editors (vi, for example).

- The "less" command has been updated. less no longer adds the "carriage return" character when wrapping long lines. Consequently, lines longer than the terminal width will be displayed incorrectly when browsing the file line per line. The command line option "--old-bot" forces less to behave as it did previously, with long text lines displayed correctly. (BZ#441691)

2.23. 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)

2.24. 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`**.

2.25. 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)

2.26. 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/knowledge/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)

2.27. 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).

2.28. 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 the "nfs/*" keys in the keytab file. Other keys are not supported.

2.29. 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)

2.30. 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)

2.31. 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 in Red Hat Enterprise Linux 5.9 does not support setting of the sha2_truncbug parameter in Red Hat Enterprise Linux 5.9, because the kernel does not support it.

2.32. 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)

2.33. 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.

2.34. 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
```

2.35. redhat-release-notes

The *redhat-release-notes* package contains the Release Notes for Red Hat Enterprise Linux 5.8.

- The Release Notes shipped in Red Hat Enterprise Linux 5.9 through the *redhat-release-notes* package contain an incorrect driver version number for the **qla2xxx** driver. In Red Hat Enterprise Linux 5.9, the **qla2xxx** driver for QLogic Fibre-Channel HBAs has been updated to version 8.03.07.15.05.09-k, not 8.04.00.05.05.09-k.

2.36. 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.

2.37. 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.

2.38. samba3x

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

- 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.

2.39. 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)

2.40. 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)

2.41. 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.

- 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.

2.42. 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)

2.43. 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)

2.44. 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.

- 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. 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)

2.48. 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)

2.49. 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)

2.50. 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.

2.51. 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)

Chapter 3. New Packages

3.1. RHEA-2013:0011 — new packages: php53-odbc64

New php53-odbc64 packages are now available for Red Hat Enterprise Linux 5.

The php53-odbc64 packages provide a module which can be used to access ODBC database interfaces from PHP 5.3 through the 64-bit API provided in the unixODBC64 package.

This enhancement update adds the php53-odbc64 package to Red Hat Enterprise Linux 5. (BZ#772293)

Users who are not encountering ODBC compatibility issues do not need to install these packages. Users who need to access ODBC database interfaces from PHP 5.3 through the 64-bit API provided in the unixODBC64 package are advised to install these new packages.

3.2. RHEA-2013:0035 — new packages: libitm

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

Libitm contains the GNU Transactional Memory Library, which provides transaction support for accesses to the memory of a process to enable synchronization of accesses to a shared memory by several threads.

This enhancement update adds the libitm packages to Red Hat Enterprise Linux 5. (BZ#813302)

All users who require libitm should install these new packages.

3.3. RHEA-2013:0049 — new packages: scl-utils

New scl-utils packages 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.

This enhancement update adds the scl-utils packages to Red Hat Enterprise Linux 5. (BZ#789469)

All users who require scl-utils should install these new packages.

3.4. RHEA-2013:0074 — new packages: ant17

New ant17 packages are now available for Red Hat Enterprise Linux 5.

The ant17 packages provide Ant version 1.7, a platform-independent build tool required for building with Java 7 OpenJDK7.

This enhancement update adds the ant17 packages to Red Hat Enterprise Linux 5. Note that the ant17 packages are released as an OpenJDK7 build requirement and are not compatible with ant 1.6. Therefore, no system or package should depend on ant17. (BZ#803797)

It is not recommended to install ant17 explicitly.

3.5. RHEA-2013:0084 — new packages: java-1.7.0-openjdk

New java-1.7.0-openjdk packages 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 so as to supply Java 7.

This enhancement update adds the java-1.7.0-openjdk packages to Red Hat Enterprise Linux 5. (BZ#803732)

Note: If creating packages dependent on Java 7, make sure your packaging system uses Java 7 packages as dependencies.

All users who require java-1.7.0-openjdk should install these new packages.

3.6. RHEA-2013:0088 — new packages: rsyslog5

New rsyslog5 packages are now available for Red Hat Enterprise Linux 5.

The rsyslog5 packages provide an enhanced, multi-threaded syslog daemon. It supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grain output format control.

The rsyslog5 package is a substitute of the existing rsyslog package which provides major version 3 of rsyslog in Red Hat Enterprise Linux 5. In order to install the rsyslog5 package, the rsyslog package must first be uninstalled.

This enhancement update adds the rsyslog5 packages to Red Hat Enterprise Linux 5. (BZ#820396)

For more information on changes included in major version 5 of rsyslog, refer to the Red Hat Enterprise Linux 5.9 Release Notes:

https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/5/html/5.9_Release_Notes/general_updates.html#rsyslog5

All users who require rsyslog5 should install these new packages.

3.7. RHEA-2013:0089 — new packages: java-1.7.0-ibm

New java-1.7.0-ibm packages are now available for Red Hat Enterprise Linux 5.

The java-1.7.0-ibm packages provide the IBM Java 7 Runtime Environment and the IBM Java 7 Software Development Kit.

This enhancement update adds the java-1.7.0-ibm packages to Red Hat Enterprise Linux 5. (BZ#841913)

All users who require java-1.7.0-ibm should install these new packages.

3.8. RHEA-2013:0090 — new packages: java-1.7.0-oracle

New java-1.7.0-oracle packages are now available for Red Hat Enterprise Linux 5.

Oracle Java SE version 7 includes the Oracle Java Runtime Environment and the Oracle Java Software Development Kit.

This update adds the java-1.7.0-oracle packages to Red Hat Enterprise Linux 5. (BZ#841910)

Note: Before applying this update, make sure that any previous Oracle Java packages have been removed.

All users who require java-1.7.0-oracle should install these new packages.

3.9. RHEA-2013:0111 — new packages: hypervkvpd

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

The hypervkvpd packages contain hypervkvpd, the guest 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.

This enhancement update adds the hypervkvpd packages to Red Hat Enterprise Linux 5. (BZ#849855)

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

Chapter 4. Package Updates

4.1. acroread

4.1.1. RHSA-2012:0469 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fix

CVE-2012-0774, CVE-2012-0775, CVE-2012-0777

This update fixes multiple security flaws in Adobe Reader. These flaws are detailed on the Adobe security page APSB12-08. 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 9.5.1, which is not vulnerable to these issues. All running instances of Adobe Reader must be restarted for the update to take effect.

4.2. aide

4.2.1. RHBA-2012:0499 — aide bug fix update

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

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

Bug Fix

BZ#811936

Previously, the aide utility incorrectly initialized the gcrypt library. This consequently prevented aide to initialize its database if the system was running in FIPS-compliant mode. The initialization routine has been corrected, and along with an extension to the libgcrypt's API introduced in the RHEA-2012:0484 advisory, aide now initializes its database as expected if run in a FIPS-compliant way.

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

4.2.2. RHBA-2012:1119 — aide bug fix update

Updated aide packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

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

Bug Fixes

BZ#547658

The help output of the aide executable did not mention the "-D" option which is a shortcut for "--config-check". The option could only be found on the aide(1) man page. With this update, the "-D" option is mentioned in both the help output and on the man page.

BZ#553137

Previously, the aide utility incorrectly initialized the gcrypt library. This consequently prevented aide to initialize its database if the system was running in FIPS-compliant mode. The initialization routine has been corrected, and along with an extension to the libgcrypt's API introduced in the RHEA-2012:0484 advisory, aide now initializes its database as expected if run in a FIPS-compliant way.

BZ#580253

The compare_dbline() function returned an "int" value, even though the function can operate with variables of size larger than "int" (for example, DB_SELINUX, DB_XATTRS or DB_WHIRPOOL). As a consequence, aide could produce incorrect results when checking a database for inconsistencies. The underlying source code has been modified so that the compare_dbline() function now returns an "unsigned long long" value, and aide correctly detects and reports database inconsistencies.

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

4.3. alsa-utils

4.3.1. RHBA-2013:0113 — alsa-utils bug fix update

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

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

Bug Fix

BZ#854012

Due to an incorrect configuration of the alsaloop utility from the alsa-utils package, high CPU usage occurred when using alsaloop. This also affected the alsa-delay script, which uses alsaloop for the configurable audio delay functionality. With this update, the alsaloop function has been reconfigured. As a result, the CPU usage is now optimized when alsaloop is used.

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

4.4. anaconda

4.4.1. RHBA-2013:0038 — anaconda bug fix and enhancement update

Updated *anaconda* packages that fix several bugs and two enhancements 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#750681

When a host name provided by the user could not be resolved during system installation, it was added to the **/etc/hosts** file as a localhost record (under 127.0.0.1). Thus when configuring the network, DNS resolution of the host name did not work properly. This update ensures that user-provided host names are no longer written to the **/etc/hosts** file and host name resolution now works as expected.

BZ#760496

During the installation process, Anaconda failed to read the Release Notes using the **getReleaseNotes()** function. Consequently, the **Release Notes** button showed a pop-up error “Release Notes are missing”. The **getReleaseNotes()** function has been fixed and now properly presents the Release Notes when the **Release Notes** button is pressed.

BZ#769287

The maximum size limit for all **ext** file systems was set to 8 TB. Consequently, Anaconda limited the maximum size artificially for the **ext3** and **ext4** file systems, even though these systems support sizes up to 16 TB. The size limits for **ext3** and **ext4** have been extended to 16 TB.

BZ#773573

Pressing the ESC key in certain Anaconda dialog boxes behaved the same way as if the **OK** button was hit. This has been fixed and pressing the ESC key now has the same effect as hitting the **Cancel** button.

BZ#784159

Previously, symbolic links in the **/dev/** directory, such as **/dev/fd/**, were not created during installation. Consequently, an attempt to use these links during the installation failed. The source code has been updated and symbolic links are now created correctly and can be used during installation.

BZ#788871

The **openibd** service was not enabled after installation when using *IP over InfiniBand* (IPoIB). Consequently, an InfiniBand device did not come up after installation. The underlying source code has been modified and the **openibd** service is now enabled when using **IPoIB** during installation.

BZ#797075

Previously, the **--label** option in the **part** section of a kickstart file was not honored. Consequently, partitions were not labeled in accordance with the kickstart option after system installation. The source code that handles partition label setting has been fixed, and partition labeling via a kickstart file works as expected.

BZ#812719

Kernel and **initrd** image sizes grew slightly in Red Hat Enterprise Linux 5.8. Consequently, the **diskboot.img** file did not have enough space to store all files and some of them were truncated or were not included in the image. The size of **diskboot.img** has been increased and all files fit as expected.

BZ#819721

Due to improper handling of invalid disks referenced in the kickstart file, Anaconda could crash with a traceback when attempting to execute the partitioning instructions. This bug has been fixed, Anaconda now checks for invalid BIOS disk references correctly and exits gracefully indicating that the referenced BIOS disk cannot be found.

BZ#841136

Newer versions of **nfs-utils** and **mount.nfs** are set to use the **TCP** protocol by default and Anaconda mounting code conflicted with this new default. Consequently, the *Network File System* (NFS) sources were not mountable and users were unable to install the system over this protocol. The Anaconda NFS mounting code has been updated to use **TCP** by default. As result, installations over NFS function as expected.

Enhancements

BZ#756213

This enhancement adds a class for *Global File System* (GFS) to the Anaconda code base. As a result, the lines with the “gfs” string in the **/etc/fstab** file are preserved on upgrade and using the **gfs** boot option enables a way to create new GFS partitions during installation. The lines with the unknown (unsupported) file system type are just commented out on upgrade instead of removed from the **/etc/fstab** file.

BZ#824880

This enhancement includes Microsoft *ParaVirtualized* (PV) drivers into the installation environment. Previously, running Red Hat Enterprise Linux as a guest on Microsoft provided only a sub-part user experience with need to download and install Microsoft tools and add the PV support. This update enables seamless installation of Red Hat Enterprise Linux as a guest on a **Hyper-V** server and Red Hat Enterprise Linux works out-of-the-box now.

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

4.5. aspell-en

4.5.1. RHEA-2012:0581 — aspell-en enhancement update

An updated aspell-en package that adds one enhancement is now available for Red Hat Enterprise Linux 5.

The aspell-en package provides the word list and dictionaries for the English language.

Enhancement

BZ#562286

Prior to this update, the default English dictionary contained profanity. With this update, the profanity is moved from the default dictionary to the "en-complete" dictionary. To run aspell with this dictionary, use the "-d" switch: "aspell -d en-complete".

All users of aspell-en are advised to upgrade to this updated package, which adds this enhancement.

4.6. autofs

4.6.1. RHBA-2012:0506 — autofs bug fix update

Updated autofs packages that fix one bug 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.

Bug Fix

BZ#810126

A function to check validity of a mount location was meant to check only for a small subset of map location errors. A recent improvement modification in error reporting inverted a logic test in this validating function. Consequently, the scope of the test was widened, which caused automount to report false positive failures. With this update, the faulty logic test has been corrected and false positive failures no longer occur.

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

4.6.2. RHSA-2013:0132 — Low: autofs security, bug fix, and enhancement update

An updated autofs package that fixes one security issue, several bugs, and adds one enhancement 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 for each vulnerability from the CVE link(s) associated with each description below.

The autofs utility controls the operation of the automount daemon. The automount daemon automatically mounts and unmounts file systems.

Security Fix

CVE-2012-2697

A bug fix included in RHBA-2012:0264 introduced a denial of service flaw in autofs. When using autofs with LDAP, a local user could use this flaw to crash autofs, preventing future mount requests from being processed until the autofs service was restarted. Note: This flaw did not impact existing mounts (except for preventing mount expiration).

Red Hat would like to thank Ray Rocker for reporting this issue.

Bug Fixes

BZ#585058

The autofs init script sometimes timed out waiting for the automount daemon to exit and returned a shutdown failure if the daemon failed to exit in time. To resolve this problem, the amount of time that the init script waits for the daemon has been increased to allow for cases where servers are slow to respond or there are many active mounts.

BZ#767428

Due to an omission when backporting a change, autofs attempted to download the entire LDAP map at startup. This mistake has now been corrected.

BZ#798448

A function to check the validity of a mount location was meant to check only for a small subset of map location errors. A recent modification in error reporting inverted a logic test in this validating

function. Consequently, the scope of the test was widened, which caused the automount daemon to report false positive failures. With this update, the faulty logic test has been corrected and false positive failures no longer occur.

BZ#847101

When there were many attempts to access invalid or non-existent keys, the automount daemon used excessive CPU resources. As a consequence, systems sometimes became unresponsive. The code has been improved so that automount checks for invalid keys earlier in the process which has eliminated a significant amount of the processing overhead.

BZ#859890

The auto.master(5) man page did not document the "-t, --timeout" option in the FORMAT options section. This update adds this information to the man page.

Enhancement

BZ#690404

Previously, it was not possible to configure separate timeout values for individual direct map entries in the autofs master map. This update adds this functionality.

All users of autofs are advised to upgrade to this updated package, which contains backported patches to correct these issues and add this enhancement.

4.7. bind

4.7.1. RHBA-2013:0136 — bind bug fix update

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

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.

Bug Fix

BZ#885731

Previously, the "named" name service daemon could terminate unexpectedly due to a race condition in the socket module. This race condition has been fixed and the "named" daemon no longer crashes.

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

4.7.2. RHSA-2012:0716 — Important: bind security update

Updated bind 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fixes

CVE-2012-1667

A flaw was found in the way BIND handled zero length resource data records. A malicious owner of a DNS domain could use this flaw to create specially-crafted DNS resource records that would cause a recursive resolver or secondary server to crash or, possibly, disclose portions of its memory.

CVE-2012-1033

A flaw was found in the way BIND handled the updating of cached name server (NS) resource records. A malicious owner of a DNS domain could use this flaw to keep the domain resolvable by the BIND server even after the delegation was removed from the parent DNS zone. With this update, BIND limits the time-to-live of the replacement record to that of the time-to-live of the record being replaced.

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

4.7.3. RHSA-2012:1123 — Important: bind security update

Updated bind 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(s) associated with each description below.

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

Security Fix

CVE-2012-3817

An uninitialized data structure use flaw was found in BIND when DNSSEC validation was enabled. A remote attacker able to send a large number of queries to a DNSSEC validating BIND resolver could use this flaw to cause it to exit unexpectedly with an assertion failure.

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

4.7.4. RHSA-2012:1267 — Important: bind security and bug fix update

Updated bind packages that fix one security issue and one bug are now available for Red Hat Enterprise Linux 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(s) associated with each description below.

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

Security Fix

CVE-2012-4244

A flaw was found in the way BIND handled resource records with a large RDATA value. A malicious owner of a DNS domain could use this flaw to create specially-crafted DNS resource records, that would cause a recursive resolver or secondary server to exit unexpectedly with an assertion failure.

Bug Fix

BZ#857056

The bind-chroot-admin script, executed when upgrading the bind-chroot package, failed to correctly update the permissions of the /var/named/chroot/etc/named.conf file. Depending on the permissions of the file, this could have prevented named from starting after installing package updates. With this update, bind-chroot-admin correctly updates the permissions and ownership of the file.

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

4.7.5. RHSA-2012:1363 — Important: bind security update

Updated bind 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(s) associated with each description below.

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

Security Fix

CVE-2012-5166

A flaw was found in the way BIND handled certain combinations of resource records. A remote attacker could use this flaw to cause a recursive resolver, or an authoritative server in certain configurations, to lockup.

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

4.8. bind97

4.8.1. RHBA-2012:1597 — bind97 bug fix update

Updated bind97 packages that fix a bug are now available for Red Hat Enterprise Linux 5.

The Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) protocols. It contains a DNS server (named), a resolver library with routines for applications to use when interfacing with DNS, and tools for verifying that the DNS server is operating correctly. These packages contain version 9.7 of the BIND suite.

Bug Fix

BZ#883402

When authoritative servers did not return a Start of Authority (SOA) record, the "named" daemon failed to cache and return answers. A patch has been provided to address this issue and "named" is now able to handle such under-performing servers correctly.

Users of bind97 are advised to upgrade to these updated packages, which fix this bug.

4.8.2. RHBA-2013:0043 — bind97 bug fix and enhancement update

Updated *bind97* packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

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

Bug Fixes

BZ#657260

Previously, the **DNS** server (**named**) init script killed all **named** processes when stopping the **named** daemon. This caused a problem for container-virtualized hosts, such as OpenVZ, because their **named** processes were killed by the init script. The init script has been fixed and now only kills the correct **named** processes.

BZ#703452

When the **/etc/resolv.conf** file contained the **search** keyword with no arguments, the **host/nslookup/dig** utility failed to parse it correctly. With this update, such lines are ignored.

BZ#719855

The **/etc/named.root.key** file was not listed in the **ROOTDIR_MOUNT** variable. Consequently, when using **bind97** with chroot, the **named.root.key** file was not mounted to the chroot environment. A patch has been applied and **/etc/named.root.key** is now mounted into chroot.

BZ#758057

A non-writable working directory is a long time feature on all Red Hat systems. Previously, **named** wrote **the working directory is not writable** as an error to the system log. This update changes the code so that **named** now writes this information only into the debug log.

BZ#803369

During a **DNS** zone transfer, **named** sometimes terminated unexpectedly with an assertion failure. A patch has been applied to make the code more robust, and **named** no longer crashes in the scenario described.

BZ#829823

Due to an error in the *bind* spec file, the *bind-chroot* subpackage did not create a **/dev/null** device. In addition, some empty directories were left behind after uninstalling bind. With this update, the *bind-chroot* packaging errors have been fixed.

BZ#829829

Previously, the **nslookup** utility did not return a non-zero exit code when it failed to get an answer. Consequently, it was impossible to determine if an **nslookup** run was successful or not from the error code. The **nslookup** utility has been fixed and now it returns **1** as the exit code when it fails to get an answer.

BZ#829831

The **named** daemon, configured as master server, sometimes failed to transfer an uncompressible zone. The following error message was logged:

```
transfer of './IN': sending zone data: ran out of space
```

The code which handles zone transfers has been fixed and this error no longer occurs in the scenario described.

Enhancements

BZ#693788

Previously, **bind97** did not contain the root zone **DNSKEY**. **DNSKEY** is now located in **/etc/named.root.key**.

BZ#703096

With this update, the size, MD5 checksum, and modification time of the **/etc/sysconfig/named** configuration file is no longer checked via the **rpm -V bind** command.

BZ#703397

The host utility now honors **debug**, **attempts**, and **timeout** options in the **/etc/resolv.conf** file.

BZ#703411

The **DISABLE_ZONE_CHECKING** option has been added to **/etc/sysconfig/named**. This option adds the possibility to bypass zone validation via the **named-checkzone** utility in the **/etc/init.d/named** init script and allows starting **named** with misconfigured zones.

BZ#749214

The return codes of the **dig** utility are now documented in the dig man page.

BZ#811566

The option to disable *Internationalized Domain Name* (IDN) support in the **dig** utility was incorrectly documented in the man page. The **dig** man page has been corrected to explain the use of the **libidn** environment option **CHARSET** for disabling IDN.

BZ#829827

Previously, the **rndc.key** file was generated during package installation by the **rndc-confgen -a** command, but this feature was removed in Red Hat Enterprise Linux 5.8 because users reported that installation of the *bind* package sometimes became unresponsive due to lack of entropy in **/dev/random**. The **named** init script now generates **rndc.key** during the service startup if it does not exist.

All users of *bind97* are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.8.3. RHSA-2012:0717 — Important: bind97 security update

Updated bind97 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fixes

CVE-2012-1667

A flaw was found in the way BIND handled zero length resource data records. A malicious owner of a DNS domain could use this flaw to create specially-crafted DNS resource records that would cause a recursive resolver or secondary server to crash or, possibly, disclose portions of its memory.

CVE-2012-1033

A flaw was found in the way BIND handled the updating of cached name server (NS) resource records. A malicious owner of a DNS domain could use this flaw to keep the domain resolvable by the BIND server even after the delegation was removed from the parent DNS zone. With this update, BIND limits the time-to-live of the replacement record to that of the time-to-live of the record being replaced.

Users of bind97 are advised to upgrade to these updated packages, which correct these issues. After installing the update, the BIND daemon (named) will be restarted automatically.

4.8.4. RHSA-2012:1122 — 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(s) associated with each description below.

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

Security Fix

CVE-2012-3817

An uninitialized data structure use flaw was found in BIND when DNSSEC validation was enabled. A remote attacker able to send a large number of queries to a DNSSEC validating BIND resolver could use this flaw to cause it to exit unexpectedly with an assertion failure.

Users of bind97 are advised to upgrade to these updated packages, which correct this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

4.8.5. RHSA-2012:1266 — 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(s) associated with each description below.

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

Security Fix

CVE-2012-4244

A flaw was found in the way BIND handled resource records with a large RDATA value. A malicious owner of a DNS domain could use this flaw to create specially-crafted DNS resource records, that would cause a recursive resolver or secondary server to exit unexpectedly with an assertion failure.

Users of bind97 are advised to upgrade to these updated packages, which correct this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

4.8.6. RHSA-2012:1364 — 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(s) associated with each description below.

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

Security Fix

CVE-2012-5166

A flaw was found in the way BIND handled certain combinations of resource records. A remote attacker could use this flaw to cause a recursive resolver, or an authoritative server in certain configurations, to lockup.

Users of bind97 are advised to upgrade to these updated packages, which correct this issue. After installing the update, the BIND daemon (named) will be restarted automatically.

4.9. binutils

4.9.1. RHBA-2012:0672 — binutils bug fix update

Updated binutils packages that fix one bug 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 Fix

BZ#818708

Due to instability in calculating the program header size, the GNU linker could terminate unexpectedly with the "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.

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

4.10. busybox

4.10.1. RHBA-2013:0075 — busybox bug fix update

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

BusyBox is a binary that combines a large number of common system utilities into a single executable. BusyBox provides replacements for most GNU file utilities, shell utilities, and other command-line tools.

Bug Fix

BZ#834277

When attempting to mount an NFS file system, the mount command in the busybox package was using the UDP protocol by default while the standard mount utility uses the TCP protocol by default. Consequently, directories could not be mounted from the server. With this update, the mount command in busybox has been fixed to use TCP by default, thus preventing this bug.

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

4.11. cman

4.11.1. RHBA-2012:0395 — cman bug fix update

An updated cman package that fixes one bug is 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#765665

The fence_rhevm fencing agent uses the Red Hat Enterprise Virtualization API to check the power status ("on" or "off") of a virtual machine. In addition to the states of "up" and "down", the API includes other states like "unassigned", "powering_up", "paused", "migrating", "unknown", "not_responding", "wait_for_launch", "reboot_in_progress", "saving_state", "restoring_state", "suspended", "image_illegal", "image_locked" or "powering_down". Previously, only if the machine was in the "up" state, the "on" power status was returned. The "off" status was returned for all other states although the machine was actually running. This allowed for successful fencing even before the machine was really powered off. With this update, the fence_rhevm agent detects power status of a cluster node more conservatively, and the "off" status is returned only if the machine is really powered off, it means in the "off" state.

All users of cman are advised to upgrade to this updated package, which fixes this bug.

4.11.2. RHBA-2012:0505 — 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#811939

Previously, cman did not handle idle connection timeout correctly when fencing a cluster node. Consequently, a connection to a fence device timed out and fencing failed if the "delay" option was set to more than 5 seconds. With this update, the "delay" option is applied before the connection is opened and the fencing thus no longer fails in this scenario.

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

4.11.3. RHBA-2012:1348 — 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#861392

The speed of fencing is critical because otherwise, broken nodes have more time to corrupt data. Previously, the operation of the fence_vmware_soap fencing agent was slow when used on the VMWare vSphere platform with hundreds of virtual machines. This update fixes a problem with virtual machines that do not have a valid UUID, which can be created during failed P2V (Physical-to-Virtual) processes. Now, the fencing process is also much faster and it does not terminate if a virtual machines without an UUID is encountered.

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

4.11.4. RHBA-2013:0076 — cman bug fix and enhancement update

Updated *cman* packages that fix several bugs and add various enhancements 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#674497

With this update, several typographical errors in the **`fence/agents/scsi/fence_scsi.pl`** file have been fixed. As a result, the debug messages of this file are now typographically correct.

BZ#745985

Prior to this update, the VMware vSphere 5.0 SOAP API was not listed as a version supported by the **fence_vmware_soap** fence agent. Consequently, the fence agent did not function properly with virtual machines managed by VMware vSphere 5.0. With this update, VMware vSphere 5.0 has been added to the list of supported interfaces, and is fully compatible with **fence_vmware_soap**.

BZ#753839

Previously, the **fence_scsi** man page contained incorrect information about the limitations of the **fence_scsi** agent. The correct description of these limitations can be found in the in the Cluster Administration guide. With this update, the misleading section has been removed from the manual page in order to avoid the potential confusion.

BZ#782919

Prior to this update, when attempting to create registrations on a multipath device with the **fence_scsi_test -o** command, some registrations failed without signalization. Consequently, there was a need to verify that all registrations had been successfully created. With this update, a **--strict** option has been added into the fence_scsi_test program. This option forces the verification step to compare the number of paths to the number of times the registration key appears on the device. Without this option, the verification step only inspects the existence of a registration key on the device. Although it is usually safe to omit the **--strict** option, it is strongly recommended to use **--strict** on multipath devices.

BZ#786485

The **fence_rhevm** fencing agent uses the Red Hat Enterprise Virtualization API to check the power status ("on" or "off") of a virtual machine. In addition to the states of "up" and "down", the API includes other states like "unassigned", "paused", etc. (14 in sum). Previously, only when the machine was in the "up" state, the "on" power status was returned. The "off" status was returned for all other states even though the machine was actually running. This behavior allowed for successful fencing even before the machine was powered off. The bug has been fixed and the "off" status is now returned only in a case the machine is in the "off" state.

BZ#804170

Previously, the **cman** utility did not apply the **--delay** option correctly when fencing a cluster node. Consequently, a connection to a fence device timed out and fencing failed when **--delay** was set to more than 5 seconds. With this update, **--delay** is applied before the connection is opened and the fencing no longer fails in the described scenario.

BZ#809390

Prior to this update, when the **method name** setting was left empty in the **/etc/cluster/cluster.conf** configuration file, an unintended core file was created. Consequently, a fenced cloud terminated with a segmentation fault. This bug has been fixed, and the termination no longer occurs in the aforementioned scenario.

BZ#809481

Due to a bug in the **fence_scsi_test** function, failing to create a reservation led to an incorrect reset of the error count to zero. The bug has been fixed, and the error count is now incremented properly when the error occurs.

BZ#836654

Previously, the **fence_vmware_soap** fencing agent operated slowly on the **VMware vSphere** platform with hundreds of virtual machines (VM). This behavior was caused by requesting for needless attributes. With this update, the unnecessary requests have been removed. This update also handles the VMs with invalid UUIDs, which can occur as a result of the failed P2V (physical to virtual machine) process. As a result, **fence_vmware_soap** performs fencing with increased speed and the process is no longer terminated when a VM without an UUID is encountered.

BZ#843083

In certain cases, the **fence_xvm** fencing agent incorrectly reported successful fencing, and ignored a communication issue between the agent and the **fence_xvmd** fencing host. This bug has been fixed and the communication errors are now reported correctly.

BZ#863567

The new href attribute on the /vms/vm element in the Red Hat Enterprise Virtualization Manager 3.1 API caused the get_id regular expression of the **fence_rhevm** fencing agent to fail. Consequently, the plug status was not available. With this update, get_id has been modified to allow arbitrary attributes to be added to the element. As a result, the plug status is now correctly shown.

Enhancements

BZ#738705

RHEL5 Cluster Suite now supports using RHEV shared storage disks as the shared storage between cluster nodes. Highly Available Logical Volume Manager (HA-LVM), Clustered Logical Volume Manager (CLVM), and the qDisk daemon are all supported on this storage. Fencing via **`fence_scsi`** will not work as shared disks are only exposed as VirtIO or IDE devices.

BZ#741985

A new fence agent, **fence_ipdu**, that handles the **IBM iPDU** fence device over the Simple Network Management Protocol (SNMP) has been added. As a result, the cman package now provides compatibility with **IBM iPDU**.

BZ#782900

Previously, using the **qdiskd** daemon for multipath devices required tuning with the **device-mapper-multipath** tool, which was a complex and error-prone process. With this update, the **qdiskd** input and output operations have been improved to automatically detect the multipath-related timeouts without requiring a manual configuration. As a result, **qdiskd** can now be easily deployed with **device-mapper-multipath**.

BZ#810949

Various **cman** fence agents differ in handling of the end-of-line (EOL) markers. Previously, changing the universal **`\r\n`** EOL could make the login process impossible for the fence agent. With this update, an automatic detection of EOL has been added to a fencing library and the described error no longer occurs.

BZ#821857

Prior to this update, it was not possible to specify more than four fencing devices per method with the **cman** utility. With this update, the maximum number of devices per method has increased to eight.

BZ#836963

The Distributed Lock Manager (DLM) now allows tuning of DLM hash table sizes from the **`/etc/sysconfig/cman`** file. The following parameters can be set in the **`/etc/sysconfig/cman`** file:

```
DLM_LKBTBL_SIZE=<size_of_table>
DLM_RSBTBL_SIZE=<size_of_table>
DLM_DIRTBL_SIZE=<size_of_table>
```

which, in turn, modifies the values in the following files respectively:

```
/sys/kernel/config/dlm/cluster/lkbtbl_size
/sys/kernel/config/dlm/cluster/rsbtbl_size
/sys/kernel/config/dlm/cluster/dirtbl_size
```

BZ#856954

Previously, it was not possible to modify the default TCP port (21064) of the Distributed Lock Manager (DLM). With this update, the ***DLM_TCP_PORT*** configuration parameter has been added into the **/etc/sysconfig/cman** file. As a result, the DLM TCP port can be manually configured.

BZ#878998

Support for clusters utilizing VMware's VMDK disk image technology with the **multi-writer** option is now provided. It is now possible to deploy Global File System 2 (GFS2) on top of VMDK.

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

4.12. cmirror

4.12.1. RHBA-2012:0524 — cmirror bug fix update

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

The cmirror package provides user-level tools for managing cluster mirroring. Cmirror is needed for LVM-based mirroring (RAID1) in a cluster environment.

Bug Fix

BZ#809642

Previously, when successively activating and deactivating cluster mirrors, cmirror could fail to initialize the mirrors properly. Consequently, any I/O operations to the device and further LVM commands became unresponsive. With this update, cmirror has been modified to fix this bug; however, the problem can still occur after a large number of iterations.

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

4.12.2. RHBA-2012:0554 — cmirror bug fix update

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

The cmirror packages provide user-level tools for managing cluster mirroring. Cmirror is needed for LVM-based mirroring (RAID1) in a cluster environment.

Bug Fix

BZ#816973

The cluster mirror daemon sends information between cluster nodes to keep the mirror log state consistent. Information about the state and health of the mirror and its devices is gathered as needed from the daemon. Some of the information does not change after the device has reached a certain state, for example when the mirror becomes "in-sync", while other information can change,

for example the health of the log device in response to a failure. To limit the amount of such requests and reduce the load on the network, processing of information which cannot change is done locally. Previously, also requests for information regarding the health of the log device - which ultimately controls the fault handling behavior of the mirror - were processed locally, which caused the daemon to miss the failure of the log device on a remote machine. With this update, the information is requested from the cluster so that log device failures are detected and processed as expected.

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

4.12.3. RHBA-2013:0017 — cmirror bug fix update

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

The cmirror packages provide a user-level utility for managing cluster mirroring. Cmirror is needed for LVM (Logical Volume Manger) based mirroring (RAID1) in a cluster environment.

Bug Fixes

BZ#711594

Prior to this update, requests for information about the health of the log device were processed locally. As a consequence, the cluster mirror daemon could not detect log device failures on remote machines. With this update, the information is requested from the cluster so that log device failures are detected and processed as expected.

BZ#806919

Prior to this update, the cmirror utility could fail to initialize the mirrors correctly when successively activating and deactivating cluster mirrors. As a consequence, any I/O operation to the device and further LVM commands became unresponsive.This update modifies the underlying code so that the problem only occurs after a large number of iterations.

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

4.13. conga

4.13.1. RHSA-2013:0128 — Low: conga security, bug fix, and enhancement update

Updated conga packages that fix one security issue, multiple bugs, and add two enhancements 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 for each vulnerability from the CVE link(s) associated with each description below.

The Conga project is a management system for remote workstations. It consists of luci, which is a secure web-based front end, and ricci, which is a secure daemon that dispatches incoming messages to underlying management modules.

Security Fix

CVE-2012-3359

It was discovered that luci stored usernames and passwords in session cookies. This issue prevented the session inactivity timeout feature from working correctly, and allowed attackers able to get access to a session cookie to obtain the victim's authentication credentials.

Red Hat would like to thank George Hedfors of Cybercom Sweden East AB for reporting this issue.

Bug Fixes

BZ#832181

Prior to this update, luci did not allow the fence_apc_snmp agent to be configured. As a consequence, users could not configure or view an existing configuration for fence_apc_snmp. This update adds a new screen that allows fence_apc_snmp to be configured.

BZ#832183

Prior to this update, luci did not allow the SSL operation of the fence_ilo fence agent to be enabled or disabled. As a consequence, users could not configure or view an existing configuration for the 'ssl' attribute for fence_ilo. This update adds a checkbox to show whether the SSL operation is enabled and allows users to edit that attribute.

BZ#832185

Prior to this update, luci did not allow the "identity_file" attribute of the fence_ilo_mp fence agent to be viewed or edited. As a consequence, users could not configure or view an existing configuration for the "identity_file" attribute of the fence_ilo_mp fence agent. This update adds a text input box to show the current state of the "identity_file" attribute of fence_ilo_mp and allows users to edit that attribute.

BZ#835649

Prior to this update, redundant files and directories remained on the file system at /var/lib/luci/var/pts and /usr/lib{,64}/luci/zope/var/pts when the luci package was uninstalled. This update removes these files and directories when the luci package is uninstalled.

BZ#839732

Prior to this update, the "restart-disable" recovery policy was not displayed in the recovery policy list from which users could select when they configure a recovery policy for a failover domain. As a consequence, the "restart-disable" recovery policy could not be set with the luci GUI. This update adds the "restart-disable" recovery option to the recovery policy pulldown list.

BZ#842865

Prior to this update, line breaks that were not anticipated in the "yum list" output could cause package upgrade and/or installation to fail when creating clusters or adding nodes to existing clusters. As a consequence, creating clusters and adding cluster nodes to existing clusters could fail. This update modifies the ricci daemon to be able to correctly handle line breaks in the "yum list" output.

Enhancements

BZ#741986

This update adds support for configuring the Intel iPDU fence agent to the luci package.

BZ#822633

This update adds support for viewing and changing the state of the new 'nfsrestart' attribute to the FS and Cluster FS resource agent configuration screens.

All users of conga are advised to upgrade to these updated packages, which resolve these issues and add these enhancements. After installing this update, the luci and ricci services will be restarted automatically.

4.14. coreutils

4.14.1. RHBA-2012:0408 — coreutils bug fix update

An updated coreutils package that fixes one bug is now available for Red Hat Enterprise Linux 5.

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

Bug Fix

BZ#803356

An incomplete fix for behavior of the "mv --backup" command, that was released with the RHBA-2011:1074 errata advisory, caused the "cp --backup" command to work incorrectly. When used with a directory as a source argument, the "cp --backup" command did not backup individual files within the directory but whole directory. This update corrects the problem and the "--backup" feature of the "cp" utility now works as intended again.

All users of coreutils are advised to upgrade to this updated package, which fixes this bug.

4.15. cpio

4.15.1. RHBA-2012:1055 — 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 file archiver utility. GNU cpio can be used to copy and extract files into or from cpio and Tar archives. This update is related to the following bug:

BZ#573943

Prior to this update, the cpio man page did not document how to use tape devices that do not use the default block size of 512 bytes for I/O operations. As a result, the cpio utility could fail with the error message "cpio: read error: Cannot allocate memory" if another block size was used. With this update, the man page states that setting the block size with the "--block-size" long option avoids this problem.

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

4.16. crash

4.16.1. RHBA-2013:0140 — crash bug fix update

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

The crash packages contain a self-contained utility that can be used to investigate live systems and kernel core dumps created by the netdump, diskdump, and kdump utilities.

Bug Fix

BZ#883727

The Xen dom0 dump files created with the "makedumpfile -d1" command on very large systems could create an ELF vmcore that the crash utility incorrectly determined to be an old-style netdump vmcore. Consequently, the crash session failed during initialization with the error message "crash: cannot read xen kdump p2m mfn page". With this update, the code has been fixed and the crash utility now properly starts in the described scenario.

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

4.17. crontabs

4.17.1. RHEA-2013:0031 — crontabs enhancement update

An updated crontabs package that adds one enhancement is now available for Red Hat Enterprise Linux 5.

The crontabs package contains root crontab files and directories. Crontab files are used to schedule jobs to be executed by the cron daemon, such as cronie. Crontabs handles a basic system function so it should be installed on your system.

Enhancement

BZ#532157

The cron daemon had no mechanism to manage cron job rescheduling in a shared environment selectively. Therefore, when a large number of hosts attempted to execute their jobs at the same time, a network or server running the jobs could become overloaded. This update modifies the run-parts script to provide cron job randomization. When cron job randomization is enabled and configured, and a cron job fails to be executed at the scheduled time, cron retries to execute jobs after a random interval. The network and server overloading due to too many simultaneous cron jobs can no longer occur.

All users of crontabs are advised to upgrade to this updated package, which adds this enhancement.

4.18. cscope

4.18.1. RHBA-2012:1137 — cscope bug fix update

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

The cscope packages contain ncurses-based C source code tree browsing tool which allows users to search large source code bases for variables, functions, macros, as well as perform general regex and plain text searches. Results are returned in lists, from which the user can select individual matches for use in file editing.

Bug Fix

BZ#440628

Previously, the spec file contained the %{dist} tag on the "Release" line. To comply with the packaging and naming guidelines, the tag has been changed to %{?dist} with this update.

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

4.19. ctdb

4.19.1. RHBA-2013:0059 — ctdb bug fix update

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

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.

Bug Fix

BZ#739502

Due to a name conflict of tools provided by the samba and tdb-tools packages, some binaries from the tdb-tools have to be renamed upon installation. The ctdb init script did not contain the updated names for the tdb-tools utilities. Consequently, the ctdb service could not be started via the init script. This update corrects the ctdb init script to search for tdb-tools utilities under their new name.

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

4.20. cyrus-sasl

4.20.1. RHBA-2012:1224 — cyrus-sasl bug fix update

Updated cyrus-sasl packages that resolve memory leaks are now available.

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

Bug Fix

BZ#849581

A memory leak in the digest-md5 plugin was discovered. Specifically, make_client_request was called twice without being freed. Consequently, applications that used DIGEST-MD5 with very large datasets could (and did) crash. This update frees make_client_request correctly and closes the memory leak. Applications using DIGEST-MD5 as part of authentication with large datasets now work as expected.

Note: this update also incorporates two upstream memory leak fixes reported during customer testing.

All cyrus-sasl users should upgrade to these updated packages, which fix these leaks.

4.21. device-mapper-multipath

4.21.1. RHBA-2012:0437 — 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#806204

The multipathd daemon creates its private namespace which is supposed to keep only the file systems that are necessary for multipathd to run. However, multipathd did not check every file system in the namespace, and the namespace thus could contain also non-essential file systems. As a consequence, devices containing such file systems could not be removed from the system. With this update, multipathd verifies all file systems in its private namespace and removes every non-essential file system found. The devices containing the non-essential file systems can now be removed as expected when the file systems are unmounted.

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

4.21.2. RHBA-2012:1599 — 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#858010

If the initrd RAM disk was not rebuilt when a new storage device was added to the system, the new device could be assigned a user_friendly_names value that collided with a value already assigned to another device. Consequently, the original device then stopped working correctly. Now, the multipathd daemon accepts the "-B" option, which makes the user_friendly_names bindings file read-only. When initrd calls multipath with the "-B" option, devices without a binding to a user_friendly_names use their World Wide Identifier (WWID) instead, thus fixing this bug.

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

4.21.3. RHBA-2013:0080 — device-mapper-multipath bug fix and enhancement update

Updated device-mapper-multipath packages that fix numerous bugs and add several enhancements are now available for Red Hat Enterprise Linux 5.

The device-mapper-multipath packages provide the tools for managing multipath devices.

Bug Fix

BZ#833193

The multipathd daemon ignored all subdirectories in /var/lib/ when deciding which file systems to unmount. Now, the only subdirectory of /var/lib/ that multipathd does not unmount is /var/lib/multipath/. Also, multipathd now unmounts all unnecessary file systems before mounting the ramfs on the /tmp/, /bin/, and /sbin/ directories.

BZ#769990

If initrd was not rebuilt when a new storage device was added to the system, the new device could have been assigned a user_friendly_names value already assigned to another device, and the device stopped working correctly. multipathd now accepts the -B option, which makes the user_friendly_names bindings file read-only. When started with the -B option, multipath devices

without a binding to a user_friendly_names use their World Wide Identifier (WWID).

BZ#803849

The multipathd daemon failed to unmount some file systems because the daemon was deleting unnecessary file systems while reading through the list of mounted file systems. Consequently, Multipath could have missed the deleted file systems. The multipathd daemon now reads through all file systems first and creates a list of the file systems to unmount, which are then unmounted based on this list.

BZ#771571

The multipathd daemon incorrectly returned exit code 1 when called with the -h option. The deamon now returns exit code 0 when called with the -h option.

BZ#783522

The multipathd daemon did not always flush the log buffer if it failed during start-up and error messages logged during start-up could be lost. multipathd now always flushes the log buffer on failures and error messages are logged correctly if multipathd terminates unexpectedly during start-up.

BZ#781480

The multipath priority callout programs did not work correctly with CCISS (Compaq Command Interface for SCSI-3 Support) devices because multipath could not convert the ! character in a CCISS sysfs name to the / character in the CCISS device name. Consequently, callout programs failed to set path priorities for these devices. The code has been modified and Multipath now supports the "%c" wildcard for callout functions and the CCISS names are converted correctly.

Enhancements

BZ#742906

This update adds the default configuration for HP P2000 G3 MSA Smart Array Systems.

BZ#744231

Multiple default settings and parameters have been enhanced: - The multipathd daemon did not set the max_fds option and the user had to manually set the max_fds option in multipath.conf. - Multipath did not disable queuing when it stopped: when multipathd stopped on node shutdown, if a multipath device had no working paths and was set to queue_if_no_path, the device queued outstanding IO forever, rendering the machine unresponsive. - The user_friendly_names option was only configurable in the defaults section and users could not override its value in their device-specific configurations. - A path group with many secondary paths could be used instead of the path group with the primary path by default. This happened because Multipath set the priority of path groups to the sum of their path priorities and used the path group with the primary path instead of using a path group with many secondary paths.

Device Mapper Multipath now sets max_fds to the system maximum, queue_if_no_daemon to the "no", and pg_prio_calc to "average" by default. The user_friendly_names property can be configured in the devices section of multipath.conf.

BZ#788965

Configuration for Fujitsu ETERNUS storage systems has been added.

BZ#799847

The built-in configuration for NetApp LUNs has been updated to use the tur path checker by

default and multiple hardware table parameters have been updated.

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. RHSA-2012:1140 — Moderate: dhcp security update

Updated dhcp 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 for each vulnerability from the CVE link(s) associated with each description below.

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.

CVE-2012-3571

A denial of service flaw was found in the way the dhcpd daemon handled zero-length client identifiers. A remote attacker could use this flaw to send a specially-crafted request to dhcpd, possibly causing it to enter an infinite loop and consume an excessive amount of CPU time.

Upstream acknowledges Markus Hietava of the Codenomicon CROSS project as the original reporter of this issue.

Users of DHCP should upgrade to these updated packages, which contain a backported patch to correct this issue. After installing this update, all DHCP servers will be restarted automatically.

4.23. diffutils

4.23.1. RHBA-2013:0036 — diffutils bug fix update

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

The diffutils package contains utilities for comparing text files. These utilities include diff, cmp, diff3, and sdiff.

Bug Fixes

BZ#484892

Prior to this update, the "-E" option of the sdiff command was not accepted and returned the following error message:

sdiff: invalid option -- E sdiff: Try `sdiff --help' for more information.

This was because the "-E" option was accidentally omitted from the list of accepted options. This update fixes this bug, and the "-E" option works as expected.

BZ#563618

When using the cmp command's "-s" option to compare files, incorrect results were returned for special files whose metadata is not accurate, for example files in the proc file system. This update fixes this bug by always reading the content of files whose length is reported as zero bytes.

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

4.24. doxygen

4.24.1. RHBA-2012:0718 — doxygen bug fix update

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

Doxygen can generate an online class browser in HTML and/or a reference manual in LaTeX from a set of documented source files. The documentation is extracted directly from the sources.

Bug Fix

BZ#448293

Prior to this update, the doxygen utility could create conflicts with multilib when doxygen added timestamps by creating doc files. This update modifies doxygen so that no more conflicts between multilib and doxygen occur.

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

4.25. e2fsprogs

4.25.1. RHBA-2012:1016 — e2fsprogs bug fix update

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

[Updated 13 August 2012] This advisory has been updated with the correct product name (that is, Red Hat Enterprise Linux 5) in the Details section. The package included in this revised update has not been changed in any way from the package included in the original advisory.

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

Bug Fix

BZ#824051

Previously, the status of the uuidd daemon was not correct when shown by the service tool, because the stored PID was not the PID of the running uuidd daemon. This was due to the incorrect PID that was written by the uuidd daemon upon startup. With this update, this bug has been fixed so that the returned status of the uuidd daemon is now correct.

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

4.25.2. RHBA-2013:0093 — e2fsprogs bug fix update

Updated e2fsprogs packages that fix two bugs 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 Fixes

BZ#701776

Due to a bug in the resize2fs program, the size of the ext3 file system created on a 16TB block device could not be modified. Consequently, the "device too big" error occurred. This bug has been fixed and file systems residing on 16T block devices can now be re-sized within the existing file system size limits.

BZ#707433

Previously, the uuidd daemon (uuidd) wrote an incorrect PID on startup to the /var/lib/libuuid/uuidd.pid file. Consequently, the service utility showed the incorrect status of uuidd because the stored PID was not the PID of the running uuidd process. This bug has been fixed and the returned status of uuidd is now correct in the described scenario.

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

4.26. e4fsprogs

4.26.1. RHBA-2013:0094 — e4fsprogs bug fix update

Updated e4fsprogs packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

Bug Fixes

BZ#707314

Due to a bug in the resize2fs program, the size of the ext4 file system created on a 16TB block device could not be modified. Consequently, the "device too big" error occurred. This bug has been fixed and file systems residing on 16TB block devices can now be re-sized within the existing file system size limits.

BZ#785200

Prior to this update, the mke4fs command created an ext2 file system by default. In order to create an ext4 file system, the "-t ext4" command-line option had to be inserted. This behavior has been changed, and mke4fs now creates an ext4 file system by default, without the need for extending the command.

Users of e4fsprogs package are advised to upgrade to these updated packages, which fix these bugs.

4.27. esc

4.27.1. RHBA-2012:0471 — esc bug fix update

Updated esc packages that fix two bugs 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 Fixes

BZ#807269

The ESC utility did not start when the latest 10 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.

BZ#807801

After removing and replacing an enrolled token, ESC could terminate unexpectedly followed by a traceback. A patch has been applied to address this issue and ESC now displays the enrolled smart card details as expected.

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

4.28. etherboot

4.28.1. RHBA-2013:0056 — etherboot bug fix update

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

The etherboot packages provide an open-source network bootloader. Etherboot replaces the proprietary Preboot eXecution Environment (PXE) ROMs. It also provides additional features, such as DNS, HTTP and iSCSI.

Bug Fix

BZ#714880

The etherboot-zroms-kvm package runs the update-alternatives utility during installation; however, the chkconfig package which provides the utility was previously not required by etherboot-zroms-kvm. As a consequence, the installation could fail with a "No such file or directory" error message. The chkconfig package has been added as a dependency to ensure successful installation of etherboot-zroms-kvm.

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

4.29. expat

4.29.1. RHSA-2012:0731 — Moderate: expat security update

Updated expat 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Expat is a C library written by James Clark for parsing XML documents.

Security Fixes

CVE-2012-0876

A denial of service flaw was found in the implementation of hash arrays in Expat. An attacker could use this flaw to make an application using Expat consume an excessive amount of CPU time by providing a specially-crafted XML file that triggers multiple hash function collisions. To mitigate this issue, randomization has been added to the hash function to reduce the chance of an attacker successfully causing intentional collisions.

CVE-2012-1148

A memory leak flaw was found in Expat. If an XML file processed by an application linked against Expat triggered a memory re-allocation failure, Expat failed to free the previously allocated memory. This could cause the application to exit unexpectedly or crash when all available memory is exhausted.

All Expat users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, applications using the Expat library must be restarted for the update to take effect.

4.30. file

4.30.1. RHBA-2012:1029 — file bug fix update

Updated file packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

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

Bug Fixes

BZ#758105

Prior to this update, the swap signature on the Itanium architecture was not stored in the same place as on other architectures. As a consequence, the file utility failed to detect the swap signature on Itanium. This update adds a new "magic" pattern to detect the swap signature on Itanium architecture.

BZ#789830

Prior to this update, the "magic" pattern to detect Infocom Game Data was too weak. As a consequence, Some files were wrongly identified as Infocom Game Data when they were actually in different format. This update modifies the Infocom Game Data "magic" pattern so only valid Infocom Game Data files are detected by this pattern.

BZ#758631

Prior to this update, the file utility did not contain a "magic" pattern to detect zip64 (zip 3.0) files. As a consequence, the file utility failed to detect archives in the zip64 format. This update adds a new "magic" pattern to detect the zip64 format.

BZ#758634

Prior to this update, the file utility did not contain a "magic" pattern to detect WebM video files. As a consequence, the file utility failed to detect WebM video files. This update adds a new "magic" pattern to detect the WebM files.

BZ#809801

Prior to this update, the file utility did not contain a "magic" pattern to detect LZMA archives. As a consequence, the file utility failed to detect archives in LZMA format were not detected. This update adds a new "magic" pattern to detect the LZMA files.

BZ#826899

Prior to this update, the "magic" pattern to detect Dell BIOS headers was outdated. As a consequence, the file utility failed to detect newer BIOS formats. This update modifies the ""magic"" pattern to detect also new formats of Dell BIOS correctly.

BZ#826901

Prior to this update, the file utility contained ""magic"" patterns that incorrectly detected files according to one byte only. As a consequence, Unicode text files that contained the particular byte in a particular position could be incorrectly recognized as DOS executable files. This update removes the problematic patterns. Patterns that match less than 16 bits are no longer accepted, and the utility no longer detects Unicode files as DOS executables.

All users of the file utility are advised to upgrade to these updated packages, which fix these bugs.

4.31. firefox

4.31.1. RHBA-2012:1429 — firefox bug fix update

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

The firefox packages provides an open source web browser, Mozilla Firefox.

Bug Fix

BZ#871568

The "out-of-process plug-ins" feature was previously disabled for wrapped plug-ins by default. This could cause Firefox to terminate unexpectedly when accessing a page that contained a flash object and the flash plug-in and the nswrapperplugin plug-in viewer were installed. To resolve this problem, the "out-of-process plug-ins" feature has been enabled for the wrapped plug-ins. Firefox no longer crashes in this scenario.

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

4.31.2. RHSA-2012:1210 — Critical: firefox security update

Updated firefox 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 critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Firefox is an open source web browser. XULRunner provides the XUL Runtime environment for Mozilla 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-2012-1970, CVE-2012-1972, CVE-2012-1973, CVE-2012-1974, CVE-2012-1975, CVE-2012-1976, CVE-2012-3956, CVE-2012-3957, CVE-2012-3958, CVE-2012-3959, CVE-2012-3960, CVE-2012-3961, CVE-2012-3962, CVE-2012-3963, CVE-2012-3964)

Security Fixes

CVE-2012-3969, CVE-2012-3970

A web page containing a malicious Scalable Vector Graphics (SVG) image file could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-3967, CVE-2012-3968

Two flaws were found in the way Firefox rendered certain images using WebGL. A web page containing malicious content could cause Firefox to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-3966

A flaw was found in the way Firefox decoded embedded bitmap images in Icon Format (ICO) files. A web page containing a malicious ICO file could cause Firefox to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Firefox. (CVE-2012-3966)

CVE-2012-3980

A flaw was found in the way the "eval" command was handled by the Firefox Web Console. Running "eval" in the Web Console while viewing a web page containing malicious content could possibly cause Firefox to execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-3972

An out-of-bounds memory read flaw was found in the way Firefox used the format-number feature of XSLT (Extensible Stylesheet Language Transformations). A web page containing malicious content could possibly cause an information leak, or cause Firefox to crash.

CVE-2012-3976

It was found that the SSL certificate information for a previously visited site could be displayed in the address bar while the main window displayed a new page. This could lead to phishing attacks as attackers could use this flaw to trick users into believing they are viewing a trusted site.

CVE-2012-3978

A flaw was found in the location object implementation in Firefox. Malicious content could use this flaw to possibly allow restricted content to be loaded.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 10.0.7 ESR.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Gary Kwong, Christian Holler, Jesse Ruderman, John Schoenick, Vladimir Vukicevic, Daniel Holbert, Abhishek Arya, Frédéric Hoguin, miaubiz, Arthur Gerkis, Nicolas Grégoire, Mark Poticha, moz_bug_r_a4, and Colby Russell as the original reporters of these issues.

All Firefox users should upgrade to these updated packages, which contain Firefox version 10.0.7 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.31.3. RHEA-2012:0327 — firefox enhancement update

Updated firefox packages that address security issues, fix bugs, add enhancements, and upgrade Firefox to version 10.0, are now available for Red Hat Enterprise Linux 5 and 6.

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

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 10.0.

The firefox packages have been upgraded from version 3.6.26 to version 10.0.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#789048, BZ#786872)

These updated firefox packages include numerous bug fixes and enhancements. Space precludes documenting these changes in this advisory. For details concerning these changes, refer to the Firefox release notes.

Bug Fix

BZ#794721, BZ#789051

Previously, with the xulrunner-5.0-2.el6 package installed, the yelp plug-in failed to start and returned the "Could not initialize gecko!" error message. Now, the updated yelp package has been provided and yelp works as expected in the described scenario.

Important: Firefox 10 is not completely backwards-compatible with all Mozilla add-ons and Firefox plug-ins that worked with Firefox 3.6. Firefox 10 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 10. After installing the update, Firefox must be restarted for the changes to take effect.

4.31.4. RHSA-2012:0387 — Critical: firefox security and bug fix update

Updated firefox packages that fix multiple security issues and three bugs 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Firefox is an open source web browser.

CVE-2012-0461, CVE-2012-0462, CVE-2012-0464

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-2012-0456, CVE-2012-0457

Two flaws were found in the way Firefox parsed certain Scalable Vector Graphics (SVG) image files. A web page containing a malicious SVG image file could cause an information leak, or cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0455

A flaw could allow a malicious site to bypass intended restrictions, possibly leading to a cross-site scripting (XSS) attack if a user were tricked into dropping a "javascript:" link onto a frame.

CVE-2012-0458

It was found that the home page could be set to a "javascript:" link. If a user were tricked into setting such a home page by dragging a link to the home button, it could cause Firefox to repeatedly crash, eventually leading to arbitrary code execution with the privileges of the user running Firefox.

CVE-2012-0459

A flaw was found in the way Firefox parsed certain web content containing "cssText". 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-2012-0460

It was found that by using the DOM fullscreen API, untrusted content could bypass the mozRequestFullscreen security protections. A web page containing malicious web content could exploit this API flaw to cause user interface spoofing.

CVE-2012-0451

A flaw was found in the way Firefox handled pages with multiple Content Security Policy (CSP) headers. This could lead to a cross-site scripting attack if used in conjunction with a website that has a header injection flaw.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 10.0.3 ESR.

Bug Fixes

BZ#729632

When using the Traditional Chinese locale (zh-TW), a segmentation fault sometimes occurred when closing Firefox.

BZ#784048

Inputting any text in the Web Console (Tools -> Web Developer -> Web Console) caused Firefox to crash.

BZ#799042

The java-1.6.0-ibm-plugin and java-1.6.0-sun-plugin packages require the "/usr/lib/mozilla/plugins/" directory on 32-bit systems, and the "/usr/lib64/mozilla/plugins/" directory on 64-bit systems. These directories are created by the xulrunner package; however, they were missing from the xulrunner package provided by the RHEA-2012:0327 update. Therefore, upgrading to RHEA-2012:0327 removed those directories, causing dependency errors when attempting to install the java-1.6.0-ibm-plugin or java-1.6.0-sun-plugin package. With this update, xulrunner once again creates the plugins directory. This issue did not affect users of Red Hat Enterprise Linux 6.

All Firefox users should upgrade to these updated packages, which contain Firefox version 10.0.3 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.31.5. RHSA-2012:0515 — Critical: firefox security update

Updated firefox 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 critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fixes

CVE-2011-3062

A flaw was found in Sanitiser for OpenType (OTS), used by Firefox to help prevent potential exploits in malformed OpenType fonts. A web page containing malicious content could cause Firefox to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0467, **CVE-2012-0468**, **CVE-2012-0469**

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-2012-0470

A web page containing a malicious Scalable Vector Graphics (SVG) image file could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0472

A flaw was found in the way Firefox used its embedded Cairo library to render certain fonts. A web page containing malicious content could cause Firefox to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0478

A flaw was found in the way Firefox rendered certain images using WebGL. A web page containing malicious content could cause Firefox to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-0471

A cross-site scripting (XSS) flaw was found in the way Firefox handled certain multibyte character sets. A web page containing malicious content could cause Firefox to run JavaScript code with the permissions of a different website.

CVE-2012-0473

A flaw was found in the way Firefox rendered certain graphics using WebGL. A web page containing malicious content could cause Firefox to crash.

CVE-2012-0474

A flaw in Firefox allowed the address bar to display a different website than the one the user was visiting. An attacker could use this flaw to conceal a malicious URL, possibly tricking a user into believing they are viewing a trusted site, or allowing scripts to be loaded from the attacker's site, possibly leading to cross-site scripting (XSS) attacks.

CVE-2012-0477

A flaw was found in the way Firefox decoded the ISO-2022-KR and ISO-2022-CN character sets. A web page containing malicious content could cause Firefox to run JavaScript code with the permissions of a different website.

CVE-2012-0479

A flaw was found in the way Firefox handled RSS and Atom feeds. Invalid RSS or Atom content loaded over HTTPS caused Firefox to display the address of said content in the location bar, but not the content in the main window. The previous content continued to be displayed. An attacker could use this flaw to perform phishing attacks, or trick users into thinking they are visiting the site reported by the location bar, when the page is actually content controlled by an attacker.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 10.0.4 ESR.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Mateusz Jurczyk of the Google Security Team as the original reporter of CVE-2011-3062; Aki Helin from OUSPG as the original reporter of CVE-2012-0469; Atte Kettunen from OUSPG as the original reporter of CVE-2012-0470; wushi of team509 via iDefense as the original reporter of CVE-2012-0472; Ms2ger as the original

reporter of CVE-2012-0478; Anne van Kesteren of Opera Software as the original reporter of CVE-2012-0471; Matias Juntunen as the original reporter of CVE-2012-0473; Jordi Chancel and Eddy Bordi, and Chris McGowen as the original reporters of CVE-2012-0474; Masato Kinugawa as the original reporter of CVE-2012-0477; and Jeroen van der Gun as the original reporter of CVE-2012-0479.

4.31.6. RHSA-2012:0710 — Critical: firefox security update

Updated firefox 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 critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fixes

CVE-2011-3101, CVE-2012-1937, CVE-2012-1938, CVE-2012-1939, CVE-2012-1940, CVE-2012-1941, CVE-2012-1946, CVE-2012-1947

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-2012-1944

Note: CVE-2011-3101 only affected users of certain NVIDIA display drivers with graphics cards that have hardware acceleration enabled.

It was found that the Content Security Policy (CSP) implementation in Firefox no longer blocked Firefox inline event handlers. A remote attacker could use this flaw to possibly bypass a web application's intended restrictions, if that application relied on CSP to protect against flaws such as cross-site scripting (XSS).

CVE-2012-1945

If a web server hosted HTML files that are stored on a Microsoft Windows share, or a Samba share, loading such files with Firefox could result in Windows shortcut files (.lnk) in the same share also being loaded. An attacker could use this flaw to view the contents of local files and directories on the victim's system. This issue also affected users opening HTML files from Microsoft Windows shares, or Samba shares, that are mounted on their systems.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 10.0.5 ESR.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Ken Russell of Google as the original reporter of CVE-2011-3101; Igor Bukanov, Olli Pettay, Boris Zbarsky, and Jesse Ruderman as the original reporters of CVE-2012-1937; Jesse Ruderman, Igor Bukanov, Bill McCloskey, Christian Holler, Andrew McCreight, and Brian Bondy as the original reporters of CVE-2012-1938; Christian Holler as the original reporter of CVE-2012-1939; security researcher Abhishek Arya of Google as the original reporter of CVE-2012-1940, CVE-2012-1941, and CVE-2012-1947; security researcher Arthur Gerkis as the original reporter of CVE-2012-1946; security researcher Adam Barth as the original reporter of CVE-2012-1944; and security researcher Paul Stone as the original reporter of CVE-2012-1945.

All Firefox users should upgrade to these updated packages, which contain Firefox version 10.0.5 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.31.7. RHSA-2012:1350 — Critical: firefox security and bug fix update

Updated firefox packages that fix several security issues and one bug 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) 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-2012-3982, CVE-2012-3988, CVE-2012-3990, CVE-2012-3995, CVE-2012-4179, CVE-2012-4180, CVE-2012-4181, CVE-2012-4182, CVE-2012-4183, CVE-2012-4185, CVE-2012-4186, CVE-2012-4187, CVE-2012-4188

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-2012-3986, CVE-2012-3991

Two flaws in Firefox could allow a malicious website to bypass intended restrictions, possibly leading to information disclosure, or Firefox executing arbitrary code. Note that the information disclosure issue could possibly be combined with other flaws to achieve arbitrary code execution.

CVE-2012-1956, CVE-2012-3992, CVE-2012-3994

Multiple flaws were found in the location object implementation in Firefox. Malicious content could be used to perform cross-site scripting attacks, script injection, or spoofing attacks.

CVE-2012-3993, CVE-2012-4184

Two flaws were found in the way Chrome Object Wrappers were implemented. Malicious content could be used to perform cross-site scripting attacks or cause Firefox to execute arbitrary code.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 10.0.8 ESR.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Christian Holler, Jesse Ruderman, Soroush Dalili, miaubiz, Abhishek Arya, Atte Kettunen, Johnny Stenback, Alice White, moz_bug_r_a4, and Mariusz Mlynski as the original reporters of these issues.

Bug Fix

BZ#809571, BZ#816234

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

If you experience this issue:

1) Start Firefox.

2) Type "about:config" (without quotes) into the URL bar and press the Enter key.

3) If prompted with "This might void your warranty!", click the "I'll be careful, I promise!" button.

4) Right-click in the Preference Name list. In the menu that opens, select New -> Boolean.

5) Type "storage.nfs_filesystem" (without quotes) for the preference name and then click the OK button.

6) Select "true" for the boolean value and then press the OK button.

All Firefox users should upgrade to these updated packages, which contain Firefox version 10.0.8 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.31.8. RHSA-2012:1407 — Critical: firefox security update

Updated firefox 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 critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fix

CVE-2012-4194, CVE-2012-4195, CVE-2012-4196

Multiple flaws were found in the location object implementation in Firefox. Malicious content could be used to perform cross-site scripting attacks, bypass the same-origin policy, or cause Firefox to execute arbitrary code.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 10.0.10 ESR.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Mariusz Mlynski, moz_bug_r_a4, and Antoine Delignat-Lavaud as the original reporters of these issues.

All Firefox users should upgrade to these updated packages, which contain Firefox version 10.0.10 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.31.9. RHSA-2012:1482 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) 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-2012-4214, CVE-2012-4215, CVE-2012-4216, CVE-2012-5829, CVE-2012-5830, CVE-2012-5833, CVE-2012-5835, CVE-2012-5839, CVE-2012-5840, CVE-2012-5842

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-2012-4202

A buffer overflow flaw was found in the way Firefox handled GIF (Graphics Interchange Format) images. A web page containing a malicious GIF image could cause Firefox to crash or, possibly, execute arbitrary code with the privileges of the user running Firefox.

CVE-2012-4210

A flaw was found in the way the Style Inspector tool in Firefox handled certain Cascading Style Sheets (CSS). Running the tool (Tools -> Web Developer -> Inspect) on malicious CSS could result in the execution of HTML and CSS content with chrome privileges.

CVE-2012-4207

A flaw was found in the way Firefox decoded the HZ-GB-2312 character encoding. A web page containing malicious content could cause Firefox to run JavaScript code with the permissions of a different website.

CVE-2012-4209

A flaw was found in the location object implementation in Firefox. Malicious content could possibly use this flaw to allow restricted content to be loaded by plug-ins.

CVE-2012-5841

A flaw was found in the way cross-origin wrappers were implemented. Malicious content could use this flaw to perform cross-site scripting attacks.

CVE-2012-4201

A flaw was found in the evalInSandbox implementation in Firefox. Malicious content could use this flaw to perform cross-site scripting attacks.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 10.0.11 ESR.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Abhishek Arya, miaubiz, Jesse Ruderman, Andrew McCreight, Bob Clary, Kyle Huey, Atte Kettunen, Mariusz Mlynski, Masato Kinugawa, Bobby Holley, and moz_bug_r_a4 as the original reporters of these issues.

All Firefox users should upgrade to these updated packages, which contain Firefox version 10.0.11 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.31.10. RHSA-2012:1088 — Critical: firefox security update

Updated firefox 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 critical security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fixes

CVE-2012-1948, **CVE-2012-1951**, **CVE-2012-1952**, **CVE-2012-1953**, **CVE-2012-1954**, **CVE-2012-1958**, **CVE-2012-1962**, **CVE-2012-1967**

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-2012-1959

A malicious web page could bypass same-compartment security wrappers (SCSW) and execute arbitrary code with chrome privileges.

CVE-2012-1966

A flaw in the context menu functionality in Firefox could allow a malicious website to bypass intended restrictions and allow a cross-site scripting attack.

CVE-2012-1950

A page different to that in the address bar could be displayed when dragging and dropping to the address bar, possibly making it easier for a malicious site or user to perform a phishing attack.

CVE-2012-1955

A flaw in the way Firefox called history.forward and history.back could allow an attacker to conceal a malicious URL, possibly tricking a user into believing they are viewing a trusted site.

CVE-2012-1957

A flaw in a parser utility class used by Firefox to parse feeds (such as RSS) could allow an attacker to execute arbitrary JavaScript with the privileges of the user running Firefox. This issue could have affected other browser components or add-ons that assume the class returns sanitized input.

CVE-2012-1961

A flaw in the way Firefox handled X-Frame-Options headers could allow a malicious website to perform a clickjacking attack.

CVE-2012-1963

A flaw in the way Content Security Policy (CSP) reports were generated by Firefox could allow a malicious web page to steal a victim's OAuth 2.0 access tokens and OpenID credentials.

CVE-2012-1964

A flaw in the way Firefox handled certificate warnings could allow a man-in-the-middle attacker to create a crafted warning, possibly tricking a user into accepting an arbitrary certificate as trusted.

CVE-2012-1965

A flaw in the way Firefox handled feed:javascript URLs could allow output filtering to be bypassed, possibly leading to a cross-site scripting attack.

Bug Fix

BZ#838879

The nss update RHBA-2012:0337 for Red Hat Enterprise Linux 5 and 6 introduced a mitigation for the CVE-2011-3389 flaw. For compatibility reasons, it remains disabled by default in the nss packages. This update makes Firefox enable the mitigation by default. It can be disabled by setting the NSS_SSL_CBC_RANDOM_IV environment variable to 0 before launching Firefox.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 10.0.6 ESR.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Benoit Jacob, Jesse Ruderman, Christian Holler, Bill McCloskey, Abhishek Arya, Arthur Gerkis, Bill Keese, moz_bug_r_a4, Bobby Holley, Code Audit Labs, Mariusz Mlynski, Mario Heiderich, Frédéric Buclin, Karthikeyan Bhargavan, Matt McCutchen, Mario Gomes, and Soroush Dalili as the original reporters of these issues.

All Firefox users should upgrade to these updated packages, which contain Firefox version 10.0.6 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

4.32. freeradius2

4.32.1. RHSA-2012:1327 — Moderate: freeradius2 security update

Updated freeradius2 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 for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fix

CVE-2012-3547

A buffer overflow flaw was discovered in the way radiusd handled the expiration date field in X.509 client certificates. A remote attacker could possibly use this flaw to crash radiusd if it were configured to use the certificate or TLS tunnelled authentication methods (such as EAP-TLS, EAP-TTLS, and PEAP).

Red Hat would like to thank Timo Warns of PRESENSE Technologies GmbH for reporting this issue.

Users of FreeRADIUS are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the update, radiusd will be restarted automatically.

4.32.2. RHSA-2013:0134 — Low: freeradius2 security and bug fix update

Updated freeradius2 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 low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

FreeRADIUS is an open-source Remote Authentication Dial-In User Service (RADIUS) server which allows RADIUS clients to perform authentication against the RADIUS server. The RADIUS server may optionally perform accounting of its operations using the RADIUS protocol.

Security Fix

CVE-2011-4966

It was found that the "unix" module ignored the password expiration setting in "/etc/shadow". If FreeRADIUS was configured to use this module for user authentication, this flaw could allow users with an expired password to successfully authenticate, even though their access should have been denied.

Bug Fixes

BZ#787111

After log rotation, the freeradius logrotate script failed to reload the radiusd daemon and log messages were lost. This update has added a command to the freeradius logrotate script to reload the radiusd daemon and the radiusd daemon re-initializes and reopens its log files after log rotation as expected.

BZ#846476

The radtest script with the "eap-md5" option failed because it passed the IP family argument when invoking the radeapclient utility and the radeapclient utility did not recognize the IP family. The radeapclient utility now recognizes the IP family argument and radtest now works with eap-md5 as expected.

BZ#846471

Previously, freeradius was compiled without the "--with-udpfromto" option. Consequently, with a multihomed server and explicitly specifying the IP address, freeradius sent the reply with the wrong IP source address. With this update, freeradius has been built with the "--with-udpfromto" configuration option and the RADIUS reply is always sourced from the IP address the request was sent to.

BZ#818885

Due to invalid syntax in the PostgreSQL admin schema file, the FreeRADIUS PostgreSQL tables failed to be created. With this update, the syntax has been adjusted and the tables are created as expected.

BZ#846475

FreeRADIUS has a thread pool that dynamically grows based on load. If multiple threads using the "rlm_perl()" function are spawned in quick succession, the FreeRADIUS server sometimes terminated unexpectedly with a segmentation fault due to parallel calls to the "rlm_perl_clone()" function. With this update, a mutex for the threads has been added and the problem no longer occurs.

BZ#781877

The man page for "rlm_dbm_parser" was incorrectly installed as "rlm_dbm_parse", omitting the trailing "r". The man page now correctly appears as rlm_dbm_parser.

All users of freeradius2 are advised to upgrade to these updated packages, which contain backported patches to correct these issues. They are also advised to check for RPM backup files ending in ".rpmnew" or ".rpmsave" under the /etc/raddb/ directory after the update because the FreeRADIUS server will attempt to load every file it finds in its configuration directory. The extra files will often cause the wrong configuration values to be applied resulting in either unpredictable behavior or the failure of the server to initialize and run.

4.33. freetype

4.33. freetype

4.33.1. RHSA-2012:0467 — Important: freetype security update

Updated freetype 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 important security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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 Fixes

CVE-2012-1134, CVE-2012-1136, CVE-2012-1142, CVE-2012-1144

Multiple flaws were found in the way FreeType handled TrueType Font (TTF), Glyph Bitmap Distribution Format (BDF), Windows .fnt and .fon, and PostScript Type 1 fonts. If a specially-crafted font file was loaded by an application linked against FreeType, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2012-1126, CVE-2012-1127, CVE-2012-1130, CVE-2012-1131, CVE-2012-1132, CVE-2012-1137, CVE-2012-1139, CVE-2012-1140, CVE-2012-1141, CVE-2012-1143

Multiple flaws were found in the way FreeType handled fonts in various formats. If a specially-crafted font file was loaded by an application linked against FreeType, it could cause the application to crash.

Red Hat would like to thank Mateusz Jurczyk of the Google Security Team for reporting these issues.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct these issues. The X server must be restarted (log out, then log back in) for this update to take effect.

4.34. ftp

4.34.1. RHEA-2013:0102 — ftp enhancement update

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

The ftp package provides the standard UNIX command line File Transfer Protocol (FTP) client. FTP is a widely used protocol for transferring files over the Internet, and for archiving files.

Enhancement

BZ#665240

Previously, the command line width in the ftp client was limited to 200 characters. With this update, the maximum possible length of the FTP command line is extended to 4296 characters.

All users of ftp are advised to upgrade to these updated packages, which add this enhancement.

4.35. gawk

4.35.1. RHBA-2012:0738 — gawk bug fix update

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

Problem Description: The gawk package contains the GNU version of awk, a text processing utility. Awk interprets a special-purpose programming language to do quick and easy text pattern matching and reformatting jobs.

Bug Fix

BZ#827372

Prior to this update, the "re_string_skip_chars" function incorrectly used the character count instead of the raw length to estimate the string length. As a consequence, text in multi-byte encoding that did not use the UTF-8 format failed to be processed correctly. This update modifies the underlying code so that the correct string length is used. multi-byte encoding is processed correctly.

All users of gawk requiring multi-byte encodings that do not use UTF-8 are advised to upgrade to these updated packages, which fix this bug.

4.36. gcc

4.36.1. RHBA-2012:0527 — gcc bug fix update

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

The gcc packages provide compilers for C, C++, Java, Fortran, Objective C, and Ada 95 GNU, as well as related support libraries.

Bug Fix

BZ#806394

GCC did not, under rare circumstances, handle exceptions properly when GCC 4.1 libstdc++ was used with GCC 4.4 or later C++11 code. This update improves exception handling so that GCC now processes exceptions as expected when using GCC 4.4 or later to compile code written in C++11.

Users of gcc are advised to upgrade to these updated packages only if they are encountering functionality problems related to C++11 exception handling.

4.36.2. RHBA-2013:0029 — gcc bug fix update

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

The gcc packages provide compilers for C, C++, Java, Fortran, Objective C, and Ada 95 GNU, as well as related support libraries.

Bug Fixes

BZ#750545

GCC was missing a lazy declaration of a class type destructor in the locate_dtor function in the method implementation. As a consequence, exception handling did not work as expected under certain circumstances and the generated code could terminate unexpectedly. This update adds the missing destructor declaration and the problem no longer occurs.

BZ#760417

Previously, GCC did not correctly handle processor registers and used an incorrect memory operand when processing the CMPXCHG8B instruction. As a consequence, the compiler generated erroneous code if the "-fPIC" option was used. This update modifies the underlying source code so that GCC now handles memory operands correctly and compiles position-independent code with the "fPIC" option as expected.

BZ#797938

GCC previously used incorrect flags for IBM System z specific options, such as "-m31", "-m64", "-mesa", "-mzarch", "-msoft-float", "-mhard-float", "-mlong-double-64" and "-mlong-double-128". As a consequence, when compiling code with any of these options, GCC did not recognize the option and the command failed. With this update, negative flags are now used for these options and code can be compiled successfully in this scenario.

BZ#806275

GCC did not, under rare circumstances, handle exceptions properly when GCC 4.1 libstdc++ was used with GCC 4.4 or later C++11 code. This update improves exception handling so that GCC now processes exceptions as expected when using GCC 4.4 or later to compile code written in C++11.

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

4.37. gcc44

4.37.1. RHBA-2013:0030 — gcc44 bug fix and enhancement update

Updated gcc44 packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The gcc44 packages provide the GNU Compiler Collection (GCC), which includes GNU compilers and related support libraries for C, C++, and Fortran programming languages. These packages also include libgomp, the GNU implementation of the OpenMP Application Programming Interface for multi-platform shared-memory parallel programming.

Note

The gcc44 packages have been upgraded to upstream version 4.4.7, which provides a number of bug fixes and enhancements over the previous version. Among others, this update fixes bugs causing GCC internal errors when compiling code with the "-O2" and "-O3" optimization options. Also, support for the OpenMP API version 3.1 has been added to libgomp to ensure compatibility with future GCC releases. (BZ#813708)

Bug Fixes

BZ#815207

Previous version of gcc44 incorrectly stated that the gcc44 package includes a technical preview of GCC version 4.4. The package description has been corrected and no longer claims to provide the technical preview of GCC version 4.4.

BZ#784360

Due to misplaced space characters in the x86 architecture driver, the "-mxop", "-mfma4", "-mbmi" and "-mtbm" compiler options were concatenated incorrectly when compiling code with gcc44. Consequently, compilation failed with an "unrecognized command line option" error. This update fixes space characters position and the options are concatenated correctly. Code is now compiled successfully with these options.

Enhancement

BZ#556962

G++ previously assumed that a value of enumeration type is always in the range specified by the C++ standard. Consequently, if a program converted an arbitrary integer value to the enumeration type, the code compiled with the "-fPIC -O2" or "-fPIC -O3" options could terminate unexpectedly. With this update, the underlying code has been modified to no longer assume strict evaluation of enumeration type. The old functionality can be turned on by specifying the "fstrict-enums" option.

All users of gcc44 are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.38. gdb

4.38.1. RHBA-2012:1257 — gdb bug fix update

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

The GNU Debugger (GDB) allows debugging of programs written in C, C++, Java, and other languages by executing them in a controlled fashion and then printing out their data.

Bug Fix

BZ#837894

When a struct member was at an offset greater than 256 MB, the resulting bit position within the struct overflowed and caused an invalid access by GDB. With this update, the code has been modified to ensure that GDB can access such positions.

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

4.38.2. RHBA-2013:0044 — gdb bug fix update

Updated gdb packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

The gdb packages provide the GNU Debugger (GDB) to debug programs written in C, C++, Java, and other languages by executing them in a controlled fashion and then printing out their data.

Bug Fixes

BZ#795423

Prior to this update, a bit position within a structure overflowed when a member of this structure was at an offset greater than 256 MB and GDB failed to access the position. This update modifies the underlying code to ensure that GDB can access such positions.

BZ#818343

Prior to this update, GDB incorrectly tried to load virtual dynamic shared objects (vDSO) from the file system when using the "solib-absolute-prefix" command. As a consequence, vDSOs could abort. This update modifies the underlying code to handle vDSOs as expected.

BZ#823789

Prior to this update, GDB failed to debug XLF generated code due to incorrect symbol handling. As a consequence, the type of variable in modules was not found. This update modifies the underlying code to handle symbols correctly and the type of a variable is found.

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

4.39. gdbm

4.39.1. RHBA-2012:0579 — gdbm bug fix update

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

Gdbm is a GNU database indexing library, which includes routines which use extensible hashing. Gdbm works in a similar way to standard UNIX dbm routines.

Bug Fix

BZ#671156

Prior to this update, gdbm-devel had no explicit requirements to gdbm, which could introduce interoperability problems. With this update, the gdbm-devel adds explicit requirements to the gdbm package.

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

4.40. gfs-kmod

4.40.1. RHBA-2013:0082 — gfs-kmod bug fix update

Udated gfs-kmod packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The gfs-kmod packages contain kernel modules that provide the ability to mount and use the Global File System (GFS).

Bug Fix

BZ#788694

Prior to this update, registered kobjects could, under certain circumstances, be freed while they were still in use. As a consequence, a kernel panic could occur when processing the gfs_controld daemon. This update adds the kobject release() method. Now, processing the gfs_controld daemon no longer causes a kernel panic.

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

4.41. gfs-utils

4.41.1. RHBA-2013:0095 — gfs-utils bug fix update

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

The gfs-utils packages provide various user-space tools necessary to mount, create, maintain, and test Global File Systems (GFS).

Bug Fix

BZ#788694

Prior to this update, the gfs_fsck file system checker failed to detect "bad indirect block pointer" corruptions due to incorrect error paths. This update modifies the gfs_fsck error paths. Now, gfs_fsck detects and repairs corruptions as expected.

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

4.42. gfs2-utils

4.42.1. RHBA-2013:0079 — 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 packages provide the user-space utilities necessary to mount, create, maintain and test GFS2 file systems.

Bug Fix

BZ#838910

Prior to this update, an overly long cluster name in /etc/cluster/cluster.conf could cause a buffer overflow when running fsck.gfs2 on a GFS2 file system with a corrupt super block. This update modifies the underlying code to to ensure that the cluster name is truncated appropriately when the super block is being rebuilt. Now, this buffer overflow condition is prevented.

All users of gfs2-utils are advised to upgrade to these updated packages, which fix this bug.

4.43. ghostscript

4.43.1. RHSA-2012:1256 — Moderate: ghostscript security update

Updated ghostscript 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 for each vulnerability from the CVE link(s) associated with each description below.

Ghostscript is a set of software that provides a PostScript interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language) and an interpreter for Portable Document Format (PDF) files.

Security Fix

CVE-2012-4405

An integer overflow flaw, leading to a heap-based buffer overflow, was found in Ghostscript's International Color Consortium Format library (icclib). An attacker could create a specially-crafted PostScript or PDF file with embedded images that would cause Ghostscript to crash or, potentially, execute arbitrary code with the privileges of the user running Ghostscript.

Red Hat would like to thank Marc Schönefeld for reporting this issue.

Users of Ghostscript are advised to upgrade to these updated packages, which contain a backported patch to correct this issue.

4.44. gimp

4.44.1. RHBA-2012:1242 — gimp bug fix update

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

The GIMP (GNU Image Manipulation Program) is an image composition and editing program. GIMP provides a large image manipulation toolbox, including channel operations and layers, effects, sub-pixel imaging and anti-aliasing, and conversions, all with multi-level undo.

Bug Fix

BZ#452998

Prior to this update, the Postscript plug-in could abort with a segmentation fault when saving images as Postscript files from GIMP if a preview was embedded in the file. This update modifies the underlying code so to handle embedded previews.

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

4.44.2. RHSA-2012:1181 — Moderate: gimp security update

Updated gimp 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. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The GIMP (GNU Image Manipulation Program) is an image composition and editing program.

Security Fixes

CVE-2009-3909, CVE-2012-3402

Multiple integer overflow flaws, leading to heap-based buffer overflows, were found in the GIMP's Adobe Photoshop (PSD) image file plug-in. An attacker could create a specially-crafted PSD image file that, when opened, could cause the PSD plug-in to crash or, potentially, execute arbitrary code with the privileges of the user running the GIMP.

CVE-2012-3481

An integer overflow flaw, leading to a heap-based buffer overflow, was found in the GIMP's GIF image format plug-in. An attacker could create a specially-crafted GIF image file that, when opened, could cause the GIF plug-in to crash or, potentially, execute arbitrary code with the privileges of the user running the GIMP.

CVE-2011-2896

A heap-based buffer overflow flaw was found in the Lempel-Ziv-Welch (LZW) decompression algorithm implementation used by the GIMP's GIF image format plug-in. An attacker could create a specially-crafted GIF image file that, when opened, could cause the GIF plug-in to crash or, potentially, execute arbitrary code with the privileges of the user running the GIMP.

CVE-2012-3403

A heap-based buffer overflow flaw was found in the GIMP's KiSS CEL file format plug-in. An attacker could create a specially-crafted KiSS palette file that, when opened, could cause the CEL plug-in to crash or, potentially, execute arbitrary code with the privileges of the user running the GIMP.

Red Hat would like to thank Secunia Research for reporting CVE-2009-3909, and Matthias Weckbecker of the SUSE Security Team for reporting CVE-2012-3481.

Users of the GIMP are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The GIMP must be restarted for the update to take effect.

4.45. glibc

4.45.1. RHBA-2012:0498 — 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#810323

Previously, glibc did not walk through the entire list of Network Information Service (NIS) password or group buffers. As a consequence, when utilizing the NIS password or group maps, allocated memory was not freed properly, which caused memory leaks. This update modifies glibc to walk through the entire lists so that memory is freed as expected and memory leaks no longer occur in this scenario.

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

4.45.2. RHBA-2013:0022 — glibc bug fix and enhancement update

Updated *glibc* packages that fix multiple bugs and add several enhancements 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.*glibc* is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.

Bug Fixes

BZ#823905

Using the **`iconv()`** or the **`iconv`** command to convert a file or string from IBM-930 encoding to another encoding, such as UTF-8, resulted in a segmentation fault. This happened if the file or string contained the invalid multibyte character **`0xffff`**. Now, the conversion code for the IBM-930 encoding recognizes this invalid character and calls an error handler and the segmentation fault no

longer occurs.

BZ#837852

Due to logic errors, functions **exp()**, **exp2()**, **pow()**, **sin()**, **tan()**, and **rint()** could return different results in non-default rounding modes or terminate with a segmentation fault. Multiple fixes have been applied to the function implementations and the functions now return correct results in all rounding modes.

Note that the change can cause runtime performance loss as values which were previously handled by the fast function implementation are now handled by the slower multi-precision library to achieve accurate results.

BZ#813348

The dynamic linker previously sorted cyclic dependencies incorrectly when there were more that 127 Dynamic Shared Objects (DSO). The changed order of the dependencies caused some programs to behave differently or crash due to symbol resolution failure. This update fixes the initialization order of the cyclic dependencies and the problem no longer occurs.

BZ#848481

Various functions that called the **nl_explode_name()** function failed to check its return value for errors. As a result, applications could terminate unexpectedly after passing a NULL pointer or uninitialized values to the calling functions. The callers of **nl_explode_name()** have been updated to check for error conditions and fail gracefully.

BZ#808014

Previously, if the Name Service Cache Daemon (nscd) daemon received a CNAME (Canonical Name) record as a response to a DNS (Domain Name System) query, the cached DNS entry adopted the TTL (Time to Live) value of the underlying **A** or **AAAA** response. This caused the nscd daemon to wait for an unexpectedly long time before reloading the DNS entry. With this update, nscd uses the shortest TTL from the response as the TTL value for the entire record and DNS entries are now reloaded as expected in this scenario.

BZ#799853

The Slovak currency was set to the Slovak Crown. However, Slovakia now uses the Euro. The Slovak currency was set to the Euro.

BZ#809325

Previously, glibc did not walk through the entire list of buffers. As a consequence, when utilizing the NIS password or group maps, allocated memory was not freed properly, which caused memory leaks. This update modifies glibc to walk through the entire list so that memory is freed as expected and memory leaks no longer occur in this scenario.

BZ#751748

A race between the **_IO_flush_all_lockp()** function and **pthread_cancel()** function could cause a process to become unresponsive during forking. This happened because the **_IO_unlock_lock** macro decremented the lock count before it attempted to unlock its lock and did not check if the count contained a positive value. If the lock was never held since **_IO_unlock_lock()**, the macro did not release the lock due to the lock count being less than zero. With this update, the lock count is decremented only if it contains a positive value.

BZ#639000

The Ukrainian currency symbol was incorrectly set to **rp**. With this update, the currency symbol was corrected to **rpH**.

BZ#759341

A race condition existed between functions which allocated and reclaimed stacks in multi-threaded applications. As a result, some applications could enter a deadlock. The code for managing lists of stacks has been changed to publish its changes to all threads at the appropriate time. This fixes synchronization between the multiple threads and eliminates the race condition.

BZ#788989

The Name Service Cache Daemon (nscd) terminated unexpectedly if a group contained a few thousand members. This was caused by a stack overflow which resulted in a segmentation fault in nscd. With this update, when a large amount of memory is needed for a group with many members, the memory is allocated on the heap instead of the stack. This prevents the stack overflow and nscd no longer crashes in this scenario.

BZ#839572

During installation on IBM System z, Red Hat Enterprise Linux Server installer returned traceback with the following error value after the stage2 download:

```
ValueError: (3, 'No such process')
```

This was due to a workaround implementation for IBM System z in the **fegetenv()** function in the **math.h** header file. With this update, the function implementation was modified so as to follow the IEEE standard and the problem no longer occurs.

BZ#769852

A race condition between the **setuid()** function and the **sighandler_setxid()** function could result in a lock remaining unreleased. As a result, an application could remain in a deadlock. With this update, the lock is released in this scenario and proper synchronization between the threads is maintained.

BZ#843672

Prior to this update, when a multi-threaded process called the **qsort()** function, a race condition could occur. This could result in an uninitialized memory read and the process could receive a floating point exception or other fault condition. The race condition in the function code has been fixed and the problem no longer occurs.

BZ#766832

Calling the **strncmp()** function on the Power4 processors could cause the program to terminate unexpectedly. This occurred because the function occasionally attempted to read past the zero byte in certain cases. With this update, strings are aligned correctly and the function no longer attempts to read past the zero byte.

BZ#710216

The Portuguese locale (pt_PT.utf8) incorrectly used the **$** character instead of the **,** character as its decimal point. The error has been corrected and the **,** character is now used as the decimal point as expected.

BZ#703239

Previously, if the **/etc/resolv.conf** file contained an IPv6 DNS server address with trailing

spaces, the address failed to be parsed correctly and DNS lookups with the **ping6** command failed. With this update, the parsing code has been corrected so as to cope with trailing spaces and the problem no longer occurs.

BZ#692182

The **sysconf()** function allows applications to determine values for system limits or options at runtime. The mechanism that sysconf uses to acquire various CACHE parameters previously failed to look up the requested information on Intel Xeon X5670 processors and incorrectly returned zero values. The **sysconf()** function has been modified to acquire the system information on these processors correctly and the problem no longer occurs.

BZ#806403

A missing check of memory allocation and an incorrect loop test in the **nss/getnssent.c** source file could cause an application to fail. The memory allocation check and the loop test code have been added and the problem no longer occurs.

BZ#851450

Previously, the **ttyname()** and **ttyname_r()** calls returned an error if the **/proc/** directory was not mounted. Consequently, some applications did not run in the chroot environment properly. With this update, if the **/proc/self/fd/** directory cannot be read, the calls iterate through devices first and only then return an error. As a result, applications which were previously failing now work correctly.

BZ#500767

The **getgrent()** function generated an error when it requested to read a Network Information Services (NIS) group record of 1024 bytes from the NIS master server. This happened because the function attempted to free an unallocated pointer. With this update, the **free()** function is not called under these circumstances and **getgrent()** now works as expected in this scenario.

BZ#797096

Various functions (**glob_in_dir**, **getaddrinfo**) could potentially allocate unlimited amounts of data on the stack. As a result, these functions were potential security attack vectors. With this update, these routines use **malloc()** when allocating large amounts of memory and the security issue is eliminated.

BZ#657266

The Finnish locale included redundant trailing spaces in month abbreviations. This could cause parsing and conversion problems when working with dates. With this update, the trailing spaces have been removed from the definition of abbreviated month format and the parsing and conversion of abbreviated month names work as expected.

BZ#657588

Abbreviated month names in the simplified Chines locale (zh_CN) contained redundant spaces, which caused incorrect output of dates. With this update, the spaces have been removed from the format definition and the system returns dates formatted correctly.

BZ#678227

The Name Service Cache Daemon (nscd) initscript was returning a non-zero exit status when a stop was requested on an already stopped daemon. However, the expected behavior is to consider the request to be successful and return the exit status of zero. The nscd initscript has been modified to handle this case correctly and set the exit status appropriately.

BZ#819430

Previously, the **fnmatch()** function failed and returned the -1 status code when its pattern argument contained the wildcard character * and the file name argument contained an invalid multibyte encoding character. The **fnmatch()** function now handles such arguments gracefully: it considers the invalid characters not to match and proceeds.

BZ#800240

If the maximum number of memory pools (arenas) used by a thread was set to 1 (MALLOC_ARENA_MAX=1), the setting was ignored and the program still used multiple pools due to incorrect logic when checking the number of pools in use and reusing pools. With this update, the underlying code has been modified and the pool setting is applied as expected.

BZ#857387

The **vfprintf()** function returned the **ERANGE** errno instead of **EOVERFLOW** when a string of a too long format was specified. The errno is now set correctly to **EOVERFLOW** in this scenario.

Enhancements

BZ#795896

A Virtual Dynamic Shared Object (VDSO) allows an application in user space to perform some kernel actions with less overhead than if using a system call. The VDSO is often used to provide fast access to the **gettimeofday** system call data. Support for VDSOs on the IBM System z series platform has been added to glibc.

BZ#641094

Previously, the **pthread_create()** function used the MAP_32BIT flag to reserve the lower 32 bits of virtual address space for thread stacks so as to provide better performance. This setting is no longer of benefit and in some cases can negatively impact performance. A patch has been backported so that **pthread_create()** now uses the MAP_STACK flag instead of the MAP_32BIT flag.

BZ#765710

The **getaddrinfo()** function returns one or more **addrinfo** structures, each of which contains an Internet socket address. If the hints argument to **getaddrinfo()** is not NULL, it specifies criteria for selecting the socket address structures to be returned. Previously, **getaddrinfo()** did not support the Stream Control Transmission Protocol (SCTP) hints. With this update, the **getaddrinfo()** function has been enhanced to accept SCTP hints.

Users of *glibc* are advised to upgrade to these updated packages, that fix these bug and add these enhancements.

4.45.3. RHSA-2012:0397 — Moderate: glibc security update

Updated glibc 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 for each vulnerability from the CVE link(s) associated with each description below.

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.

Security Fix

CVE-2012-0864

An integer overflow flaw was found in the implementation of the printf functions family. This could allow an attacker to bypass FORTIFY_SOURCE protections and execute arbitrary code using a format string flaw in an application, even though these protections are expected to limit the impact of such flaws to an application abort.

All users of glibc are advised to upgrade to these updated packages, which contain a patch to resolve this issue.

4.45.4. RHSA-2012:1097 — Moderate: glibc security and bug fix update

Updated glibc packages that fix one security issue and one bug 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 for each vulnerability from the CVE link(s) associated with each description below.

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 properly.

Security Fix

CVE-2012-3406

It was discovered that the formatted printing functionality in glibc did not properly restrict the use of alloca(). This could allow an attacker to bypass FORTIFY_SOURCE protections and execute arbitrary code using a format string flaw in an application, even though these protections are expected to limit the impact of such flaws to an application abort.

Bug Fix

BZ#837896

If a file or a string was in the IBM-930 encoding, and contained the invalid multibyte character "0xffff", attempting to use iconv() (or the iconv command) to convert that file or string to another encoding, such as UTF-8, resulted in a segmentation fault. With this update, the conversion code for the IBM-930 encoding recognizes this invalid character and calls an error handler, rather than causing a segmentation fault.

All users of glibc are advised to upgrade to these updated packages, which contain backported patches to fix these issues.

4.45.5. RHSA-2012:1207 — Moderate: glibc security and bug fix update

Updated glibc packages that fix multiple security issues and one bug 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 for each vulnerability from the CVE link(s) associated with each description below.

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 properly.

Security Fix

CVE-2012-3480

Multiple integer overflow flaws, leading to stack-based buffer overflows, were found in glibc's functions for converting a string to a numeric representation (strtod(), strtof(), and strtold()). If an application used such a function on attacker controlled input, it could cause the application to crash or, potentially, execute arbitrary code.

Bug Fix

BZ#839411

Previously, logic errors in various mathematical functions, including exp, exp2, expf, exp2f, pow, sin, tan, and rint, caused inconsistent results when the functions were used with the non-default rounding mode. This could also cause applications to crash in some cases. With this update, the functions now give correct results across the four different rounding modes.

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

4.46. gnbd

4.46.1. RHBA-2013:0110 — gnbd bug fix update

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

The gnbd package provides user-level tools for manipulating the global network block device (GNBD).

Bug Fix

BZ#500591

Prior to this update, the gnbd makefile stripped the binaries of their debugging symbols. As a consequence, the gnbd debuginfo package was empty. This update removes the strip commands from the gnbd makefiles. Now, the debuginfo packages have all the appropriate information.

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

4.47. gnome-session

4.47.1. RHBA-2012:1220 — gnome-session bug fix update

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

The gnome-session package provides a utility to start up and manage the GNOME desktop session. Gnome-session starts up other core components of GNOME and handles log-outs and saves the sessions.

Bug Fix

BZ#477688

Prior to this update, the gnome-session utility did not fully honor the "Hidden=" key in autostart desktop files. As a consequence, users could not mark autostart files as Hidden= in their home directory to disable autostart files in system directories.With this update, gnome-session allows

users to "mask" system autostart files by installing a file of the same name in ~/.config/autostart with a key Hidden=true when loading autostart files.

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

4.48. gnome-vfs2

4.48.1. RHSA-2013:0131 — Low: gnome-vfs2 security and bug fix update

Updated gnome-vfs2 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 for each vulnerability from the CVE link(s) associated with each description below.

The gnome-vfs2 packages provide the GNOME Virtual File System, which is the foundation of the Nautilus file manager. neon is an HTTP and WebDAV client library embedded in the gnome-vfs2 packages.

Security Fix

CVE-2009-2473

A denial of service flaw was found in the neon Extensible Markup Language (XML) parser. Visiting a malicious DAV server with an application using gnome-vfs2 (such as Nautilus) could possibly cause the application to consume an excessive amount of CPU and memory.

Bug Fixes

BZ#580855

When extracted from the Uniform Resource Identifier (URI), gnome-vfs2 returned escaped file paths. If a path, as stored in the URI, contained non-ASCII characters or ASCII characters which are parsed as something other than a file path (for example, spaces), the escaped path was inaccurate. Consequently, files with the described type of URI could not be processed. With this update, gnome-vfs2 properly unescapes paths that are required for a system call. As a result, these paths are parsed properly.

BZ#586015

In certain cases, the trash info file was populated by foreign entries, pointing to live data. Emptying the trash caused an accidental deletion of valuable data. With this update, a workaround has been applied in order to prevent the deletion. As a result, the accidental data loss is prevented, however further information is still gathered to fully fix this problem.

BZ#621394

Due to a wrong test checking for a destination file system, the Nautilus file manager failed to delete a symbolic link to a folder which was residing in another file system. With this update, a special test has been added. As a result, a symbolic link pointing to another file system can be trashed or deleted properly.

BZ#772307

Prior to this update, when directories without a read permission were marked for copy, the Nautilus file manager skipped these unreadable directories without notification. With this update, Nautilus displays an error message and properly informs the user about the aforementioned problem.

BZ#822817

Previously, gnome-vfs2 used the stat() function calls for every file on the MultiVersion File System (MVFS), used for example by IBM Rational ClearCase. This behavior significantly slowed down file operations. With this update, the unnecessary stat() operations have been limited. As a result, gnome-vfs2 user interfaces, such as Nautilus, are more responsive.

All gnome-vfs2 users are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

4.49. gnutls

4.49.1. RHBA-2012:0319 — gnutls bug fix update

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

The gnutls package provides the GNU Transport Layer Security (GnuTLS) library, which provides a secure layer over a transport layer using protocols such as TLS, SSL and DTLS.

Bug Fix

BZ#789041

Under certain circumstances, a NULL pointer could have been dereferenced in the GnuTLS library. This caused TLS clients, such as the rsyslog utility, to terminate unexpectedly with a segmentation fault. This update adds a test condition ensuring that a NULL pointer can no longer be dereferenced and TLS clients no longer crash.

All users of gnutls are advised to upgrade to these updated packages, which fix this bug. All applications linked with the GnuTLS library must be restarted (or the system rebooted) in order for this update to take effect.

4.49.2. RHBA-2013:0028 — gnutls bug fix update

Updated gnutls packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

The gnutls packages provides the GNU Transport Layer Security (GnuTLS) library, which provides a secure layer over a transport layer using protocols such as TLS, SSL, and DTLS.

Bug Fixes

BZ#592112

The gnutls packages reported wrong distinguished names (DNs) for chain CA certificates used for the client authentication; the issuer DN was reported instead of the subject DN. As a consequence, the TLS clients were not able to provide a client certificate signed by a chain CA certificate when connecting to a gnutls TLS server. The underlying source code has been modified and gnutls now reports the right DN and the TLS clients work as expected in the described scenario.

BZ#730816

Previously, in the certool utility was a missing check used for an empty string when a challenge password was entered. Consequently, certificate requests generated by certtool were sometimes invalid when an empty challenge password was used. This missing empty-string check has been added and now the certtool's certificate requests are valid even if the challenge password is not entered.

BZ#785001

Under certain circumstances, a null pointer could be dereferenced in the GnuTLS library. This caused TLS clients, such as the rsyslog utility, to terminate unexpectedly with a segmentation fault. This update adds a test condition ensuring that null pointers can no longer be dereferenced and TLS clients no longer crash.

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

4.49.3. RHSA-2012:0428 — Important: gnutls security update

Updated gnutls 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The GnuTLS library provides support for cryptographic algorithms and for protocols such as Transport Layer Security (TLS). GnuTLS includes libtasn1, a library developed for ASN.1 (Abstract Syntax Notation One) structures management that includes DER (Distinguished Encoding Rules) encoding and decoding.

Security Fixes

CVE-2012-1573

A flaw was found in the way GnuTLS decrypted malformed TLS records. This could cause a TLS/SSL client or server to crash when processing a specially-crafted TLS record from a remote TLS/SSL connection peer.

CVE-2012-1569

A flaw was found in the way libtasn1 decoded DER data. An attacker could create a carefully-crafted X.509 certificate that, when parsed by an application that uses GnuTLS, could cause the application to crash.

CVE-2011-4128

A boundary error was found in the gnutls_session_get_data() function. A malicious TLS/SSL server could use this flaw to crash a TLS/SSL client or, possibly, execute arbitrary code as the client, if the client passed a fixed-sized buffer to gnutls_session_get_data() before checking the real size of the session data provided by the server.

Red Hat would like to thank Matthew Hall of Mu Dynamics for reporting CVE-2012-1573 and CVE-2012-1569.

Users of GnuTLS are advised to upgrade to these updated packages, which contain backported patches to correct these issues. For the update to take effect, all applications linked to the GnuTLS library must be restarted, or the system rebooted.

4.50. gpxe

4.50.1. RHBA-2013:0057 — gpxe bug fix update

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

The gpxe packages provide gPXE, an open source Preboot Execution Environment (PXE) implementation and bootloader.

Bug Fix

BZ#714882

The gpxe-roms-qemu runs the update-alternatives utility during installation; however, the chkconfig package, which provides the utility, was previously not required by gpxe-roms-qemu. As a consequence, the installation could fail with a "No such file or directory" error message. The chkconfig package has been added as a dependency to ensure successful installation of gpxe-roms-qemu.

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

4.51. grub

4.51.1. RHBA-2013:0087 — grub bug fix update

Updated grub packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

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

Bug Fixes

BZ#212649

The grub documentation contained incorrect information about the planned but unimplemented "grub-set-default" command; the "savedefault" command has been implemented instead, providing similar functionality. This update corrects the grub documentation that now reflect only those commands which have been implemented in GRUB.

BZ#782096

Prior to this update, the "grub-install" command was matching only against one letter after the "sd" string in the disk's device path name. Consequently, disks named "sdaa" and higher were not recognized as disks. The matching expression has been changed and now the "grub-install" command matches against any number of reasonable characters after the "sd" string in the disk's device path name.

BZ#829228

Previously, the number of disks was hard-coded to a maximum of 8. As a consequence, no more than 8 devices could be used. This update has changed the definition of allowed disks to a maximum of 128 and now up to 128 devices can be used.

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

4.52. gtk+

4.52.1. RHBA-2013:0108 — gtk+ bug fix update

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

The gtk+ packages provide a multi-platform toolkit for creating graphical user interfaces.

Bug Fix

BZ#694888

Using a Wacom tablet with a dual head configuration caused an error in the GTK+ toolkit when the input coordinates of the Wacom tablet were bound to a single monitor. Consequently, drawing with a pen with pressure sensitivity enabled led to an offset between the pen position and the content drawn on the screen. This update changes the way that input coordinates are translated by the library in this specific case.

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

4.53. gtk2

4.53.1. RHBA-2013:0001 — 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#830901

Previously, performing drag-and-drop operations on tabs in applications using the GtkNotebook widget could lead to releasing the same resource twice. Eventually, this behavior caused a segmentation fault. This bug has been fixed, and the applications using GtkNotebook no longer crash in the described scenario.

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

4.53.2. RHSA-2013:0135 — Low: gtk2 security and bug fix update

Updated gtk2 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 for each vulnerability from the CVE link(s) associated with each description below.

GIMP Toolkit (GTK+) is a multi-platform toolkit for creating graphical user interfaces.

Security Fix

CVE-2012-2370

An integer overflow flaw was found in the X BitMap (XBM) image file loader in GTK+. A remote attacker could provide a specially-crafted XBM image file that, when opened in an application linked against GTK+ (such as Nautilus), would cause the application to crash.

Bug Fixes

BZ#487630

Due to a bug in the Input Method GTK+ module, the usage of the Taiwanese Big5 (zh_TW.Big-5) locale led to the unexpected termination of certain applications, such as the GDM greeter. The bug has been fixed, and the Taiwanese locale no longer causes applications to terminate unexpectedly.

BZ#518483

When a file was initially selected after the GTK+ file chooser dialog was opened and the Location field was visible, pressing the Enter key did not open the file. With this update, the initially selected file is opened regardless of the visibility of the Location field.

BZ#523657

When a file was initially selected after the GTK+ file chooser dialog was opened and the Location field was visible, pressing the Enter key did not change into the directory. With this update, the dialog changes into the initially selected directory regardless of the visibility of the Location field.

BZ#603809

Previously, the GTK Print dialog did not reflect the user-defined printer preferences stored in the ~/.cups/lpoptions file, such as those set in the Default Printer preferences panel. Consequently, the first device in the printer list was always set as a default printer. With this update, the underlying source code has been enhanced to parse the option file. As a result, the default values in the print dialog are set to those previously specified by the user.

BZ#702342

The GTK+ file chooser did not properly handle saving of nameless files. Consequently, attempting to save a file without specifying a file name caused GTK+ to become unresponsive. With this update, an explicit test for this condition has been added into the underlying source code. As a result, GTK+ no longer hangs in the described scenario.

BZ#743658

When using certain graphics tablets, the GTK+ library incorrectly translated the input coordinates. Consequently, an offset occurred between the position of the pen and the content drawn on the screen. This issue was limited to the following configuration: a Wacom tablet with input coordinates bound to a single monitor in a dual head configuration, drawing with a pen with the pressure sensitivity option enabled. With this update, the coordinate translation method has been changed, and the offset is no longer present in the described configuration.

BZ#830901

Previously, performing drag and drop operations on tabs in applications using the GtkNotebook widget could lead to releasing the same resource twice. Eventually, this behavior caused the applications to terminate with a segmentation fault. This bug has been fixed, and the applications using GtkNotebook no longer terminate in the aforementioned scenario.

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

4.54. guagga

4.54.1. RHSA-2012:1258 — Moderate: quagga security update

Updated quagga 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. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Quagga is a TCP/IP based routing software suite. The Quagga bgpd daemon implements the BGP (Border Gateway Protocol) routing protocol. The Quagga ospfd and ospf6d daemons implement the OSPF (Open Shortest Path First) routing protocol.

Security Fixes

CVE-2011-3327

A heap-based buffer overflow flaw was found in the way the bgpd daemon processed malformed Extended Communities path attributes. An attacker could send a specially-crafted BGP message, causing bgpd on a target system to crash or, possibly, execute arbitrary code with the privileges of the user running bgpd. The UPDATE message would have to arrive from an explicitly configured BGP peer, but could have originated elsewhere in the BGP network.

CVE-2010-1674

A NULL pointer dereference flaw was found in the way the bgpd daemon processed malformed route Extended Communities attributes. A configured BGP peer could crash bgpd on a target system via a specially-crafted BGP message.

CVE-2011-3323

A stack-based buffer overflow flaw was found in the way the ospf6d daemon processed malformed Link State Update packets. An OSPF router could use this flaw to crash ospf6d on an adjacent router.

CVE-2011-3324

A flaw was found in the way the ospf6d daemon processed malformed link state advertisements. An OSPF neighbor could use this flaw to crash ospf6d on a target system.

CVE-2011-3325

A flaw was found in the way the ospfd daemon processed malformed Hello packets. An OSPF neighbor could use this flaw to crash ospfd on a target system.

CVE-2011-3326

A flaw was found in the way the ospfd daemon processed malformed link state advertisements. An OSPF router in the autonomous system could use this flaw to crash ospfd on a target system.

CVE-2012-0249

An assertion failure was found in the way the ospfd daemon processed certain Link State Update packets. An OSPF router could use this flaw to cause ospfd on an adjacent router to abort.

CVE-2012-0250

A buffer overflow flaw was found in the way the ospfd daemon processed certain Link State Update packets. An OSPF router could use this flaw to crash ospfd on an adjacent router.

Red Hat would like to thank CERT-FI for reporting CVE-2011-3327, CVE-2011-3323, CVE-2011-3324, CVE-2011-3325, and CVE-2011-3326; and the CERT/CC for reporting CVE-2012-0249 and CVE-2012-0250. CERT-FI acknowledges Riku Hietamäki, Tuomo Untinen and Jukka Taimisto of the Codenomicon CROSS project as the original reporters of CVE-2011-3327, CVE-2011-3323, CVE-2011-3324, CVE-2011-3325, and CVE-2011-3326. The CERT/CC acknowledges Martin Winter at OpenSourceRouting.org as the original reporter of CVE-2012-0249 and CVE-2012-0250.

Users of quagga should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the bgpd, ospfd, and ospf6d daemons will be restarted automatically.

4.55. hal

4.55.1. RHBA-2013:0107 — hal bug fix update

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

The HAL daemon collects and maintains information about the hardware on the system from several sources, and provides a live device list through D-BUS.

Bug Fixes

BZ#704079

Previously, the HAL daemon sometimes identified a non-existent error when running a new process and displayed the following warning:

Warning: Error while wite r->input () to stdin_v.

This bug has been fixed and the HAL daemon now works properly in the described scenario.

BZ#555303

The previous version of the hal package did not provide a manual page for the hal-device utility. This update adds the hal-device(1) manual page to this package.

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

4.56. hplip3

4.56.1. RHSA-2013:0133 — Low: hplip3 security and bug fix update

Updated hplip3 packages that fix one security issue and one bug 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 for each vulnerability from the CVE link(s) associated with each description below.

Hewlett-Packard Linux Imaging and Printing (HPLIP) provides drivers for Hewlett-Packard (HP) printers and multifunction peripherals.

Security Fix

CVE-2011-2722

It was found that the HP CUPS (Common UNIX Printing System) fax filter in HPLIP created a temporary file in an insecure way. A local attacker could use this flaw to perform a symbolic link attack, overwriting arbitrary files accessible to a process using the fax filter (such as the hp3-sendfax tool).

Bug Fix

BZ#501834

Previous modifications of the hplip3 package to allow it to be installed alongside the original hplip package introduced several problems to fax support; for example, the hp-sendfax utility could become unresponsive. These problems have been fixed with this update.

All users of hplip3 are advised to upgrade to these updated packages, which contain backported patches to correct these issues.

4.57. hsqldb

4.57.1. RHBA-2013:0114 — hsqldb bug fix update

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

HSQLDB is a relational database engine written in Java, with a JDBC driver, supporting a subset of ANSI-92 SQL. It offers a small (about 100k), fast database engine which offers both in-memory and disk-based tables. Embedded and server modes are available. Additionally, it includes tools such as a minimal web server, in-memory query and management tools (which can be run as applets or servlets), and a number of demonstration examples.

BZ#844877

The HSQLDB database did not depend on java packages of version 1:1.6.0 or later, which caused the hsqldb packages to be installed incorrectly in some cases. Consequently, the build-classpath command did not work on systems without the java-1.6.0-openjdk package installed. This update modifies the hsqldb spec file to add a requirement for java-1.6.0-openjdk, and the installation of hsqldb now proceeds correctly as expected.

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

4.58. httpd

4.58.1. RHBA-2012:0714 — 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#825675

Due to a bug in the "mod_cache" module, an unexpected "304 Not Modified" HTTP response could be incorrectly returned to the client on non-conditional HTTP GET requests. With this update, the "mod_cache" module has been modified to correctly handle 304 responses, which are not returned in this scenario.

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

4.58.2. RHBA-2012:1448 — httpd bug fix update

Updated httpd packages that fix two bugs 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 Fixes

BZ#873677

Due to a bug in the "mod_mem_cache" module, an aborted HTTP connection could result in a cached entity becoming corrupt. With this update, the "mod_mem_cache" module has been fixed to correctly handle aborted connections, avoiding cache corruption in this scenario.

BZ#873730

Due to a bug in the "mod_cache" module, the "304 Not Modified" response from an origin server was not properly handled when a cached entity was being refreshed. Consequently, the entity could be returned to the HTTP client with incorrect headers. With this update, the "mod_cache" module has been modified to correctly handle headers in the "304 Not Modified" response. The cached entity is now returned with correct headers in this scenario.

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

4.58.3. RHSA-2013:0130 — Low: httpd security, bug fix, and enhancement update

Updated httpd packages that fix multiple 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 low security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The httpd packages contain the Apache HTTP Server (httpd), which is the namesake project of The Apache Software Foundation.

Security Fix

CVE-2008-0455, CVE-2008-0456, CVE-2012-2687

Input sanitization flaws were found in the mod_negotiation module. A remote attacker able to upload or create files with arbitrary names in a directory that has the MultiViews options enabled, could use these flaws to conduct cross-site scripting and HTTP response splitting attacks against users visiting the site.

Bug Fix

BZ#752618

Previously, no check was made to see if the /etc/pki/tls/private/localhost.key file was a valid key prior to running the "%post" script for the "mod_ssl" package. Consequently, when /etc/pki/tls/certs/localhost.crt did not exist and "localhost.key" was present but invalid, upgrading the Apache HTTP Server daemon (httpd) with mod_ssl failed. The "%post" script has been fixed to test for an existing SSL key. As a result, upgrading httpd with mod_ssl now proceeds as expected.

BZ#773473

The "mod_ssl" module did not support operation under FIPS mode. Consequently, when operating Red Hat Enterprise Linux 5 with FIPS mode enabled, httpd failed to start. An upstream patch has been applied to disable non-FIPS functionality if operating under FIPS mode and httpd now starts as expected.

BZ#783242

Prior to this update, httpd exit status codes were not Linux Standard Base (LSB) compliant. When the command "service httpd reload" was run and httpd failed, the exit status code returned was "0" and not in the range 1 to 6 as expected. A patch has been applied to the init script and httpd now returns "1" as an exit status code.

BZ#840845

Chunked Transfer Coding is described in RFC 2616. Previously, the Apache server did not correctly handle a chunked encoded POST request with a "chunk-size" or "chunk-extension" value of 32 bytes or more. Consequently, when such a POST request was made the server did not respond. An upstream patch has been applied and the problem no longer occurs.

BZ#845532

Due to a regression, when mod_cache received a non-cacheable 304 response, the headers were served incorrectly. Consequently, compressed data could be returned to the client without the cached headers to indicate the data was compressed. An upstream patch has been applied to merge response and cached headers before data from the cache is served to the client. As a result cached data is now correctly interpreted by the client.

BZ#853128

In a proxy configuration, certain response-line strings were not handled correctly. If a response-line without a "description" string was received from the origin server, for a non-standard status code, such as the "450" status code, a "500 Internal Server Error" would be returned to the client. This bug has been fixed so that the original response line is returned to the client.

Enhancements

BZ#727342

The configuration directive "LDAPReferrals" is now supported in addition to the previously introduced "LDAPChaseReferrals".

BZ#767890

The AJP support module for "mod_proxy", "mod_proxy_ajp", now supports the "ProxyErrorOverride" directive. Consequently, it is now possible to configure customized error pages for web applications running on a backend server accessed via AJP.

BZ#833042

The "%posttrans" scriptlet which automatically restarts the httpd service after a package upgrade can now be disabled. If the file /etc/sysconfig/httpd-disable-posttrans exists, the scriptlet will not restart the daemon.

BZ#833043

The output of "httpd -S" now includes configured alias names for each virtual host.

BZ#840036

New certificate variable names are now exposed by "mod_ssl" using the "_DN_userID" suffix, such as "SSL_CLIENT_S_DN_userID", which use the commonly used object identifier (OID) definition of "userID", OID 0.9.2342.19200300.100.1.1.

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

4.58.4. RHBA-2013:0139 — httpd bug fix update

4.58.4. RHBA-2013:0139 — 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#873678

Due to a bug in the mod_mem_cache module, an aborted HTTP connection could result in a cached entity becoming corrupt. This update fixes mod_mem_cache to correctly handle aborted connections, thus avoiding cache corruption in this scenario.

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

4.59. hwdata

4.59.1. RHBA-2013:0101 — hwdata bug fix and enhancement update

Updated hwdata packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 5.

The hwdata packages contain various hardware identification and configuration data.

Bug Fix

BZ#824559

Due to a syntax error in the usb.ids file, the lsusb utility failed to display a list of used USB devices. The syntax error has been removed from the usb.ids file and the lsusb utility now displays the information correctly.

Enhancement

BZ#839225, BZ#870363

The PCI ID numbers have been updated for the Beta and the Final compose lists.

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

4.60. ImageMagick

4.60.1. RHSA-2012:0545 — Moderate: ImageMagick security and bug fix update

Updated ImageMagick packages that fix three security issues and one bug 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

ImageMagick is an image display and manipulation tool for the X Window System that can read and write multiple image formats.

CVE-2012-0247

A flaw was found in the way ImageMagick processed images with malformed Exchangeable image file format (Exif) metadata. An attacker could create a specially-crafted image file that, when opened by a victim, would cause ImageMagick to crash or, potentially, execute arbitrary code.

CVE-2012-0248

A denial of service flaw was found in the way ImageMagick processed images with malformed Exif metadata. An attacker could create a specially-crafted image file that, when opened by a victim, could cause ImageMagick to enter an infinite loop.

CVE-2012-0260

A denial of service flaw was found in the way ImageMagick decoded certain JPEG images. A remote attacker could provide a JPEG image with specially-crafted sequences of RST0 up to RST7 restart markers (used to indicate the input stream to be corrupted), which once processed by ImageMagick, would cause it to consume excessive amounts of memory and CPU time.

Red Hat would like to thank CERT-FI for reporting CVE-2012-0260. CERT-FI acknowledges Aleksis Kauppinen, Joonas Kuorilehto, Tuomas Parttimaa and Lasse Ylivainio of Codenomicon's CROSS project as the original reporters.

Bug Fix

BZ#804546

The fix for Red Hat Bugzilla bug 694922, provided by the RHSA-2012:0301 ImageMagick update, introduced a regression. Attempting to use the "convert" utility to convert a PostScript document could fail with a "/undefinedfilename" error. With this update, conversion works as expected.

Users of ImageMagick are advised to upgrade to these updated packages, which contain backported patches to correct these issues. All running instances of ImageMagick must be restarted for this update to take effect.

4.61. initscripts

4.61.1. RHBA-2012:1155 — initscripts bug fix update

Updated initscripts packages that fix a bug 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 Fix

BZ#845246

Previously, the kpartx utility was not called with the "-p p" option in the netfs init script. Consequently, inconsistent partition mappings occurred. This bug has been fixed and kpartx is now called as expected.

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

4.62. ipa-client

4.62.1. RHBA-2012:0684 — ipa-client bug fix update

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

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

Bug Fix

BZ#818313

If the client requested keys for encryption types that the server did not support, and the requested key was not returned, the ipa-getkeytab utility, and consequently the client enrollment, failed. With this update, the ipa-getkeytab utility has been modified to no longer fail if the key is not retrieved; a warning message is now displayed instead.

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

4.62.2. RHBA-2013:0019 — ipa-client bug fix update

Updated ipa-client packages that fixes two bugs are now available for Red Hat Enterprise Linux 5.

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

Bug Fixes

BZ#813387

During the installation, the ipa-client-install utility created a zero-length /etc/sysconfig/network file. Consequently, the information about the network configuration was not specified. The underlying source code has been modified and the installation process no longer erases the configuration file.

BZ#816693

If the client requested keys for encryption types that the server did not support, and the requested key was not returned, the ipa-getkeytab utility, and consequently the client enrollment, failed. With this update, the ipa-getkeytab utility has been modified to no longer fail if the key is not retrieved; a warning message is now displayed instead.

All users of ipa-client are advised to upgrade to these updated packages, which fix these bugs.

4.63. iproute

4.63.1. RHBA-2012:1153 — iproute bug fix update

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

The iproute packages provide networking utilities like ip and rtmon, which use the advanced networking capabilities of the Linux kernel.

Bug Fix

BZ#738965

Prior to this update, the print_route() could, udner circumstances use the wrong "hz" value. As a consequence, the "ip route show" option returned an incorrect value for rto_min (minimum TCP retransmission timeout). This update modifies the underlying code to identify the different "hz" values. Now, the correct rto_min value is displayed.

BZ#751285

Prior to this update, the tc command-line utility generated a wrong filter match for the IPv6 "priority", the resulting match did not reflect the IPv6 header field proper. This update modifies the underlying code to match the IPv6 "Priority" header as expected.

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

4.64. iprutils

4.64.1. RHBA-2013:0034 — iprutils bug fix and enhancement update

Updated iprutils packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The iprutils packages provide a suite of utilities to manage and configure SCSI devices that are supported by the IBM Power RAID SCSI storage device driver.

Note

The iprutils packages have been upgraded to upstream version 2.3.11, which provides a number of bug fixes and enhancements over the previous version. (BZ#795953)

Bug Fixes

BZ#750702

Prior to this update, the iprutils suite did not correctly compute the size of the serial number. As a consequence, the attempt to delete arrays could fail. This update modifies the serial number comparison and increases the buffer size for new adapter configuration data.

BZ#843639

Prior to this update, iprconfig tool failed to delete RAID arrays. This update modifies the underlying code by sending the "START_STOP_STOP" executible before deleting the device. Now, RAID arrays are deleted as expected.

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

4.65. ipsec-tools

4.65.1. RHBA-2012:1249 — ipsec-tools bug fix update

Updated ipsec-tools packages that fix two bugs is now available for Red Hat Enterprise Linux 5.

The ipsec-tools packages contain configuration and management tools for the IPsec protocol.

Bug Fixes

BZ#852735

Under certain circumstances, the racoon daemon terminated unexpectedly due to referencing a NULL pointer when writing to the system log. The update ensures that the NULL pointer is never referenced by racoon in this scenario, thus fixing this bug.

BZ#852734

When using the setkey command to dump the pfkey database, the setkey command could decrease the size of a kernel buffer that is used to send the data. Consequently, the dumped database was incomplete and the operation failed with an error in the recv() function. With this update, setkey never decreases the kernel buffer size, thus preventing this bug.

All users of ipsec-tools are advised to upgrade to these updated package, which fix these bugs.

4.66. iptables

4.66.1. RHEA-2012:1415 — iptables enhancement update

Updated iptables packages that add an enhancement are now available for Red Hat Enterprise Linux 5.

The iptables utility controls the network packet filtering code in the Linux kernel.

Enhancement

BZ#847729

A new iptables module has been added that allows to configure the Differentiated Services Code Point (DSCP) match extension for the IPv6 protocol.

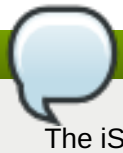
Users are advised to upgrade to these updated iptables packages, which add this enhancement.

4.67. iscsi-initiator-utils

4.67.1. RHBA-2013:0092 — iscsi-initiator-utils bug fix and enhancement update

Updated iscsi-initiator-utils packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The iscsi-initiator-utils packages provide the server daemon for the Internet Small Computer System Interface (iSCSI) protocol, as well as the utility programs used to manage it. iSCSI is a protocol for distributed disk access using SCSI commands sent over Internet Protocol (IP) networks.



Note

The iSCSI user-space driver, iscsiuio, has been upgraded to upstream version 0.7.4.3, which provides a number of bug fixes and enhancements over the previous version. In particular, VLAN and routing support. (BZ#796836)

Bug Fix

BZ#849661

The source RPM package for the iSCSI user-space driver, iscsiuio, did not include the NEW and AUTHORS files as required by the GNU packaging guidelines, and did not set the automake foreign option. The iscsiuio autoconf script uses libtool macros, but libtool was not specified as a build requirement in the RPM spec file. Consequently, attempting to rebuild the source RPM package in an environment with automake installed failed. Attempting to rebuild the source RPM package in an environment with autoconf installed, but without libtool, failed. The iscsiuio source has been updated to set the foreign automake option, in order to disable strict enforcing of the GNU packaging guidelines. In addition, libtool has been added as a build requirement for iscsi-initiator-utils, so that the required autoconf macros are available at build time. As a result, the iscsi-initiator-utils package can be built from the source RPM in a build environment that has automake and autoconf installed.

Enhancement

BZ#798178

Some iSCSI offload hardware requires the network interface to be "up" to function properly. Previously, this required additional network configuration steps before starting iSCSI. With this update, when the iSCSI daemon (iscsid) is starting an offloaded iSCSI session, the operational state of the associated network interface is now checked. The network interface is brought into an administrative up state automatically if needed. Offloaded iSCSI sessions can now be established without manually configuring the network interface first, iscsid will bring the interface up if needed.

All users of iscsi-initiator-utils are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.68. java-1.6.0-openjdk

4.68.1. RHBA-2013:0099 — java-1.6.0-openjdk bug fix update

Updated java-1.6.0-openjdk packages that fix various bugs are now available for Red Hat Enterprise Linux 5.

The java-1.6.0-openjdk packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Java Software Development Kit.

Bug Fixes

BZ#729502

Previously, the CCacheInputStream class could not to read Kerberos ticket cache files as it failed to handle the configuration settings stored in the ticket cache file under a special principal name. The configuration credentials are now ignored and the ticket cache is parsed correctly. Also, the initial context token generated by the GSSAPI/SPNEGO plug-in was previously rejected by the MIT Kerberos library due to incorrect data type of the reqFlags and NegTokenInit fields. The fields now use the correct data types.

BZ#808293

A JStack exception was thrown when a program was trying to capture both java and native stacktrace (mixed mode). Safety checks have been added and the problem no longer occurs.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which fix these bugs.

4.68.2. RHSA-2012:0730 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2012-1711, CVE-2012-1719

Multiple flaws were discovered in the CORBA (Common Object Request Broker Architecture) implementation in Java. A malicious Java application or applet could use these flaws to bypass Java sandbox restrictions or modify immutable object data.

CVE-2012-1716

It was discovered that the SynthLookAndFeel class from Swing did not properly prevent access to certain UI elements from outside the current application context. A malicious Java application or applet could use this flaw to crash the Java Virtual Machine, or bypass Java sandbox restrictions.

CVE-2012-1713

Multiple flaws were discovered in the font manager's layout lookup implementation. A specially-crafted font file could cause the Java Virtual Machine to crash or, possibly, execute arbitrary code with the privileges of the user running the virtual machine.

CVE-2012-1723, CVE-2012-1725

Multiple flaws were found in the way the Java HotSpot Virtual Machine verified the bytecode of the class file to be executed. A specially-crafted Java application or applet could use these flaws to crash the Java Virtual Machine, or bypass Java sandbox restrictions.

CVE-2012-1724

It was discovered that the Java XML parser did not properly handle certain XML documents. An attacker able to make a Java application parse a specially-crafted XML file could use this flaw to make the XML parser enter an infinite loop.

CVE-2012-1718

It was discovered that the Java security classes did not properly handle Certificate Revocation Lists (CRL). CRL containing entries with duplicate certificate serial numbers could have been ignored.

CVE-2012-1717

It was discovered that various classes of the Java Runtime library could create temporary files with insecure permissions. A local attacker could use this flaw to gain access to the content of such temporary files.

This erratum also upgrades the OpenJDK package to IcedTea6 1.10.8. 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.

4.68.3. RHSA-2012:1222 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2012-1682

It was discovered that the Beans component in OpenJDK did not perform permission checks properly. An untrusted Java application or applet could use this flaw to use classes from restricted packages, allowing it to bypass Java sandbox restrictions.

CVE-2012-0547

A hardening fix was applied to the AWT component in OpenJDK, removing functionality from the restricted SunToolkit class that was used in combination with other flaws to bypass Java sandbox restrictions.

This erratum also upgrades the OpenJDK package to IcedTea6 1.10.9. Refer to the NEWS file 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.

4.68.4. RHSA-2012:1385 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Software Development Kit.

Security Fixes

CVE-2012-5086, **CVE-2012-5084**, **CVE-2012-5089**

Multiple improper permission check issues were discovered in the Beans, Swing, and JMX components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2012-5068, **CVE-2012-5071**, **CVE-2012-5069**, **CVE-2012-5073**, **CVE-2012-5072**

Multiple improper permission check issues were discovered in the Scripting, JMX, Concurrency, Libraries, and Security components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass certain Java sandbox restrictions.

CVE-2012-5079

It was discovered that java.util.ServiceLoader could create an instance of an incompatible class while performing provider lookup. An untrusted Java application or applet could use this flaw to bypass certain Java sandbox restrictions.

CVE-2012-5081

It was discovered that the Java Secure Socket Extension (JSSE) SSL/TLS implementation did not properly handle handshake records containing an overly large data length value. An unauthenticated, remote attacker could possibly use this flaw to cause an SSL/TLS server to terminate with an exception.

CVE-2012-5075

It was discovered that the JMX component in OpenJDK could perform certain actions in an insecure manner. An untrusted Java application or applet could possibly use this flaw to disclose sensitive information.

CVE-2012-4416

A bug in the Java HotSpot Virtual Machine optimization code could cause it to not perform array initialization in certain cases. An untrusted Java application or applet could use this flaw to disclose portions of the virtual machine's memory.

CVE-2012-5077

It was discovered that the SecureRandom class did not properly protect against the creation of multiple seeders. An untrusted Java application or applet could possibly use this flaw to disclose sensitive information.

CVE-2012-3216

It was discovered that the java.io.FilePermission class exposed the hash code of the canonicalized path name. An untrusted Java application or applet could possibly use this flaw to determine certain system paths, such as the current working directory.

CVE-2012-5085

This update disables Gopher protocol support in the java.net package by default. Gopher support can be enabled by setting the newly introduced property, "jdk.net.registerGopherProtocol", to true.

This erratum also upgrades the OpenJDK package to IcedTea6 1.10.10. 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.

4.69. flash-plugin

4.69.1. RHSA-2012:1569 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2012-5676, **CVE-2012-5677**, **CVE-2012-5678**

This update fixes three vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB12-27. 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 11.2.202.258.

4.69.2. RHSA-2012:1431 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2012-5274, **CVE-2012-5275**, **CVE-2012-5276**, **CVE-2012-5277**, **CVE-2012-5278**, **CVE-2012-5279**, **CVE-2012-5280**

This update fixes several vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB12-24. 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 11.2.202.251.

4.69.3. RHSA-2012:1346 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2012-5248, **CVE-2012-5249**, **CVE-2012-5250**, **CVE-2012-5251**, **CVE-2012-5252**, **CVE-2012-5253**, **CVE-2012-5254**, **CVE-2012-5255**, **CVE-2012-5256**, **CVE-2012-5257**, **CVE-2012-5258**, **CVE-2012-5259**, **CVE-2012-5260**, **CVE-2012-5261**, **CVE-2012-5262**, **CVE-2012-5263**, **CVE-2012-5264**, **CVE-2012-5265**, **CVE-2012-5266**, **CVE-2012-5267**, **CVE-2012-5268**, **CVE-2012-5269**, **CVE-2012-5270**, **CVE-2012-5271**, **CVE-2012-5272**

This update fixes several vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed on the Adobe security page APSB12-22. 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 11.2.202.243.

4.69.4. RHSA-2012:1203 — 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 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fixes

CVE-2012-1535, **CVE-2012-4163**, **CVE-2012-4164**, **CVE-2012-4165**, **CVE-2012-4166**, **CVE-2012-4167**

This update fixes several vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed on the Adobe security pages APSB12-18 and APSB12-19. 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-2012-4168

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.

Note: This erratum upgrades Adobe Flash Player from version 10.3.183.20 to version 11.2.202.238.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.238.

4.69.5. RHSA-2012:0722 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fixes

CVE-2012-2034, **CVE-2012-2035**, **CVE-2012-2036**, **CVE-2012-2037**, **CVE-2012-2039**

This update fixes several vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed on the Adobe security page APSB12-14.

Several security flaws were found in the way flash-plugin displayed certain SWF content. An attacker could use these flaws to create a specially-crafted SWF file that would cause flash-plugin to crash or, potentially, execute arbitrary code when the victim loaded a page containing the specially-crafted SWF content.

CVE-2012-2038

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 10.3.183.20.

4.69.6. RHSA-2012:0688 — 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 for each vulnerability from the CVE link(s) associated with each description below.

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fixes

CVE-2012-0779

This update fixes one vulnerability in Adobe Flash Player. This vulnerability is detailed on the Adobe security page APSB12-09, listed in associated with each description below. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the specially-crafted SWF content.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 10.3.183.19.

4.69.7. RHSA-2012:0434 — 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 for each vulnerability from the CVE link(s) associated with each description below.

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2012-0773

This update fixes one vulnerability in Adobe Flash Player. This vulnerability is detailed on the Adobe security page APSB12-07, listed in associated with each description below. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the specially-crafted SWF content.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 10.3.183.18.

4.69.8. RHSA-2012:0359 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fixes

CVE-2012-0768

This update fixes two vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed on the Adobe security page APSB12-05.

A flaw was found in the way flash-plugin displayed certain SWF content. An attacker could use this flaw to create a specially-crafted SWF file that would cause flash-plugin to crash or, potentially, execute arbitrary code when the victim loaded a page containing the specially-crafted SWF content

CVE-2012-0769

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 10.3.183.16.

4.70. java-1.4.2-ibm

4.70.1. RHSA-2012:1485 — Critical: java-1.4.2-ibm security update

Updated java-1.4.2-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 Supplementary. This is the last update of these packages for Red Hat Enterprise Linux 5 Supplementary.

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

IBM J2SE version 1.4.2 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

CVE-2012-1531, **CVE-2012-3216**, **CVE-2012-4820**, **CVE-2012-4822**, **CVE-2012-5073**, **CVE-2012-5079**, **CVE-2012-5081**, **CVE-2012-5083**, **CVE-2012-5084**

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.

This is the last update of the java-1.4.2-ibm packages in Red Hat Enterprise Linux 5 Supplementary. Customers are advised to migrate to later versions of Java at this time. More current versions of IBM Java SE continue to be available via the Red Hat Enterprise Linux 5 Supplementary channel. Customers should also

consider OpenJDK which is the default Java development and runtime environment in Red Hat Enterprise Linux. In cases where it is not feasible to move to a later version of supported Java, customers are advised to contact IBM to evaluate other options.

All users of java-1.4.2-ibm are advised to upgrade to these updated packages, which contain the IBM J2SE 1.4.2 SR13-FP14 release. All running instances of IBM Java must be restarted for this update to take effect

4.70.2. RHSA-2012:1243 — Critical: java-1.4.2-ibm security update

Updated java-1.4.2-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 Supplementary.

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

IBM J2SE version 1.4.2 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

CVE-2012-1713, CVE-2012-1717, CVE-2012-1718, CVE-2012-1719

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-1.4.2-ibm are advised to upgrade to these updated packages, which contain the IBM J2SE 1.4.2 SR13-FP13 release. All running instances of IBM Java must be restarted for this update to take effect.

4.70.3. RHSA-2012:0702 — Critical: java-1.4.2-ibm security update

Updated java-1.4.2-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 Supplementary.

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

The IBM Java SE version 1.4.2 release includes the IBM Java 1.4.2 Runtime Environment and the IBM Java 1.4.2 Software Development Kit.

Security Fix

CVE-2011-3563, CVE-2012-0499, CVE-2012-0502, CVE-2012-0503, CVE-2012-0505, CVE-2012-0506

This update fixes several vulnerabilities in the IBM Java 1.4.2 Runtime Environment and the IBM Java 1.4.2 Software Development Kit. Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.4.2-ibm are advised to upgrade to these updated packages, which contain the IBM Java 1.4.2 SR13-FP12 release. All running instances of IBM Java must be restarted for this update to take effect.

4.71. java-1.5.0-ibm

4.71.1. RHSA-2012:1465 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) 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-2012-1531, **CVE-2012-3143**, **CVE-2012-3216**, **CVE-2012-4820**, **CVE-2012-4822**, **CVE-2012-5069**, **CVE-2012-5071**, **CVE-2012-5073**, **CVE-2012-5075**, **CVE-2012-5079**, **CVE-2012-5081**, **CVE-2012-5083**, **CVE-2012-5084**, **CVE-2012-5089**

This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. 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 SR15 release. All running instances of IBM Java must be restarted for this update to take effect.

4.71.2. RHSA-2012:1245 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) 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-2012-1713, **CVE-2012-1716**, **CVE-2012-1717**, **CVE-2012-1718**, **CVE-2012-1719**, **CVE-2012-1725**

This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. 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 SR14 release. All running instances of IBM Java must be restarted for this update to take effect.

4.71.3. RHSA-2012:0508 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The IBM 1.5.0 Java release includes the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit.

Security Fix

CVE-2011-3389, CVE-2011-3557, CVE-2011-3560, CVE-2011-3563, CVE-2012-0498, CVE-2012-0499, CVE-2012-0501, CVE-2012-0502, CVE-2012-0503, CVE-2012-0505, CVE-2012-0506, CVE-2012-0507

This update fixes several vulnerabilities in the IBM Java 2 Runtime Environment and the IBM Java 2 Software Development Kit. 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 1.5.0 SR13-FP1 Java release. All running instances of IBM Java must be restarted for this update to take effect.

4.72. java-1.6.0-ibm

4.72.1. RHSA-2012:1466 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) 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-2012-0547, CVE-2012-1531, CVE-2012-1532, CVE-2012-1533, CVE-2012-1682, CVE-2012-3143, CVE-2012-3159, CVE-2012-3216, CVE-2012-4820, CVE-2012-4822, CVE-2012-4823, CVE-2012-5068, CVE-2012-5069, CVE-2012-5071, CVE-2012-5072, CVE-2012-5073, CVE-2012-5075, CVE-2012-5079, CVE-2012-5081, CVE-2012-5083, CVE-2012-5084, CVE-2012-5089

This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. 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 SR12 release. All running instances of IBM Java must be restarted for the update to take effect.

4.72.2. RHSA-2012:1238 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) 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-2012-0551, CVE-2012-1713, CVE-2012-1716, CVE-2012-1717, CVE-2012-1718, CVE-2012-1719, CVE-2012-1721, CVE-2012-1722, CVE-2012-1725

This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. 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 SR11 release. All running instances of IBM Java must be restarted for the update to take effect.

4.72.3. RHSA-2012:0514 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The IBM Java SE version 6 release includes the IBM Java 6 Runtime Environment and the IBM Java 6 Software Development Kit.

Security Fix

CVE-2011-3563, CVE-2011-5035, CVE-2012-0497, CVE-2012-0498, CVE-2012-0499, CVE-2012-0500, CVE-2012-0501, CVE-2012-0502, CVE-2012-0503, CVE-2012-0505, CVE-2012-0506, CVE-2012-0507

This update fixes several vulnerabilities in the IBM Java 6 Runtime Environment and the IBM Java 6 Software Development Kit. 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 6 SR10-FP1 release. All running instances of IBM Java must be restarted for the update to take effect.

4.73. java-1.6.0-sun

4.73.1. RHBA-2013:0116 — java-1.6.0-sun bug fix update

Updated java-1.6.0-sun packages that fix one bug are now available for Red Hat Enterprise Linux 5.

Oracle Java SE version 6 includes the Oracle Java Runtime Environment and the Oracle Java Software Development Kit.

Bug Fix

BZ#868174

Prior to this update, the java-1.6.0-sun-plugin package did not contain an architecture-specific dependency on the java-1.6.0-sun package. Consequently, an error occurred during package unpacking when installation was done in a specific sequence. With this update the dependency has been added, and the aforementioned error no longer occurs.

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which fix this bug.

4.73.2. RHSA-2012:1392 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) 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-2012-0547, CVE-2012-1531, CVE-2012-1532, CVE-2012-1533, CVE-2012-3143, CVE-2012-3159, CVE-2012-3216, CVE-2012-4416, CVE-2012-5068, CVE-2012-5069, CVE-2012-5071, CVE-2012-5072, CVE-2012-5073, CVE-2012-5075, CVE-2012-5077, CVE-2012-5079, CVE-2012-5081, CVE-2012-5083, CVE-2012-5084, CVE-2012-5085, CVE-2012-5086, CVE-2012-5089

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 and Oracle Security Alert pages.

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which provide Oracle Java 6 Update 37. All running instances of Oracle Java must be restarted for the update to take effect.

4.73.3. RHSA-2012:0734 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The Sun 1.6.0 Java release includes the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit.

Security Fix

CVE-2012-0551, CVE-2012-1711, CVE-2012-1713, CVE-2012-1716, CVE-2012-1717, CVE-2012-1718, CVE-2012-1719, CVE-2012-1721, CVE-2012-1722, CVE-2012-1723, CVE-2012-1724, CVE-2012-1725

This update fixes several vulnerabilities in the Sun Java 6 Runtime Environment and the Sun Java 6 Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch page.

All users of java-1.6.0-sun are advised to upgrade to these updated packages, which provide JDK and JRE 6 Update 33 and resolve these issues. All running instances of Sun Java must be restarted for the update to take effect.

4.74. jpackage-utils

4.74.1. RHBA-2013:0115 — jpackage-utils bug fix update

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

The jpackage-utils package installs directory structures, RPM macros, configuration files, and scripts that provide support for jpackage.org Java packaging. It is required by all packages that follow the JPackage conventions.

Bug Fix

BZ#865102

Previously, jpackage-utils did not install java-1.7.0 directories in the /usr/share/ and /usr/lib/ directories. This caused failures when running the build-classpath script with Java 7 set as the javac alternative. These directories are now created and the build-classpath script works as expected with Java 7.

All users of jpackage-utils should upgrade to these updated packages that fix this bug.

4.75. kbd

4.75.1. RHBA-2013:0015 — kbd bugfix update

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

The kbd packages provide tools for managing console behavior on a Linux system, including the keyboard, screen fonts, virtual terminals and font files.

Bug Fix

BZ#622981

Prior to this update, the "bin/unicode_start" script was called twice. As a consequence, "unicode_start" with environment variables set to "BASH_ENV=~/.bashrc" and "TERM=linux" could enter an infinite loop. This update modifies the "/etc/unicode_start" init script so that "unicode_start" is now called once and no longer causes a loop.

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

4.76. kdebase

4.76.1. RHBA-2012:1177 — kdebase bug fix update

Updated kdebase packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

The K Desktop Environment (KDE) is a graphical desktop environment for the X Window System. The kdebase packages include core applications for the K Desktop Environment.

Bug Fixes

BZ#500399

If multiple users were using a KDE desktop on the same machine (for example by using the XDMCP protocol), only one user was able to lock the desktop. A patch has been applied to address this problem, and all users can now lock their desktops in the described scenario.

BZ#663638

Previously, the kdebase package did not honor mount options set in the HAL configuration files. This update corrects the problem, so that kdebase honors these mount options.

BZ#669354

On 64-bit systems, if the user changed time backwards, the KWin window manager incorrectly detected applications as not responding. This was due to a timestamp problem, which has been corrected, and KWIN no longer incorrectly reports applications as not responding.

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

4.77. kernel

4.77.1. RHSA-2013:1166 — Important: kernel security and bug fix update

Updated *kernel* packages that fix several security issues and bugs are now available for Red Hat Enterprise Linux 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

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-2013-2147, CVE-2013-2164, CVE-2013-2234, CVE-2013-2237, Low

Information leak flaws in the Linux kernel could allow a privileged, local user to leak kernel memory to user-space.

Bug Fixes

BZ#948187

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#972583

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#976441

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#979920

Due to a segment register that was not reset after a 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 KVM. Guest machines no longer hang on boot and the booting process is now significantly faster when using 64-bit Intel hardware with the VT feature enabled.

BZ#980811

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#983452

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#983628

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#987976

A 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 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.

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.

4.77.2. 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 the descriptions 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.

Bug Fixes

BZ#884702

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#884708

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#884740

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#884742

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#885062

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#885692

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#885700

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#886124

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#886876

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.

All 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.

4.77.3. RHBA-2013:0006 — Red Hat Enterprise Linux 5.9 kernel update

Updated *kernel* packages that fix several hundred bugs and add numerous enhancements are now available as part of the ongoing support and maintenance of Red Hat Enterprise Linux version 5. This is the ninth regular update.

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

Bug Fixes

BZ#563247

Under memory pressure, memory pages that are still a part of a checkpointing transaction can be invalidated. However, when the pages were invalidated, the journal head was re-filed onto the transactions' forget list, which caused the current running transaction's block to be modified. As a result, block accounting was not properly performed on that modified block because it appeared to have already been modified due to the journal head being re-filed. This could trigger an assertion failure in the "journal_commit_transaction()" function on the system. With this update, the "b_modified" flag is cleared before the journal head is filed onto any transaction, and assertion failures no longer occur.

BZ#862811

On certain platforms, the be2net driver could incorrectly indicate UE bits and stop further access to be2net-based network interface cards (NICs). With this update, these UE bits are ignored and if a real UE occurs, the corresponding hardware block will automatically go offline and stop the traffic.

BZ#857448

Previously, two threads could race to automount the same Distributed File System (DFS) share. The second thread called the do_add_mount() function after the first thread had completed the automount, and received a reference to the existing vfs_mount inserted by the first thread. Consequently, the new vfs_mount created by this thread for the mount process was dropped. This resulted in the use count for the dentry pointed to by vfs_mount to drop to -1 and the system terminated with a kernel panic. The underlying source code has been modified, and a kernel panic no longer occurs under these circumstances.

BZ#854067

A bug in the ipvs code caused insufficient performance of the Transmission Control Protocol (TCP) when generic receive offload (GRO) or generic segmentation offload (GSO) was enabled on a machine running the IP Virtual Server (IPVS) or Linux Virtual Server (LVS). The TCP connection continued to work, however, only by retransmitting all data, as only TCP segments with a single packet were allowed to go through. This update allows reception of GRO-aggregated packet buffers, through the IPVS framework. On transmission the GSO-aggregated packet buffer is automatically deaggregated by GSO. Use of GSO/GRO together with this update will result in an improved throughput and lower CPU utilization.

BZ#852526

Prior to this update, a process of continuously opening and closing a file within a second could prevent the data cache of a file from ever expiring. This resulted in stale data being presented on the client. With this update, the modify time and size stored in cache for an existing inode are compared with the modify time and size returned by the open() call; the cache is invalidated if the values differ.

BZ#850977

To resolve a kernel panic that occurred under certain circumstances, an upstream cleanup patch for VFS automount support was backported to Red Hat Enterprise Linux 5, which also fixed the panic. This upstream change occurred after the VFS automount support was added to Red Hat Enterprise Linux 5 so was not present.

BZ#840642

An unnecessary check for the RXCW.CW bit could cause the Intel e1000e NIC (Network Interface Controller) to not work properly. The check has been removed so that the Intel e1000e NIC now works as expected.

BZ#839753

When attempting to mount a NFS share twice on the same mount point, a check in the do_add_mount() function causes an error to be returned. However, when using the "noac" option, the user was abe to mount the same share on the same mount point multiple times. This was because the "noac" option was automatically assigned the MS_SYNCHRONOUS flag in the nfs_initialise_sb() function. This flag was set after the check for already existing superblocks had been performed in the sget() function, and was therefore not taken into account during the check of mount flags. This update checks for the "noac" option and assigns the MS_SYNCHRONOUS fag before sget() is called to obtain an already existing superblock structure. As a result, it is no longer possible to mount a NFS share on the same location multiple times.

BZ#836244

Failures and errors could occur due to a NULL pointer dereference in the vm_enough_memory() function. To prevent such problems, the NULL checking has been revised

BZ#835660

Previously, if a command timed out to a device with a reservation conflict, the SCSI error handling marked the device as offline. This was because the RESERVATION_CONFLICT return code was treated as a fatal error when a TUR command was sent to confirm that the device was reachable and responding. Consequently, the error handling progressed to the next error routine, eventually marking the device offline. The error processing in the scsi_eh_completed_normally() function has been changed to consider RESERVATION_CONFLICT for a TUR command as success. This causes the scsi_eh_tur() call to pass successfully, and the devices are no longer set as offline.

BZ#834562

An insufficiently designed calculation in the CPU accelerator in the previous kernel caused an arithmetic overflow in the sched_clock() function when system uptime exceeded 208.5 days. This overflow led to a kernel panic on systems using the Time Stamp Counter (TSC) or Virtual Machine Interface (VMI) clock source. This update corrects the aforementioned calculation so that this arithmetic overflow and kernel panic can no longer occur under these circumstances.

BZ#746122

The way how the kernel processes dentries in the dcache when unmounting file systems allowed the concurrent activity on the list of dentries. If the list was large enough, the kernel could, under certain circumstances, panic due to NMI watchdog timeout triggered by the waiting concurrent process. This update modifies underlying functions to use a private dcache list for certain operations on the dcache so that concurrent activities are no longer affected in this scenario.

BZ#834379

When two processes attempted to automount an NFS file system at the same time, an account usage error occurred in the dentry of the mount point, leading to EBUSY errors when trying to unmount the file system. In addition, a kernel panic could occur when the automount timeout expired or the shutdown procedure tried to unmount the file system. This was because the vfsmount structure was missing a reference of the mount point. This update ensures that a reference of the mount point is placed on the vfsmount structure before the do_add_mount() function is called. The NFS file system can now be unmounted as expected, and the kernel panic no longer occurs in this scenario.

BZ#833000

Previously, the SAS-2 tape drive was not detected after connecting it to a SATA/SAS Storage Control Unit (SCU) port. This was because the speed values in the isci driver were not updated and the negotiated connection speed for the SAS-2 device was therefore incorrect. With this update, the PHY_LINKRATE values defined in the scsi_transport_sas header file are now used, which ensures correct detection of SAS-2 devices.

BZ#822166

A race condition between a device being opened and the device being disconnected occurred in the evdev code. During this condition, the evdev structure for a device continued to be used after it had been freed. If the memory was reallocated afterward and zeroed by the new owner, the evdev_open() function could become stuck and generate a soft lockup. This update directly uses a kref structure to implement proper reference counting, which prevents the race condition from occurring in this scenario.

BZ#819830

Previously, when listing of IPv6 routing table was prematurely ended, it could cause corruption of that table, leading to various problems, including a kernel panic. To prevent the problems, the routing table is now traversed correctly.

BZ#818787

An insufficiently designed calculation in the CPU accelerator in the previous kernel caused an arithmetic overflow in the sched_clock() function when system uptime exceeded 208.5 days. This overflow led to a kernel panic on the systems using the Time Stamp Counter (TSC) or Virtual Machine Interface (VMI) clock source. This update corrects the calculation so that this arithmetic overflow and kernel panic can no longer occur under these circumstances. Note: This advisory does not include a fix for this bug for the 32-bit architecture

BZ#753244

The function that used to find a resource block (rsb) during directory recovery was searching the rsb's single linear list, which took an excessive amount of time. Consequently, recovery of Distributed Lock Manager (DLM) could take a long time. With this update, the standard hash table is used to find the rsb, which decreases the search time, and DLM recovery finishes in a reasonable time.

BZ#749813

If the IP stack proper is accessed from bridge netfilter, the socket buffer needs to be in a form the IP stack expects. Previously, the entry point on the NF_FORWARD hook did not meet the requirements of the IP stack. Consequently, hosts could terminate unexpectedly. A backported upstream patch has been provided to address this issue and the crashes no longer occur in the described scenario.

BZ#814626

The kernel version 2.6.18-308.4.1.el5 contained several bugs which led to an overrun of the NFS server page array. Consequently, any attempt to connect an NFS client running on Red Hat Enterprise Linux 5.8 to the NFS server running on the system with this kernel caused the NFS server to terminate unexpectedly and the kernel to panic. This update corrects the bugs causing NFS page array overruns and the kernel no longer crashes in this scenario.

BZ#809937

A process scheduler did not handle RPC priority wait queues correctly. Consequently, the process scheduler failed to wake up all scheduled tasks as expected after RPC timeout, which caused the system to become unresponsive and could significantly decrease system performance. This update modifies the process scheduler to handle RPC priority wait queues as expected. All scheduled tasks are now properly woken up after RPC timeout and the system behaves as expected.

BZ#756506

A kernel panic occurred when the size of a block device was changed and I/O was issued at the same time. This was because the direct and non-direct I/O code was written with the assumption that the block size would not change. This update introduces a new read-write lock, bd_block_size_semaphore. The lock is taken for read during I/O and for write when changing block size. As a result, block size cannot be changed while I/O is being submitted. This prevents the kernel from crashing in the described scenario.

BZ#808489

Previously, requests for large data blocks with the ZSECSENDCPRB ioctl() system call failed due to an invalid parameter. A misleading error code was returned, concealing the real problem. With this update, the parameter for the ZSECSENDCPRB request code constant is validated with the correct maximum value. Now, if the parameter length is not valid, the EINVAL error code is returned, thus fixing this bug.

BZ#805799

A bug in the vsyscall interface caused 32-bit multi-threaded programs, which received the SIGCANCEL signal right after they returned from a system call, to terminate unexpectedly with a segmentation fault when run on the AMD64 or Intel 64 architecture. A patch has been provided to address this issue and the crashes no longer occur in the described scenario.

BZ#804778

Previously, the restriction of the way epoll file descriptors could nest was overly aggressive. Consequently, certain applications were unable to add the desired number of epoll watches and

possibly terminated unexpectedly or became unresponsive. With this update, there is no restriction on the number of epoll file descriptors that can be attached to the source file descriptor, thus preventing the described problems. Note that if an application requests a deeply-nested epoll file descriptor, the request fails gracefully rather that causing the kernel to terminate unexpectedly.

BZ#800653

The qla2xxx driver set up interrupts for Qlogic 4Gb Fibre Channel adapters incorrectly due to a bug in a test condition for MSI-X support. This update corrects the bug and qla2xxx now sets up interrupts as expected.

BZ#800575

When a slave started up, the active flags failed to be marked inactive while unsetting the current_arp_slave parameter. Consequently, more than one slave with active flags in active-backup mode could be present on the system. With this update, the active flags are properly marked inactive from a slave before the current_arp_slave is unset, thus preventing this bug.

BZ#799530

When the Fibre Channel (FC) layer sets a device to "running", the layer also scans for other new devices. Previously, there was a race condition between these two operations. Consequently, for certain targets, thousands of invalid devices were created by the SCSI layer and the udev service. This update ensures that the FC layer always sets a device to "online" before scanning for others, thus fixing this bug. Additionally, when attempting to transition priority groups on a busy FC device, the multipath layer retried immediately. If this was the only available path, a large number of retry operations was performed in a short period of time. Consequently, the logging of retry messages slowed down the system. This bug has been fixed by ensuring that the DM Multipath feature delays retry operations in the described scenario.

BZ#799170

When the kvmclock initialization was used in a guest, it could write to the time stamp counter (TSC) and, under certain circumstances, could cause the kernel to become unresponsive on boot. With this update, TSC synchronization, which is unnecessary due to kvmclock, has been disabled, thus fixing this bug.

BZ#798048

The mlx4 driver did not contain the necessary callbacks to implement Enhanced I/O Error Handling and recovery, so the PCI layer used the probe and remove callbacks to try to recover the device after an error occurred on the bus. However, a race condition occurred between these callbacks and the internal catastrophic error recovery functions which also detected the error, and consequently caused a kernel oops if both EEH and the internal recovery functions attempted to reset the device. This update adds the necessary error recovery callbacks and ensures that the internal catastrophic error functions do not try to reset the device in such scenarios. Also, additional calls have been added to suppress read and write operations on the bus when the slot cannot accept I/O operations, which prevents unnecessary accesses to the bus and speeds up the device removal.

BZ#797011

Due to a regression, the ifdef macro was used with an invalid value. Consequently, the tg3 driver did not support VLAN tagging and the vconfig utility was unable to configure VLAN tagging properly, thus blocking the network connection. This update removes incorrect usages of ifdef from the code and the VLAN support now works as expected.

BZ#771366

When using the Intel e1000e ethernet driver, the RXCW register's invalid bit (IV) was being set periodically due to incorrect register read logic for the 82571 Serializer-Deserializer (SERDES), which resulted in link flapping. The read logic has been improved: RXCW is now read twice to filter one-time false events and obtain correct values for the IV bit. Link flaps no longer occur in this scenario.

BZ#795672

Certain Broadcom devices, mostly the BMC5704 controllers, failed to work due to incorrect TSO (TCP Segmentation Offload) handling in the tg3 driver. The TSO handling code has been revised so that the devices now work as expected.

BZ#772192

Due to a bug in the qla2xxx driver and the HBA firmware, storage I/O traffic could become unresponsive during storage fault testing. With this update, these bugs have been fixed and the hangs no longer happen in the described scenario.

BZ#772216

Previously, secondary, tertiary, and other IP addresses added to bond interfaces could overwrite the bond->master_ip and vlan_ip values. Consequently, a wrong IP address could be occasionally used, the MII (Media Independent Interface) status of the backup slave interface went down, and the bonding master interfaces were switching. This update removes the master_ip and vlan_ip elements from the bonding and vlan_entry structures, respectively. Instead, devices are directly queried for the optimal source IP address for ARP requests, thus fixing this bug.

BZ#790900

When running more than 30 instances of the cclengine utility concurrently on IBM System z with IBM Communications Controller for Linux, the system could become unresponsive. This was caused by a missing wake_up() function call in the qeth_release_buffer() function in the QETH network device driver. This update adds the missing wake_up() function call and the system now responds as expected in this scenario.

BZ#773022

Due to a bug in the error clean-up code, the kernel could fail to boot when a tg3 NIC utilized the 4 KB transmit segmentation code but could not map all the physical memory fragments. This update rectifies the situation so that the tg3 driver no longer prevents the kernel from booting.

BZ#773735

When using the be2net driver, if a card was reset due to EEH (Enhanced Error Handling), the error recovery involves ring clean-up and re-creation. However, because worker threads touch this ring, there was a race condition that caused kernel to terminate unexpectedly. With this update, a worker thread is stopped during this clean-up process, thus preventing this bug.

BZ#790840

The QDIO (Queued Direct I/O) data transfer architecture maintains a "buffers-used" counter for its hardware buffers. If the buffers were returned in the ERROR state, the counter was updated incorrectly when running under the z/VM operating system with the QIOASSIST flag switched on. Consequently, the buffer handling logic in QDIO was working incorrectly. This update fixes the code to update the counter correctly in the described scenario, thus fixing this bug.

BZ#782124

When a network interface card (NIC) with a fan experiences a fan failure, the PHY chip is usually powered down by its firmware. Previously, the bnx2x driver did not handle fan failures correctly,

which could trigger a non-maskable interrupt (NMI). Consequently, the kernel could crash or panic. This update modifies the bnx2x driver to handle fan failures properly, the NIC is now shut down as expected and the kernel does not crash in this scenario.

BZ#790103

A kernel panic could occur on IBM Power systems while running the fsfuzz test. This was caused by an attempt to perform an I/O operation on an unmapped buffer, which triggered a BUG_ON() function call. This update modifies the kernel so that I/O operations can be performed only on mapped buffers. The kernel no longer panics in this scenario.

BZ#782677

Due to recent changes in the tg3 driver, the driver attempted to use an already freed pointer to a socket buffer (SKB) when the NIC was recovering from unsuccessful memory mapping. Consequently, the NIC went offline and the kernel panicked. With this update, the SKB pointer is newly allocated in this scenario. The NIC recovers as expected and a kernel panic does not occur. Also, the tg3 driver could, under certain circumstances, attempt to unmap a memory fragment that had not been mapped. Consequently, the kernel panicked. This update fixes the bug by correcting the "last" parameter supplied.

BZ#782790

A recent change in the QLogic qla2xxx driver introduced a bug which could, under rare circumstances, cause the system to become unresponsive. This problem occurred during I/O error recovery on systems using SAN configurations with QLogic Fibre Channel Hot Bus Adapters (HBAs). This update corrects the qla2xxx driver so the system no longer hangs in this scenario.

BZ#788777

When SAS (Serial Attached SCSI) disks were present on the system and the CK_COND=1 parameter was set in the Command Descriptor Block (CDB), the SAT ATA PASS-THROUGH commands produced a large number of irrelevant warning messages, clogging up logs with useless information. With this update, the logging has been disabled in the described scenario, thus fixing this bug.

BZ#783043

An Ethernet physical transceiver (a PHY chip) was always powered up when a network interface card (NIC) using the igb driver was brought down. Recent changes had modified the kernel so that the PHY chip was powered down in such a scenario. With this PHY power saving feature, the PHY chip could unexpectedly lose its settings on rare occasions. Consequently, the PHY chip did not recover after the NIC had been re-attached and the NIC could not be brought up. The igb driver has been modified so that the PHY chip is now reset when the NIC is re-attached to the network. NICs using the igb driver are brought up as expected.

BZ#783540

Previously, a kernel panic could occur on IBM S/390 systems after a reboot. This happened due to a race condition between the raw3215_tasklet() and the tty3215_close() functions, which could result in calling the tty_wakeup() function with either a NULL pointer or with a pointer to an already freed tty structure. This update prevents the race condition by adding the tasklet_kill() function call to the tty3215_close() function. The kernel no longer panics when closing the 3215 console on IBM S/390 systems.

BZ#785062

In NFSv4, both write and open code paths depended on the I_LOCK flag in inode->i_state. In addition to this, the write code path also needs the latest stateid returned by open to before it can

proceed. It waits for this while holding the I_LOCK bit in inode->state. As a consequence, multi-threaded applications could be blocked when using NFSv4. With this update, the nfs_fhget() function has been modified to use the I_NEW flag for the open code path, thus fixing this bug.

BZ#789067

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. The only workaround is to reboot. The fix is common, when taking a spinlock, disable the interrupts too.

BZ#773777

When a single, large data stream was being written to an NFS server while other applications periodically wrote small amounts of data to a local file system, other applications could experience long pauses when dirty memory reaches the dirty_ratio limit. With this update, the code for COMMIT calls has been improved to not skip such calls if the system is under memory pressure and to allow high priority COMMIT calls to bypass inode commit locks. Now, the pauses in traffic no longer occur in the described scenario.

BZ#798809

The vfs-automount infrastructure assumes that the LOOKUP_DIRECTORY flag is included in nameidata flags if a trailing slash character (/) is given on a path being walked. But this flag is private to the __link_path_walk() function so it must be added when looking up the last component. Previously, during a path walk where the path included a trailing slash character, LOOKUP_DIRECTORY was not propagated to path walk functions. Consequently, directories that needed to trigger an automount failed to do so, which resulted in a -ENOTDIR error. This bug has been fixed and the error code is no longer returned in the described scenario.

BZ#804800

Starting with Red Hat Enterprise Linux 5.6, all devices that used the ixgbe driver would stop stripping VLAN tags when the device entered promiscuous mode. Placing a device in a bridge group causes the device to enter promiscuous mode. This caused various issues under certain configurations of bridging and VLANs. A patch has been provided to address this issue and the devices now properly strip VLAN tags in the driver whether in promiscuous mode or not.

BZ#848098

Previously, the code checking for a NULL pointer was incorrect; it checked for a non-NULL pointer instead. As a consequence, this could lead to a kernel panic. This update corrects the problem, so that the kernel no longer crashes in this scenario.

BZ#830226

Recent changes removing support for the Flow Director from the ixgbe driver introduced bugs that caused the RSS (Receive Side Scaling) functionality to stop working correctly on Intel 82599EB 10 Gigabit Ethernet network devices. This update corrects the return code in the ixgbe_cache_ring_fdir function and setting of the registers that control the RSS redirection table. Also, obsolete code related to Flow Director support has been removed. The RSS functionality now works as expected on these devices.

BZ#814418

If a path followed a symlink that ended with the slash ("/") character, the LOOKUP_DIRECTORY flag could be set earlier than the last path component. This led to an ENOTDIR (Not a directory) error. The LOOKUP_DIRECTORY flag is now propagated only for the last component. For the purpose of possible automounting, the flag is not needed for intermediate path components; the

LOOKUP_CONTINUE flag is set in such a case. The ENOTDIR error no longer occurs in this scenario.

BZ#839770

In the ext4 file system, splitting an unwritten extent while using Direct I/O could fail to mark the modified extent as dirty, resulting in multiple extents claiming to map the same block. This could lead to the kernel or fsck reporting errors due to multiply claimed blocks being detected in certain inodes. In the ext4_split_unwritten_extents() function used for Direct I/O, the buffer which contains the modified extent is now properly marked as dirty in all cases. Errors due to multiply claimed blocks in inodes should no longer occur for applications using Direct I/O.

BZ#830351

On ext4 file systems, when the fallocate() system call failed to allocate blocks due to the ENOSPC condition (no space left on device) for a file larger than 4 GB, the size of the file became corrupted and, consequently, caused file system corruption. This was due to a missing cast operator in the ext4_fallocate() function. With this update, the underlying source code has been modified to address this issue, and file system corruption no longer occurs.

BZ#756091

Calculations for sizing certain memory allocation thresholds (dcache, files-max, ...) depend on the number of physical pages found in a system; this generally includes (occasionally a large amount of) non-RAM pages. Due to a miscalculated number of usable RAM pages, memory allocation thresholds calculation on large systems with discontiguous memory (such as modern NUMA systems) could result in bad sizing. This could impact workload performance. With this update, the aforementioned calculation basis has been switched to what actually is usable as storage (RAM). The sizing of the memory allocation thresholds is now fixed and they render the expected values when they are verified.

BZ#852340

A kernel panic can occur when attempting to create a Fibre Channel over Ethernet (FCoE) session on a network interface controller (NIC) with a virtual LAN (VLAN) enabled. Software-based Fibre Channel over Ethernet (FCoE) is a Technology Preview in Red Hat Enterprise Linux 5, 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#858724

This update changes Xen hypervisor's behavior introduced in the CVE-2012-2934 issue: the host was prevented from booting on AMD processors with the AMD #121 erratum applied. Users were prompted to pass the "allow_unsafe" parameter on the command line to allow booting the Xen host However, this could prevent remotely managed hosts from being started. With this update, the boot process is no longer denied by default; only guest creation is denied. The allow_unsafe semantics has changed to allow creation of guests instead of allowing booting the host.

BZ#800708

Previously, the interrupt handlers of the qla2xxx driver could clear pending interrupts right after the IRQ lines were attached during system start-up. Consequently, the kernel could miss the interrupt that reported completion of the link initialization, and the qla2xxx driver then failed to detect all attached LUNs. With this update, the qla2xxx driver has been modified to no longer clear interrupt bits after attaching the IRQ lines. The driver now correctly detects all attached LUNs as expected.

BZ#782866

The Ethernet channel bonding driver reported the MII (Media Independent Interface) status of the bond interface in 802.3ad mode as being up even though the MII status of all of the slave devices was down. This could pose a problem if the MII status of the bond interface was used to determine if failover should occur. With this update, the agg_device_up() function has been added to the bonding driver, which allows the driver to report the link status of the bond interface correctly, that is, down when all of its slaves are down, in the 802.3ad mode.

BZ#712513

The kdump kernel maintains the configuration of MSI-X interrupts as created by the crashed kernel but enables only one CPU in the new environment. Previously, this caused the tg3 driver to abort MSI-X setup which caused interrupt delivery to fail. Consequently, the link became unavailable and any attempt to dump a core file to a remote host to failed. With this update, the tg3 driver has been modified to enforce single-vector MSI-X interrupt mode by disabling the multivector interrupt mode for tg3 in the kdump kernel. The NIC is now brought up as expected and kdump can successfully dump a core file to the remote host in this scenario.

BZ#683303

The bnx2x driver performed the initialization of hardware in a way that was unsafe if the previous instance of the driver terminated in an unclean manner. Consequently, the kernel could become unresponsive or panic while initializing the NIC in the kdump environment. With this update, the bnx2x driver has been modified to perform a safer initialization, solving the possible crash scenarios. The NIC is now initialized as expected and kdump can successfully dump a core file to a remote host when using the bnx2x driver.

BZ#845169

Previously, when Enhanced I/O Error Handling (EEH) detected an error while a firmware dump was being collected, a reset of the PCI adapter could have been triggered before the dumping operation could complete. As a consequence, the firmware dump was interrupted and recovery of the PCI adapter failed leaving the adapter in an inconsistent state. This update modifies the be2net driver to wait for the firmware dump to complete before resetting EEH. A core file is successfully dumped and the PCI adapter recovers as expected in this scenario.

BZ#842486

When bringing up a network interface with VLANs configured on top of it using the mlx4 driver, the kernel could panic due to a NULL pointer dereference. This was caused by the core networking code which called the VLAN addition routine before setting the VLAN device entry in the VLAN group table. This update modifies the mlx4 driver to prevent this behavior so that the VLAN device entry in now added to the VLAN group table before adding the VLAN and the kernel no longer panics in this scenario.

BZ#786403

Due to incorrect information provided by firmware, the netxen_nic driver did not calculate the correct Generic Segmentation Offload (GSO) length of packets that were received using the Large Receive Offload (LRO) optimization. This caused network traffic flow to be extensively delayed for the NICs using LRO on netxen_nic, which had a huge impact on NIC's performance (in some cases, throughput for some 1 GB NICs could be below 100 kbs). With this update, firmware now provides the correct GSO packet length and the netxen_nic driver has been modified to handle new information provided by firmware correctly. Throughput of the NICs using the LRO optimization with the netxen_nic driver is now within expected levels.

Enhancements

Note

For more information on the most important of the Red Hat Enterprise Linux 5.9 kernel enhancements, refer to the *Kernel* and *Device Drivers* chapters in the *Red Hat Enterprise Linux 5.9 Release Notes* on https://access.redhat.com/knowledge/docs/Red_Hat_Enterprise_Linux/.

BZ#872612

The INET socket interface has been modified to send a warning message when the ip_options structure is allocated directly by a third-party module using the kmalloc() function.

BZ#640206

With this update, NIC speed and duplex information are now exported through sysfs. This feature allows users to determine the state and status of the NIC and it's connections.

BZ#605727

This update modifies IPMI to support configurable timeouts and retry attempts for the keyboard controller-style (KCS) interface. Ability to configure timeouts and retry attempts ensures that no IPMI requests or responses are dropped due to the default limit of the KCS host driver, which increases reliability of communication over KCS.

BZ#790841

With this update, the mlx4 driver has been upgraded to the The OpenFabrics Alliance Enterprise Distribution (OFED) level 1.5.4.1 with the exception of the XRC support. Among other changes, the update includes support for IBoE, which is, however, disabled by default, and a fix for a bug related to the mlx4 multicast support.

All Red Hat Enterprise Linux 5 users are advised to install these updated packages, which correct these issues and add these enhancements. The system must be rebooted for this update to take effect.

4.77.4. RHBA-2012:0361 — kernel bug fix update

Updated kernel packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

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

Bug Fix

BZ#749246

The root user without the CAP_SYS_ADMIN capability was able to reset the contents of the "/proc/sys/kernel/dmesg_restrict" configuration file to 0. Consequently, the unprivileged root user could bypass the protection of the "dmesg_restrict" file and read the kernel ring buffer. This update ensures that only the root user with the CAP_SYS_ADMIN capability is allowed to write to the dmesg_restrict file. Any unauthorized attempt on writing to this file now fails with an EPERM error.

BZ#786168

An Ethernet physical transceiver (a PHY chip) was always powered up when a network interface card (NIC) using the igb driver was brought down. Recent changes had modified the kernel so that the PHY chip was powered down in such a scenario. With this PHY power saving feature, the PHY chip could unexpectedly lose its settings on rare occasions. Consequently, the PHY chip did not

recover after the NIC had been re-attached and the NIC could not be brought up. The igb driver has been modified so that the PHY chip is now reset when the NIC is re-attached to the network. NICs using the igb driver are brought up as expected.

BZ#789369

The way how the kernel processes dentries in the dcache when unmounting file systems allowed the concurrent activity on the list of dentries. If the list was large enough, the kernel could, under certain circumstances, panic due to NMI watchdog timeout triggered by the waiting concurrent process. This update modifies underlying functions to use a private dcache list for certain operations on the dcache so that concurrent activities are no longer affected in this scenario.

BZ#790778

The Abstract Control Model (ACM) driver uses spinlocks to protect the lists of USB Request Blocks (URBs) and read buffers maintained by the driver. Previously, when a USB device used the ACM interface, a race condition between scheduled ACM tasklets could occur. Consequently, the system could enter a deadlock situation because tasklets could take spinlocks without disabling interrupt requests (IRQs). This situation resulted in various types of soft lockups ending up with a kernel panic. This update fixes the problem so that IRQs are disabled when a spinlock is taken. Deadlocks no longer occur and the kernel no longer crashes in this scenario.

BZ#790907

A recent change in the QLogic qla2xxx driver introduced a bug which could, under rare circumstances, cause the system to become unresponsive. This problem occurred during I/O error recovery on systems using SAN configurations with QLogic Fibre Channel Hot Bus Adapters (HBAs). This update corrects the qla2xxx driver so the system no longer hangs in this scenario.

BZ#790910

Due to recent changes in the tg3 driver, the driver attempted to use an already freed pointer to a socket buffer (SKB) when the NIC was recovering from unsuccessful memory mapping. Consequently, the NIC went offline and the kernel panicked. With this update, the SKB pointer is newly allocated in this scenario. The NIC recovers as expected and a kernel panic does not occur. Also, the tg3 driver could, under certain circumstances, attempt to unmap a memory fragment that had not been mapped. Consequently, the kernel panicked. This update fixes the bug by correcting the "last" parameter supplied.

BZ#790912

When a network interface card (NIC) with a fan experiences a fan failure, the PHY chip is usually powered down by its firmware. Previously, the bnx2x driver did not handle fan failures correctly, which could trigger a non-maskable interrupt (NMI). Consequently, the kernel could crash or panic. This update modifies the bnx2x driver to handle fan failures properly, the NIC is now shut down as expected and the kernel does not crash in this scenario.

All users are advised to upgrade to these updated packages, which fix these bugs. The system must be rebooted for this update to take effect.

4.77.5. RHSA-2012:1061 — 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 for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fix

CVE-2012-3375, Moderate

The fix for CVE-2011-1083 (RHSA-2012:0150) introduced a flaw in the way the Linux kernel's Event Poll (epoll) subsystem handled resource clean up when an ELOOP error code was returned. A local, unprivileged user could use this flaw to cause a denial of service.

Bug Fixes

BZ#816373

The qla2xxx driver handled interrupts for QLogic Fibre Channel adapters incorrectly due to a bug in a test condition for MSI-X support. This update corrects the bug and qla2xxx now handles interrupts as expected.

BZ#817571

A process scheduler did not handle RPC priority wait queues correctly. Consequently, the process scheduler failed to wake up all scheduled tasks as expected after RPC timeout, which caused the system to become unresponsive and could significantly decrease system performance. This update modifies the process scheduler to handle RPC priority wait queues as expected. All scheduled tasks are now properly woken up after RPC timeout and the system behaves as expected.

BZ#820358

The kernel version 2.6.18-308.4.1.el5 contained several bugs which led to an overrun of the NFS server page array. Consequently, any attempt to connect an NFS client running on Red Hat Enterprise Linux 5.8 to the NFS server running on the system with this kernel caused the NFS server to terminate unexpectedly and the kernel to panic. This update corrects the bugs causing NFS page array overruns and the kernel no longer crashes in this scenario.

BZ#824654

An insufficiently designed calculation in the CPU accelerator in the previous kernel caused an arithmetic overflow in the sched_clock() function when system uptime exceeded 208.5 days. This overflow led to a kernel panic on the systems using the Time Stamp Counter (TSC) or Virtual Machine Interface (VMI) clock source. This update corrects the calculation so that this arithmetic overflow and kernel panic can no longer occur under these circumstances.

Note: This advisory does not include a fix for this bug for the 32-bit architecture.

BZ#827205

Under memory pressure, memory pages that are still a part of a checkpointing transaction can be invalidated. However, when the pages were invalidated, the journal head was re-filed onto the transactions' "forget" list, which caused the current running transaction's block to be modified. As a result, block accounting was not properly performed on that modified block because it appeared to have already been modified due to the journal head being re-filed. This could trigger an assertion failure in the "journal_commit_transaction()" function on the system. The "b_modified" flag is now cleared before the journal head is filed onto any transaction; assertion failures no longer occur.

BZ#829059

When running more than 30 instances of the cclengine utility concurrently on IBM System z with IBM Communications Controller for Linux, the system could become unresponsive. This was

caused by a missing wake_up() function call in the qeth_release_buffer() function in the QETH network device driver. This update adds the missing wake_up() function call and the system now responds as expected in this scenario.

BZ#832169

Recent changes removing support for the Flow Director from the ixgbe driver introduced bugs that caused the RSS (Receive Side Scaling) functionality to stop working correctly on Intel 82599EB 10 Gigabit Ethernet network devices. This update corrects the return code in the ixgbe_cache_ring_fdir function and setting of the registers that control the RSS redirection table. Also, obsolete code related to Flow Director support has been removed. The RSS functionality now works as expected on these devices.

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.

4.77.6. RHSA-2012:0480 — Important: kernel security, bug fix, and enhancement update

Updated kernel packages that fix one security issue, various 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. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

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

Security Fix

CVE-2012-1583, Important

A flaw in the xfrm6_tunnel_rcv() function in the Linux kernel's IPv6 implementation could lead to a use-after-free or double free flaw in tunnel6_rcv(). A remote attacker could use this flaw to send specially-crafted packets to a target system that is using IPv6 and also has the xfrm6_tunnel kernel module loaded, causing it to crash.

If you do not run applications that use xfrm6_tunnel, you can prevent the xfrm6_tunnel module from being loaded by creating (as the root user) a "/etc/modprobe.d/xfrm6_tunnel.conf" file, and adding the following line to it:

```
blacklist xfrm6_tunnel
```

This way, the xfrm6_tunnel module cannot be loaded accidentally. A reboot is not necessary for this change to take effect.

This update also fixes various bugs and adds an enhancement. Documentation for these changes is available in the Technical Notes document.

Users should upgrade to these updated packages, which contain backported patches to correct this issue, and fix the bugs and add the enhancement noted in the Technical Notes. The system must be rebooted for this update to take effect.

4.77.7. RHSA-2012:0690 — Important: kernel security and bug fix update

Updated kernel packages that fix one security issue and various 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. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

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

Security Fix

CVE-2012-2136, Important

It was found that the data_len parameter of the sock_alloc_send_pskb() function in the Linux kernel's networking implementation was not validated before use. A local user with access to a TUN/TAP virtual interface could use this flaw to crash the system or, potentially, escalate their privileges. Note that unprivileged users cannot access TUN/TAP devices until the root user grants them access.

This update also fixes various bugs. Documentation for these changes is available in the Technical Notes document.

Users should upgrade to these updated packages, which contain backported patches to correct this issue, and fix the bugs noted in the Technical Notes. The system must be rebooted for this update to take effect.

4.77.8. RHSA-2012:0721 — 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. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fixes

CVE-2012-0217, Important

It was found that the Xen hypervisor implementation as shipped with Red Hat Enterprise Linux 5 did not properly restrict the syscall return addresses in the sysret return path to canonical addresses. An unprivileged user in a 64-bit para-virtualized guest, that is running on a 64-bit host that has an Intel CPU, could use this flaw to crash the host or, potentially, escalate their privileges, allowing them to execute arbitrary code at the hypervisor level.

CVE-2012-2934, Moderate

It was found that guests could trigger a bug in earlier AMD CPUs, leading to a CPU hard lockup, when running on the Xen hypervisor implementation. An unprivileged user in a 64-bit para-virtualized guest could use this flaw to crash the host. Warning: After installing this update, hosts that are using an affected AMD CPU (refer to Red Hat Bugzilla bug #824966 for a list) will fail to boot. In order to boot such hosts, the new kernel parameter, allow_unsafe, can be used ("allow_unsafe=on"). This option should only be used with hosts that are running trusted guests, as setting it to "on" reintroduces the flaw (allowing guests to crash the host).

Note: For Red Hat Enterprise Linux guests, only privileged guest users can exploit the CVE-2012-0217 and CVE-2012-2934 issues.

Red Hat would like to thank the Xen project for reporting these issues. Upstream acknowledges Rafal Wojtczuk as the original reporter of CVE-2012-0217.

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.

4.77.9. RHSA-2012:1174 — Low: kernel security and bug fix update

Updated kernel packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 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 for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fix

CVE-2012-2313, Low

A flaw was found in the way the Linux kernel's dl2k driver, used by certain D-Link Gigabit Ethernet adapters, restricted IOCTLs. A local, unprivileged user could use this flaw to issue potentially harmful IOCTLs, which could cause Ethernet adapters using the dl2k driver to malfunction (for example, losing network connectivity).

Red Hat would like to thank Stephan Mueller for reporting this issue.

This update also fixes several bugs. Documentation for these changes is available in the 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.

4.77.10. RHSA-2012:1323 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fixes

CVE-2012-3412, Important

A flaw was found in the way socket buffers (skb) requiring TSO (TCP segment offloading) were handled by the sfc driver. If the skb did not fit within the minimum-size of the transmission queue, the network card could repeatedly reset itself. A remote attacker could use this flaw to cause a denial of service.

CVE-2012-3510, Moderate

A use-after-free flaw was found in the xacct_add_tsk() function in the Linux kernel's taskstats subsystem. A local, unprivileged user could use this flaw to cause an information leak or a denial of service.

CVE-2012-2319, Low

A buffer overflow flaw was found in the hfs_bnode_read() function in the HFS Plus (HFS+) file system implementation in the Linux kernel. A local user able to mount a specially-crafted HFS+ file system image could use this flaw to cause a denial of service or escalate their privileges.

CVE-2012-3430, Low

A flaw was found in the way the msg_namelen variable in the rds_recvmsg() function of the Linux kernel's Reliable Datagram Sockets (RDS) protocol implementation was initialized. A local, unprivileged user could use this flaw to leak kernel stack memory to user-space.

Red Hat would like to thank Ben Hutchings of Solarflare (tm) for reporting CVE-2012-3412, and Alexander Peslyak for reporting CVE-2012-3510. The CVE-2012-3430 issue was discovered by the Red Hat InfiniBand team.

Bug Fixes

BZ#846125

The cpuid_whitelist() function, masking the Enhanced Intel SpeedStep (EST) flag from all guests, prevented the "cpuspeed" service from working in the privileged Xen domain (dom0). CPU scaling was therefore not possible. With this update, cpuid_whitelist() is aware whether the domain executing CPUID is privileged or not, and enables the EST flag for dom0.

BZ#847326

If a delayed-allocation write was performed before quota was enabled, the kernel displayed the following warning message:

```
        WARNING: at fs/quota/dquot.c:988
dquot_claim_space+0x77/0x112()
```

This was because information about the delayed allocation was not recorded in the quota structure. With this update, writes prior to enabling quota are properly accounted for, and the message is not displayed.

BZ#847327

In Red Hat Enterprise Linux 5.9, the DSCP (Differentiated Services Code Point) netfilter module now supports mangling of the DSCP field.

BZ#847359

Some subsystems clear the TIF_SIGPENDING flag during error handling in fork() paths. Previously, if the flag was cleared, the ERESTARTNOINTR error code could be returned. The underlying source code has been modified so that the error code is no longer returned.

BZ#852448

An unnecessary check for the RXCW.CW bit could cause the Intel e1000e NIC (Network Interface Controller) to not work properly. The check has been removed so that the Intel e1000e NIC works 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.

4.77.11. RHSA-2012:1445 — Low: kernel security and bug fix update

Updated kernel packages that fix one security issue and several bugs are now available for Red Hat Enterprise Linux 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 for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fix

CVE-2012-2100, Low

It was found that the RHSA-2010:0178 update did not correctly fix the CVE-2009-4307 issue, a divide-by-zero flaw in the ext4 file system code. A local, unprivileged user with the ability to mount an ext4 file system could use this flaw to cause a denial of service.

This update also fixes several bugs. Documentation for these changes is available in the Technical Notes document.

Users should upgrade to these updated packages, which contain backported patches to correct this issue, and fix the bugs noted in the Technical Notes. The system must be rebooted for this update to take effect.

4.77.12. RHSA-2012:1540 — Important: kernel security, bug fix, and enhancement update

Updated kernel packages that fix multiple security issues, two bugs, and add two 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. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

These packages contain the Linux kernel.

Security Fixes

CVE-2012-4508, Important

A race condition in the way asynchronous I/O and fallocate() interacted when using ext4 could allow a local, unprivileged user to obtain random data from a deleted file.

CVE-2012-5513, Important

A flaw in the way the Xen hypervisor implementation range checked guest provided addresses in the XENMEM_exchange hypercall could allow a malicious, para-virtualized guest administrator to crash the hypervisor or, potentially, escalate their privileges, allowing them to execute arbitrary code at the hypervisor level.

CVE-2012-2372, Moderate

A flaw in the Reliable Datagram Sockets (RDS) protocol implementation could allow a local, unprivileged user to cause a denial of service.

CVE-2012-3552, Moderate

A race condition in the way access to inet->opt ip_options was synchronized in the Linux kernel's TCP/IP protocol suite implementation. Depending on the network facing applications running on the system, a remote attacker could possibly trigger this flaw to cause a denial of service. A local,

unprivileged user could use this flaw to cause a denial of service regardless of the applications the system runs.

CVE-2012-4535, Moderate

The Xen hypervisor implementation did not properly restrict the period values used to initialize per VCPU periodic timers. A privileged guest user could cause an infinite loop on the physical CPU. If the watchdog were enabled, it would detect said loop and panic the host system.

CVE-2012-4537, Moderate

A flaw in the way the Xen hypervisor implementation handled set_p2m_entry() error conditions could allow a privileged, fully-virtualized guest user to crash the hypervisor.

Red Hat would like to thank Theodore Ts'o for reporting CVE-2012-4508; the Xen project for reporting CVE-2012-5513, CVE-2012-4535, and CVE-2012-4537; and Hafid Lin for reporting CVE-2012-3552. Upstream acknowledges Dmitry Monakhov as the original reporter of CVE-2012-4508. CVE-2012-2372 was discovered by Li Honggang of Red Hat.

Bug Fixes

BZ#870118

Previously, the interrupt handlers of the qla2xxx driver could clear pending interrupts right after the IRQ lines were attached during system start-up. Consequently, the kernel could miss the interrupt that reported completion of the link initialization, and the qla2xxx driver then failed to detect all attached LUNs. With this update, the qla2xxx driver has been modified to no longer clear interrupt bits after attaching the IRQ lines. The driver now correctly detects all attached LUNs as expected.

BZ#877943

The Ethernet channel bonding driver reported the MII (Media Independent Interface) status of the bond interface in 802.3ad mode as being up even though the MII status of all of the slave devices was down. This could pose a problem if the MII status of the bond interface was used to determine if failover should occur. With this update, the agg_device_up() function has been added to the bonding driver, which allows the driver to report the link status of the bond interface correctly, that is, down when all of its slaves are down, in the 802.3ad mode.

Enhancements

BZ#870120

This update backports several changes from the latest upstream version of the bnx2x driver. The most important change, the remote-fault link detection feature, allows the driver to periodically scan the physical link layer for remote faults. If the physical link appears to be up and a fault is detected, the driver indicates that the link is down. When the fault is cleared, the driver indicates that the link is up again.

BZ#874973

The INET socket interface has been modified to send a warning message when the ip_options structure is allocated directly by a third-party module using the kmalloc() function.

Users should upgrade to these updated packages, which contain backported patches to correct these issues and add these enhancements. The system must be rebooted for this update to take effect.

4.78. kexec-tools

4.78.1. RHBA-2012:1272 — kexec-tools bug fix update

Updated kexec-tools packages that fix a 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 Fix

BZ#822617

When one interface was used for a iSCSI boot environment while is other was used by kdump with the "net" option on, the ifconfig utility caused an error. Consequently, vmcore was not collected in a dump server that stores vmcore specified in the kdump.conf file. This bug has been fixed and a memory dump capture now succeeds by kdump in an iSCSI boot environment.

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

4.78.2. RHBA-2013:0012 — kexec-tools bug fix and enhancement update

Updated *kexec-tools* packages that fix multiple bugs and add one enhancement 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#716340

Previously, kdump could become unresponsive if a disk name was changed. This could happen because the kdump **`initrd`** did not include irrelevant disk drivers that were used in the first kernel. Persistent disk names change in kdump presents considerable risk to Red Hat Enterprise Linux 5 stability. Therefore, this problem has been resolved by updating the kdump.conf file to recommend to use disk **`UUIDs`** or **`LABELs`** instead of disk names for file-system based dump targets.

BZ#716386

Previously, kdump did not verify whether the target raw dump device exists before attempting to dump a core file. Instead, kdump started to rebuild an **`initrd`** image directly, which resulted in a kdump failure. Furthermore, even though raw dump succeeded, kdump did not verify whether the **`vmcore`** file was saved and the core file could not be recovered. This update modifies the kdump init script to perform verification tests on the target device. Kdump now no longer rebuilds the initrd image if the target device does not exist and properly recovers a core file if the raw dump has succeeded.

BZ#752930

Kdump previously used an IP address as a part of the core dump directory name only for remote core dumps, which was confusing the users. With this update, kdump was modified to use the IP address of the **`loopback`** device (**`127.0.0.1`**) for local dumps so that the core dump directory name has the same form for both local and remote core dumps.

BZ#771829

Usually, when dumping a vmcore file over network, kdump has to bring up only one network interface card (NIC). However, when dumping to an iSCSI device, kdump may need to bring up multiple NICs. This functionality was not previously implemented in kdump and any dump attempt to the iSCSI device that required multiple NICs failed. With this update, kdump has been modified to be able to bring up multiple NICs if needed, and vmcore can now be successfully dumped on the iSCSI device.

BZ#788678

The **mkdumprd** utility did not detect the **/var** file system if it was mounted on a separate partition, which caused kdump to fail to dump a core file. This update modifies **mkdumprd** to detect the partition that contains the **/var** file system correctly. Kdump no longer fails in this scenario.

BZ#801496

When dumping a core file using ssh and the remote kdump user is configured to use restricted shel (rksh), the core dump attempt failed. This happened because kdump used the **cat >** command to store the **vmcore** file and the restricted shell forbids redirection. This update modifies kdump to use the dd command to save the vmcore file instead and dumping is now successful in this scenario.

BZ#802928

The mkdumprd utility did not correctly handled NICs if the NIC had the ***BOOTPROTO=none*** parameter configured in the ifcfg file. Consequently, kdump was not able to bring the NIC up and failed to dump a core file over network. This update corrects mkdumprd to recognize the ***BOOTPROTO=none*** parameter, and such NICs are now properly brought up when dumping a core file over network.

BZ#809983

Previously for **ext2**, **ext3** and **ext4** file systems, if the dump location was on different file system than was the root file system, the mkdumprd utility searched only for the ext4 kernel module. Consequently, kdump failed to recognize a file system and dump a core file. This update modifies mkdumprd to find proper kernel module also for ext2 and ext3 file systems and kdump works as expected in this scenario.

BZ#832017

Currently on Red Hat Enterprise Linux 5, the **dd** utility is the default core collector when dumping or a raw partition. However, the only core collector supported by kdump is the **makedumpfile** utility, which is not able to recognize vmcore files copied by dd. Previously, when the vmcore file was dumped on a raw partition, it was considered invalid and the core file recovery failed. With this update, **mkdumprd** has been modified to display a warning message when a different core collector than **makedumpfile** was used to compress the core file on the raw partition. The user has to recover the core dump manually.

Enhancement

BZ#587361

Previously, the **vmcore** file could not be dumped to a **multipath** device because **kexec-tools** did not support this option. This update introduces multipath target support, which allows vmcore to be captured with multipath devices.

Users of *kexec-tools* are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.79. ksh

4.79.1. RHBA-2012:0432 — ksh bug fix update

An updated ksh package that fixes one bug is now available for Red Hat Enterprise Linux 5.

KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language which is also compatible with sh, the original Bourne Shell.

Bug Fix

BZ#805459

Previously, ksh did not expand the tilde (~) character properly. For example, characters in the tilde prefix were not treated as a login name but as a part of the path and the "No such file or directory" message was displayed. The underlying source code has been modified and tilde expansion now works as expected in such a scenario.

All users of ksh are advised to upgrade to this updated package, which fixes this bug.

4.79.2. RHBA-2013:0042 — ksh bug fix update

Updated ksh packages that fix several bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

KSH-93 is the most recent version of the KornShell by David Korn of AT&T Bell Laboratories. KornShell is a shell programming language which is also compatible with sh, the original Bourne Shell.

Bug Fixes

BZ#771188

Prior to this update, using the -R or -Z options of the typeset command did not work as expected. When a variable was assigned to a field that was of smaller size than the size of the variable, it would trim the incorrect values from the variable. Consequently, the resulting value in the trimmed variable was incorrect. The underlying source code has been modified and the typeset -R/-Z command works as expected.

BZ#802565

Previously, ksh did not expand the tilde (~) character properly. For example, characters in the tilde prefix were not treated as a login name but as a part of the path and the "No such file or directory" message was displayed. The underlying source code has been modified and tilde expansion now works as expected in such a scenario.

BZ#804925

In certain cases, ksh unnecessarily called the vfork() function. An extra process was created and it could be difficult to determine how many instances of a script were running. A patch has been applied to address this problem, and extra processes are no longer created if not required.

BZ#811318

Due to a missing patch that introduced the tsetio flag, the redirect output behavior changed depending on what ksh version was used. With this update, the missing patch was added and redirect output behavior is now consistent across all versions of ksh.

BZ#812930

Previously, ksh did not close certain file descriptors prior to execution. This could lead to a file descriptor leak, and certain applications could consequently report error messages. With this update, file descriptors are marked to be closed on execution if appropriate, so file descriptor leaks no longer occur.

BZ#827522

Due to a bug in the typeset command, when executed with the -Z option, output was being formatted to an incorrect width. As a result, exporting a right-aligned variable of smaller size than the predefined field size caused it to not be prepended with 0 characters. With this update, the typeset command works as expected in the aforementioned scenario.

BZ#827613

Previously, ksh did not allocate the correct amount of memory for its data structures containing information about file descriptors. When running a task that used file descriptors extensively, ksh terminated unexpectedly with a segmentation fault. With this update, the proper amount of memory is allocated, and ksh no longer crashes if file descriptors are used extensively.

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

4.80. kudzu

4.80.1. RHBA-2013:0053 — kudzu bug fix and enhancement update

Updated kudzu packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 5.

The kudzu packages provide a hardware probing library for automatic discovery and configuration of hardware.

Bug Fix

BZ#748481

Prior to this update, the X11 configuration of video cards was skipped if no kernel driver was available, even if a corresponding Xorg driver existed. This update skips the configuration only in cases when none of the mentioned drivers are aqvailable.

Enhancement

BZ#819903

This update adds native support for Microsoft Hyper-V virtual hardware.

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

4.81. kvm

4.81.1. RHBA-2012:0398 — kvm bug fix update

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

[Updated 16 May 2012] This advisory has been updated with the correct description for bug 802429. The packages included in this revised update have not been changed in any way from the packages included in the original advisory.

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#802429

An accounting error in the I/O thread subsystem in QEMU could, under certain circumstances, lead to I/O stalls on the guest. This would typically cause the guest to become unresponsive. With this update, the accounting error has been corrected, and I/O stalls no longer occur in this scenario.

All users of kvm are advised to upgrade to these updated packages, which fix this bug. Note that the procedure in the Solution section must be performed before this update will take effect.

4.81.2. RHBA-2013:0007 — 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 Fixes

BZ#814096

Under certain circumstances, the qemu-kvm utility tried to invalidate an incorrect physical memory block, which resulted in qemu-kvm to terminate unexpectedly with a segmentation fault. The code has been fixed and the crashes no longer occur.

BZ#684745

Previously, when an I/O error occurred on a KVM host, the guest running on it became paused. After the guest was migrated to another host, the guest could not be properly resumed. Consequently, it was impossible to log in to the guest via SSH or a console. This bug has been fixed and migrated guests can now be resumed as expected.

BZ#782631

Due to an accounting error in the QEMU I/O thread subsystem, I/O delays were occurring on guests, which were observed as unresponsive for the time of the delay. This bug has been fixed and the delays no longer occur.

BZ#805676

Due to an incompatibility between previously used encryption modes and FIPS mode, it was impossible to start KVM guests when running kernel in FIPS mode. With this update, VNC password authentication is disabled when the host system is operating in FIPS mode, and QEMU exits and returns an error message 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 work as expected.

BZ#838466

Previously, the typeperf command of the virtualized Microsoft Windows Server 2008 Service Pack 2 for the x86 architecture with the SQL Server 2005 Service Pack 3 installed returned an invalid value for the Processor Time. This bug has been fixed and typeperf now returns a correct value.

BZ#761350

Previously, a simple counter was used to track GSIs (Global System Interrupts) that were given to devices. Consequently, when a hot plug or unplug operation was performed approximately 30 times on certain Ethernet controllers in a Microsoft Windows Server 2008 guest on the AMD64 and Intel 64 architectures, the controller driver returned a large number of error messages on incorrectly deallocated MSI-X table entries. This update uses a bitmap to track GSIs and the errors no longer occur.

BZ#843683

Previously, KVM did not provide receive overrun status information, which is used for virtual serial devices. Consequently, virtual machines using a serial console redirection became unresponsive on startup. This update implements receive overrun status and the hangs no longer occur.

BZ#829040

Due to a coding bug, the masking in the device assignment function was invalid. Consequently, the KVM device assignment bridge test could break virtual function of certain devices that implement BAR (Base Address Register) resources. This bug has been fixed and the test now works as expected.

BZ#781922

Under certain circumstances, implementation of the Realtek 8139 Ethernet driver allowed the qemu-kvm utility to attempt to allocate unlimited buffer size. If it happened, qemu-kvm terminated unexpectedly with a glib error, unable to allocate such a buffer. This update limits the transmission buffer size of the driver, thus fixing this bug.

BZ#819413

Previously, it was possible to shut down a guest using the system_powerdown command even if the "-no-shutdown" option was specified on the command line. This bug has been fixed and "-no-shutdown" is now handled properly.

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.

4.81.3. RHSA-2012:0676 — Moderate: kvm security and bug fix update

Updated kvm packages that fix two security issues and one bug 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) 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-2012-1601

A flaw was found in the way the KVM_CREATE_IRQCHIP ioctl was handled. Calling this ioctl when at least one virtual CPU (VCPU) already existed could lead to a NULL pointer dereference later when the VCPU is scheduled to run. A malicious user in the kvm group on the host could use this flaw to crash the host.

CVE-2012-2121

A flaw was found in the way device memory was handled during guest device removal. Upon successful device removal, memory used by the device was not properly unmapped from the corresponding IOMMU or properly released from the kernel, leading to a memory leak. A malicious user in the kvm group on the host who has the ability to assign a device to a guest could use this flaw to crash the host.

Bug Fix

BZ#816207

An off-by-one error in the QEMU guest's memory management could, in rare cases, cause QEMU-KVM to crash due to a segmentation fault in tb_invalidate_phys_page_range() if a device initiated DMA into a specific guest address. In a reported case, this issue presented on a system that had a guest using the 8139cp network driver.

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.

4.81.4. RHSA-2012:1235 — 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(s) 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 Fix

CVE-2012-3515

A flaw was found in the way QEMU handled VT100 terminal escape sequences when emulating certain character devices. A guest user with privileges to write to a character device that is emulated on the host using a virtual console back-end could use this flaw to crash the qemu-kvm process on the host or, possibly, escalate their privileges on the host.

This flaw did not affect the default use of KVM. Affected configurations were:

* When guests were started from the command line ("/usr/libexec/qemu-kvm"), and without specifying a serial or parallel device that specifically does not use a virtual console (vc) back-end. (Note that Red Hat does not support invoking "qemu-kvm" from the command line on Red Hat Enterprise Linux 5.)

* Guests that were managed via libvirt, such as when using Virtual Machine Manager (virt-manager), but that have a serial or parallel device that uses a virtual console back-end. By default, guests managed via libvirt will not use a virtual console back-end for such devices.

Red Hat would like to thank the Xen project for reporting this issue.

All KVM users should upgrade to these updated packages, which correct this issue. Note: The procedure in the Solution section must be performed before this update will take effect.

4.82. lftp

4.82.1. RHBA-2013:0071 — lftp bug fix update

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

LFTP is a file transfer utility for FTP, SFTP, HTTP, and other commonly used protocols. It uses the readline library for input, and provides support for bookmarks, built-in monitoring, job control, and parallel transfer of multiple files at the same time

Bug Fix

BZ#810217

Due to an incorrect evaluation of the length of an uploaded file, the lftp tool became unresponsive after a file transfer in ASCII mode. With this update, the volume of transferred data is recognized correctly and the lftp program no longer hangs in this scenario.

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

4.83. libexif

4.83.1. RHSA-2012:1255 — Moderate: libexif security update

Updated libexif 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The libexif packages provide an Exchangeable image file format (Exif) library. Exif allows metadata to be added to and read from certain types of image files.

Security Fix

CVE-2012-2812, CVE-2012-2813, CVE-2012-2814, CVE-2012-2836, CVE-2012-2837, CVE-2012-2840, CVE-2012-2841

Multiple flaws were found in the way libexif processed Exif tags. An attacker could create a specially-crafted image file that, when opened in an application linked against libexif, could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

Red Hat would like to thank Dan Fandrich for reporting these issues. Upstream acknowledges Mateusz Jurczyk of the Google Security Team as the original reporter of CVE-2012-2812, CVE-2012-2813, and CVE-2012-2814; and Yunho Kim as the original reporter of CVE-2012-2836 and CVE-2012-2837.

Users of libexif are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. All running applications linked against libexif must be restarted for the update to take effect.

4.84. libgcrypt

4.84.1. RHEA-2012:0484 — libgcrypt enhancement update

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

The libgcrypt library provides general-purpose implementations of various cryptographic algorithms.

Enhancement

BZ#810319

With Federal Information Processing Standards (FIPS) mode enabled, the libgcrypt library always started in the soft FIPS mode which allows applications to use the MD5 cryptographic hash algorithm. The libgcrypt API previously did not allow the library to programmatically switch from the soft FIPS mode to the enforced FIPS mode. With this update, if the application does not need MD5 support for the Transport Layer Security (TLS) protocol or non-cryptographic purposes, libgcrypt can be preset in the enforced FIPS mode.

All users of libgcrypt are advised to upgrade to these updated packages, which add this enhancement.

4.85. libpng

4.85.1. RHSA-2012:0407 — Moderate: libpng security update

Updated libpng 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 for each vulnerability from the CVE link(s) associated with each description below.

The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

Security Fix

CVE-2011-3045

A heap-based buffer overflow flaw was found in the way libpng processed compressed chunks in PNG image files. An attacker could create a specially-crafted PNG image file that, when opened, could cause an application using libpng to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Users of libpng should upgrade to these updated packages, which correct this issue. For Red Hat Enterprise Linux 5, they contain a backported patch. For Red Hat Enterprise Linux 6, they upgrade libpng to version 1.2.48. All running applications using libpng must be restarted for the update to take effect.

4.85.2. RHSA-2012:0523 — Moderate: libpng security update

Updated libpng 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 for each vulnerability from the CVE link(s) associated with each description below.

The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.

Security Fix

CVE-2011-3048

A heap-based buffer overflow flaw was found in the way libpng processed tEXt chunks in PNG image files. An attacker could create a specially-crafted PNG image file that, when opened, could cause an application using libpng to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

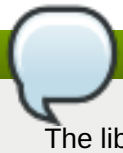
Users of libpng should upgrade to these updated packages, which correct this issue. For Red Hat Enterprise Linux 5, they contain a backported patch. For Red Hat Enterprise Linux 6, they upgrade libpng to version 1.2.49. All running applications using libpng must be restarted for the update to take effect.

4.86. libtalloc

4.86.1. RHBA-2013:0098 — libtalloc bug fix update

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

The libtalloc packages provide a library that implements a hierarchical memory allocator with destructors.



Note

The libtalloc packages have been upgraded to upstream version 2.0.7, which provides a number of bug fixes over the previous version. (BZ#855862)

Bug Fix

BZ#837853, BZ#855387

The talloc() hierarchical allocator did not ensure that the child pointers of a pointer did not become invalid during memory freeing operation. Consequently, processes that use the talloc library, such as the spoolss process of samba, could have terminated with a segmentation fault. The underlying source code has been modified and talloc() no longer causes Samba to fail in this situation.

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

4.87. libtdb

4.87.1. RHBA-2013:0016 — libtdb bug fix and enhancement update

Updated libtdb packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The libtdb packages provide a library that implements the Trivial Database (TDB). TDB is based on the GNU dbm (GDBM) library of database functions but uses internal locking to allow multiple simultaneous writers.

Note

The libtdb packages have been upgraded to upstream version 1.2.10, which provides a number of bug fixes and enhancements over the previous version. (BZ#837865)

Bug Fix

BZ#736112

Prior to this update, several names and file paths of binaries and manual pages in the tdb-tools package were in conflict with binaries and manual pages that are shipped in the samba package. With this update, these files have been renamed to avoid conflicts.

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

4.88. libtiff

4.88.1. RHSA-2012:0468 — Important: libtiff security update

Updated libtiff 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. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

Security Fix

CVE-2012-1173

Two integer overflow flaws, leading to heap-based buffer overflows, were found in the way libtiff attempted to allocate space for a tile in a TIFF image file. An attacker could use these flaws to create a specially-crafted TIFF file that, when opened, would cause an application linked against libtiff to crash or, possibly, execute arbitrary code.

All libtiff users should upgrade to these updated packages, which contain a backported patch to resolve these issues. All running applications linked against libtiff must be restarted for this update to take effect.

4.88.2. RHSA-2012:1054 — Important: libtiff security update

Updated libtiff 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 important security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

Security Fixes

CVE-2012-2088

libtiff did not properly convert between signed and unsigned integer values, leading to a buffer overflow. An attacker could use this flaw to create a specially-crafted TIFF file that, when opened, would cause an application linked against libtiff to crash or, possibly, execute arbitrary code.

CVE-2012-2113

Multiple integer overflow flaws, leading to heap-based buffer overflows, were found in the tiff2pdf tool. An attacker could use these flaws to create a specially-crafted TIFF file that would cause tiff2pdf to crash or, possibly, execute arbitrary code.

All libtiff users should upgrade to these updated packages, which contain backported patches to resolve these issues. All running applications linked against libtiff must be restarted for this update to take effect.

4.88.3. RHSA-2012:1590 — Moderate: libtiff security update

Updated libtiff 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

Security Fixes

CVE-2012-4447

A heap-based buffer overflow flaw was found in the way libtiff processed certain TIFF images using the Pixar Log Format encoding. An attacker could create a specially-crafted TIFF file that, when opened, could cause an application using libtiff to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

CVE-2012-5581

A stack-based buffer overflow flaw was found in the way libtiff handled DOTRANGE tags. An attacker could use this flaw to create a specially-crafted TIFF file that, when opened, would cause an application linked against libtiff to crash or, possibly, execute arbitrary code.

CVE-2012-3401

A heap-based buffer overflow flaw was found in the tiff2pdf tool. An attacker could use this flaw to create a specially-crafted TIFF file that would cause tiff2pdf to crash or, possibly, execute arbitrary code.

CVE-2012-4564

A missing return value check flaw, leading to a heap-based buffer overflow, was found in the ppm2tiff tool. An attacker could use this flaw to create a specially-crafted PPM (Portable Pixel Map) file that would cause ppm2tiff to crash or, possibly, execute arbitrary code.

The CVE-2012-5581, CVE-2012-3401, and CVE-2012-4564 issues were discovered by Huzaifa Sidhpurwala of the Red Hat Security Response Team.

All libtiff users should upgrade to these updated packages, which contain backported patches to resolve these issues. All running applications linked against libtiff must be restarted for this update to take effect.

4.89. libuser

4.89.1. RHBA-2012:1144 — libuser bug fix update

Updated libuser packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The libuser packages provide a library to implement a standardized interface for manipulating and administering user and group accounts. The library uses pluggable back ends to interface to its data sources. Sample applications modeled after those included with the shadow password suite are included.

Bug Fixes

BZ#506628

Prior to this update, libuser could not signal the name service caching daemon (nscd) to refresh the cache. As a consequence, delays in the name service could occur when the user account information was changed. With this update, the libuser signals nscd to rebuild its cache. Now, changes that affect the name service take effect more quickly.

BZ#670279

Prior to this update, libuser used the value of the "gecos" attribute for the "cn" attribute by default when creating a user account with the Lightweight Directory Access Protocol (LDAP). As a consequence, an invalid value for "cn" was used and the user account was not created if the "gecos" attribute was empty. With this update, the user name of the account is stored in the "cn" attribute if the "gecos" attribute is empty, thus allowing successful creation of the user account.

BZ#758117

Prior to this update, libuser could attempt to access unallocated virtual memory when searching for account information in files of certain sizes. As a consequence, libuser could terminate unexpectedly with a segmentation fault when looking for user or group account information. This update modifies modifies the libuser library to only access memory related to the file being processed.

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

4.90. libvirt

4.90.1. RHSA-2013:0127 — Low: libvirt security and bug fix update

Updated libvirt 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 for each vulnerability from the CVE link(s) associated with each description below.

The libvirt library is a C API for managing and interacting with the virtualization capabilities of Linux and other operating systems. In addition, libvirt provides tools for remote management of virtualized systems.

Security Fix

CVE-2012-2693

Bus and device IDs were ignored when attempting to attach multiple USB devices with identical vendor or product IDs to a guest. This could result in the wrong device being attached to a guest, giving that guest root access to the device.

Bug Fixes

BZ#675319

Previously, the libvirtd library failed to set the autostart flags for already defined QEMU domains. This bug has been fixed, and the domains can now be successfully marked as autostarted.

BZ#680289

Prior to this update, the virFileAbsPath() function was not taking into account the slash ("/") directory separator when allocating memory for combining the cwd() function and a path. This behavior could lead to a memory corruption. With this update, a transformation to the virAsprintff() function has been introduced into virFileAbsPath(). As a result, the aforementioned behavior no longer occurs.

BZ#783001

With this update, a man page of the virsh user interface has been enhanced with information on the "domxml-from-native" and "domxml-to-native" commands. A correct notation of the format argument has been clarified. As a result, confusion is avoided when setting the format argument in the described commands.

All users of libvirt are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, libvirtd will be restarted automatically.

4.91. libwpd

4.91.1. RHSA-2012:1043 — Important: libwpd security update

Updated libwpd 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(s) associated with each description below.

libwpd is a library for reading and converting Corel WordPerfect Office documents.

Security Fix

CVE-2012-2149

A buffer overflow flaw was found in the way libwpd processed certain Corel WordPerfect Office documents (.wpd files). An attacker could provide a specially-crafted .wpd file that, when opened in an application linked against libwpd, such as OpenOffice.org, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

All libwpd users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications that are linked against libwpd must be restarted for this update to take effect.

4.92. libxml2

4.92.1. RHSA-2012:1288 — Moderate: libxml2 security update

Updated libxml2 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The libxml2 library is a development toolbox providing the implementation of various XML standards.

Security Fixes

CVE-2012-2807

Multiple integer overflow flaws, leading to heap-based buffer overflows, were found in the way libxml2 handled documents that enable entity expansion. A remote attacker could provide a large, specially-crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

CVE-2011-3102

A one byte buffer overflow was found in the way libxml2 evaluated certain parts of XML Pointer Language (XPointer) expressions. A remote attacker could provide a specially-crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

All users of libxml2 are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The desktop must be restarted (log out, then log back in) for this update to take effect.

4.92.2. RHSA-2012:1512 — Important: 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 important security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

The libxml2 library is a development toolbox providing the implementation of various XML standards.

Security Fix

CVE-2012-5134

A heap-based buffer underflow flaw was found in the way libxml2 decoded certain entities. A remote attacker could provide a specially-crafted XML file that, when opened in an application linked against libxml2, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

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.

4.93. libxslt

4.93.1. RHSA-2012:1265 — Important: libxslt security update

Updated libxslt 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

libxslt is a library for transforming XML files into other textual formats (including HTML, plain text, and other XML representations of the underlying data) using the standard XSLT stylesheet transformation mechanism.

Security Fixes

CVE-2012-2871

A heap-based buffer overflow flaw was found in the way libxslt applied templates to nodes selected by certain namespaces. An attacker could use this flaw to create a malicious XSL file that, when used by an application linked against libxslt to perform an XSL transformation, could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

CVE-2012-2825, **CVE-2012-2870**, **CVE-2011-3970**

Several denial of service flaws were found in libxslt. An attacker could use these flaws to create a malicious XSL file that, when used by an application linked against libxslt to perform an XSL transformation, could cause the application to crash.

CVE-2011-1202

An information leak could occur if an application using libxslt processed an untrusted XPath expression, or used a malicious XSL file to perform an XSL transformation. If combined with other flaws, this leak could possibly help an attacker bypass intended memory corruption protections.

All libxslt users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. All running applications linked against libxslt must be restarted for this update to take effect.

4.94. linuxwacom

4.94.1. RHBA-2012:1271 — linuxwacom bug fix update

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

The linuxwacom package contains the drivers, libraries, and documentation for configuring and running Wacom tablets under the Linux operating system. It contains diagnostic applications as well as X.org XInput drivers.

Bug Fix

BZ#843859

Due to a regression, when a Wacom tablet was used with only a lens cursor device attached to it for input, the lens cursor could not be moved. This update fixes this bug and lens cursor devices now work as expected in the described scenario.

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

4.95. logrotate

4.95.1. RHBA-2012:0704 — logrotate bug fix and enhancement update

Updated logrotate packages that fix three bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

The logrotate utility simplifies the administration of multiple log files, allowing the automatic rotation, compression, removal, and mailing of log files.

Bug Fixes

BZ#644741

Prior to this update, a conflict could occur when string arrays between the popt library and a hand-coded method written in logrotate were allocated and freed. As a consequence, the "compressoptions" directive in the logrotate configuration file caused logrotate to abort unexpectedly. This update modifies the underlying code to use the popt library instead. Now, logrotate works as expected.

BZ#795405

Prior to this update, the ".rhn-cfg-tmp-" file exension was missing from the the list of extensions to be skipped when loading the configuration files. As a consequence, ".rhn-cfg-tmp-" files were loaded as normal configuration files and the rotation process was interrupted. This update adds the ".rhn-cfg-tmp-" extension to the list of extensions to be skipped.

BZ#736045

Prior to this update, the logrotate utility did not check whether brackets were correctly matched in the configuration file. As a consequence, files were removed because logrotate did not detect the incorrectly matched brackets and did not stop the rotation process for the particular configuration file. This update modifies the underlying code to check the presence of brackets whether they are matched. Now, configuration files with bad syntax are skipped.

Enhancement

BZ#510124

With this update, logrotate can rotate logs defined in configuration files that contain configuration errors.

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

4.96. logwatch

4.96.1. RHBA-2012:1217 — logwatch bug fix update

An updated logwatch package that fixes various bugs is now available.

Logwatch is a customizable, pluggable log-monitoring system. It will go through your logs for a given period of time and make a report in the areas that you wish with the detail that you wish. Easy to use - works right out of the package on many systems.

Bug Fixes

BZ#578806

Due to an incorrect regular expression, positive changes in temperatures reported by the smartd daemon were shown as unmatched entries in the logwatch output. This update fixes the faulty regular expression and temperature log information is now displayed correctly.

BZ#583607

Prior to this update, logwatch did not correctly parse the RSYSLOG_FileFormat time stamps and displayed them as unmatched entries. With this update, parsing of the rsyslog time stamps has been fixed and works as expected.

BZ#583721

Yum's "applydate" time ranges were not correctly parsed by logwatch and were displayed as unmatched entries. This has been fixed and "applydate" time ranges are no longer displayed as unmatched entries.

BZ#595068

Xen virtual console logins were not correctly parsed by logwatch and were displayed as unmatched entries. This update fixes this bug.

BZ#668067

Logins initiated with the "su -" or "su -l" command were not correctly parsed by logwatch and were displayed as unmatched entries. This update fixes this bug.

BZ#684577

SSH Kerberos (GSS) logins were not correctly parsed by logwatch and were displayed as unmatched entries. This update fixes this bug.

All users of logwatch are advised to upgrade to this updated package, which fixes these bugs.

4.97. lvm2

4.97.1. RHBA-2013:0023 — lvm2 bug fix update

Updated lvm2 packages that fix four bugs are now available for Red Hat Enterprise Linux 5.

The lvm2 packages provide support for Logical Volume Management (LVM).

Bug Fixes

BZ#770970

Prior to this update, the --alloc option in the lvm2 man pages was insufficiently documented. A more detailed specification of allocation policies was needed. With this update, the description has been enhanced and provides a more comprehensive insight into the allocation process.

BZ#786009

Previously, when the pv_min_size setting in the lvm.conf configuration file (/etc/lvm/lvm.conf) was set to value smaller than the default value of 2048 KB, the system ignored this configuration later on. Consequently, the lvm commands returned the following warning when processing smaller physical volumes:

Ignoring too small pv_min_size 512KB, using default 2048KB.

This bug has been fixed, and user-set pv_min_size is no longer ignored in the aforementioned case.

BZ#820237

Previously, when a physical volume (PV) with no physical extents (PE) was in a volume group (VG), the vgcfgrestore command executed on the VG failed with the following message:

Floating point exception

This behavior was caused by a division by zero error. With this update, a fix has been introduced to avoid the aforementioned exception. As a result, vgcfgrestore no longer fails in the described scenario.

BZ#821013

Previously, it was possible to use the lvcreate command with the --alloc cling option to create a linear device that exceeded any single physical volume (PV) within the volume group (VG). The lvcreate command placed the data across multiple PVs, which was in conflict with the cling allocation policy. This bug has been fixed and lvcreate now works in accordance with the selected allocation policy.

All users of lvm2 are advised to upgrade to these updated packages, which fix these bugs.

4.98. lvm2-cluster

4.98.1. RHBA-2013:0024 — lvm2-cluster bug fix update

Updated lvm2-cluster packages that fix one bug is now available for Red Hat Enterprise Linux 5.

The lvm2-cluster package provides support for Logical Volume Management (LVM) in a clustered environment.

Bug Fix

BZ#824813

If a physical volume (PV) presented in a volume group (VG) contained only metadata and no physical extents (PE), an attempt to write the volume group's metadata by running the "vgcfgrestore" command was not successful. Running the command failed with the "Floating point exception" error message, which was caused by a "division by zero" error. This bug has been fixed and lvm2-cluster now works correctly in such a case.

All users of lvm2-cluster are advised to upgrade to these updated packages, which fix this bug.

4.99. m2crypto

4.99.1. RHBA-2013:0020 — m2crypto bug fix and enhancement update

Updated m2crypto packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 5.

The m2crypto library allows Python programs to call OpenSSL functions.

Bug Fix

BZ#520817

M2Crypto generated an invalid exception object on SSL timeouts, causing an IndexError in the Python httplib module. This made it impossible to correctly handle SSL timeouts in applications. This updated package adds the required attributes to the SSL timeout exception object and lets httplib process this information correctly.

Enhancement

BZ#761596

The M2Crypto.httpslib.HTTPSConnection class always created an IPv4 socket. This made it impossible to connect to IPv6 servers using this class. With this update, the implementation now correctly creates an IPv4 or IPv6 socket, as necessary, thus adding support for IPv6 servers.

All users of m2crypto are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

4.100. man

4.100.1. RHBA-2012:0700 — man bug fix update

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

The man packages provide the man, apropos, and whatis tools to find information and documentation about the Linux system.

Bug Fix

BZ#749288

Prior to this update, the makewhatis script, which creates the whatis database of manual pages, ignored symbolic links between pages. With this update, the makewhatis script includes symbolic links in the whatis database.

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

4.101. man-pages-overrides

4.101.1. RHBA-2013:0073 — man-pages-overrides bug fix update

Updated man-pages-overrides packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The man-pages-overrides package contains a collection of manual pages to complement other packages or update those contained therein.

Bug Fixes

BZ#621953

Previously, the size of the buffer "entry" for the readdir_r() function was undocumented in the readdir(3) manual page. Consequently, a buffer overflow in user programs could occur. With this update, the readdir(3) manual page has been backported from Red Hat Enterprise Linux 6. As a result, the documentation of the readdir() and readdir_r() functions is now more accurate.

BZ#695783

Previously, the proper usage of the IPv6 addresses was not described in the ssh(1), scp(1), sftp(1) and sshd(8) manual pages. This update adapts these manual pages to reduce the possible ambiguity in the IPv6 address notation.

BZ#782006

Prior to this update, the vpdupdate(8) manual page did not contain any description of the "-a", "-s" and "-v" options. The manual page has been updated and the aforementioned options are now documented properly.

BZ#783739

The nscd.conf(5) manual page was missing some descriptions and contained several duplicate entries. With this update, the text has been clarified and redundant entries have been removed.

BZ#786684

Previously, the nsswitch.conf(5) manual page lacked information on the search mechanism, particularly about the "notfound" status. This update adds this information to the manual page.

BZ#787567

Prior to this update, the behavior of the connect() call with the local address set to INADDR_ANY was insufficiently described in the ip(7) manual page. Possible duplication of the local port after the call was not acknowledged. With this update, the documentation has been reworked in order to reflect the behavior of the connect() call correctly.

BZ#809490

Due to a vague description of the getdents() call in the getdents(2) manual page, the risk of using this call directly was not clear enough. The description has been extended with a warning to prevent incorrect usage of the getdents() call.

BZ#838395

Previously, the "-q" option of the scp program was insufficiently described in the scp(1) manual page. Part of its functionality was not mentioned, which could lead to unwanted results. The description has been extended and now provides a full characteristic of the "-q" option.

All users of man-pages-overrides are advised to upgrade to these updated packages, which fix these bugs.

4.102. mdadm

4.102.1. RHBA-2013:0018 — mdadm bug fix update

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

The mdadm packages contain a utility for creating, managing, and monitoring Linux MD (multiple disk) devices.

Bug Fixes

BZ#566828

Due to a bug in the raid-check script, non-zero mismatch counts were reported on RAID 1 arrays, although this could happen legitimately on this type of array. Consequently, the "repair" and "check" commands did not work as expected. The raid-check script has been fixed and now non-

"check" commands did not work as expected. The raid-check script has been fixed and now non-zero mismatch counts are no longer reported in the described scenario.

BZ#735803

Under certain circumstances, arrays that were always busy when running the raid-check script would never be checked due to a bug in the script. This script has been modified and all RAIDs with active I/0 are checked as expected.

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

4.103. microcode_ctl

4.103.1. RHEA-2013:0103 — 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#790195

The Intel CPU microcode file has been updated to version 20120606. This is the most recent version of the microcode available from Intel.

All 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.

4.104. mkinitrd

4.104.1. RHBA-2013:0027 — mkinitrd bug fix and enhancement update

Updated mkinitrd packages that fix two bugs and add two enhancements 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 Fixes

BZ#556785

Prior to this update, the "mkrootdev" command could incorrectly use the slave device instead of the intended multipath device to create the /dev/root node when a multipath root device was specified by the label "LABEL". As a consequence, the slave device could not be mounted as it was already used by the master and creating the "/dev/root" node failed. This update modifies the mkinitrd code so that "mkrootdev" now ignores devices which are in use.

BZ#782615

Prior to this update, the bindings file in the initial RAM disk (initrd) could, under certain circumstances, fail to match the bindings file on the root file system. As a consequence, the boot process was interrupted and the system rebooted. This update modifies the underlying code so match the bindings file as expected.

Enhancements

BZ#737081

This update adds support for using FIPS mode with dmraid root devices. The dmraid device is now activated before checking the FIPS checksum.

BZ#852686

This update adds support for Hyper-V to the mkinitrd utility.

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

4.105. mod_auth_kerb

4.105.1. RHBA-2013:0078 — mod_auth_kerb bug fix and enhancement update

Updated mod_auth_kerb packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

The mod_auth_kerb package provides a module for the Apache HTTP Server designed to provide Kerberos authentication over HTTP. The module supports the Negotiate authentication method, which performs full Kerberos authentication based on ticket exchanges.

Bug Fixes

BZ#456662

Prior to this update, the mod_auth_kerb source RPM could not be built by a non-root user. This was because the httpd-devel package places the apxs utility, which is needed to build the mod_auth_kerb package, into the /usr/sbin directory. This directory is not specified in the PATH variable for non-root users. With this update, the apxs utility is defined as being placed in the /usr/bin directory in the "mod_auth_kerb.spec" file, and the mod_auth_kerb SRPM can now be successfully built by non-root users.

BZ#734098

The "mod_auth_kerb" module did not use the Kerberos libraries in a thread-safe way. Therefore, if mod_auth_kerb ran under a multi-threaded Apache HTTP Server, authentication requests could terminate unexpectedly with a segmentation fault. With this update, the thread-safety problem has been fixed, and crashes no longer occur under these circumstances.

In addition, these updated mod_auth_kerb packages provide the following enhancement:

BZ#446670

The "KrbLocalUserMapping" Apache directive has been added to allow Kerberos principal names to be mapped to system user names.

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

4.106. mod_nss

4.106.1. RHBA-2012:1260 — mod_nss bug fix update

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

The mod_nss module provides strong cryptography for the Apache HTTP Server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, using the Network Security Services (NSS) security library.

Bug Fix

BZ#849044

Due to a regression, the mod_proxy module no longer worked when configured to support SSL reverse proxy operation. The following error message was logged:

[error] SSL Proxy: I don't have the name of the host we're supposed to connect to so I can't verify that we are connecting to who we think we should be. Giving up.

A new patch has been applied and the mod_proxy module now works correctly to support SSL reverse proxy.

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

4.106.2. RHBA-2013:0009 — mod_nss bug fix update

Updated mod_nss packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The mod_nss module provides strong cryptography for the Apache HTTP Server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, using the Network Security Services (NSS) security library.

Bug Fixes

BZ#669963

The previous release had an incorrect post-install script. Consequently, when upgrading "mod_nss" from version 1.0.3 to 1.0.8, the group and file permissions were incorrectly set. The HTTP server (httpd) did not start and the following error message was displayed:

[error] NSS_Initialize failed. Certificate database: /etc/httpd/alias. [error] SSL Library Error: -8038 SEC_ERROR_NOT_INITIALIZED

This update improves the post-install script to set file permissions and ownership correctly. As a result, all child processes of the Apache HTTP Server can enable SSL and now httpd starts as expected in the scenario described.

BZ#677698

With the release of "mod_nss" version 1.0.8 there was no lock mechanism to control sequential httpd process access to the "nss_pcache" process. This sometimes resulted in multiple requests being interpreted as a single request by "nss_pcache" and a single result returned. The calling process sometimes experienced a timeout error or a failure with the error message:

```
[error] Unable to read from pin store
```

With this update the code has been improved and multiple requests to the "nss_pcache" process are processed sequentially without the errors described.

BZ#692868

Due to a regression, the "mod_proxy" module no longer worked when configured to support reverse proxy operation. The following error was logged:

```
[error] SSL Proxy: I don't have the name of the host we're supposed
to
connect to so I can't verify that we are connecting to who we think
we
should be. Giving up.
```

A new patch has been applied and the "mod_proxy" module now works correctly to support SSL reverse proxy.

BZ#714255

Previously, a static array containing the arguments for launching the "nss_pcache" command overflowed the array size by one. This could lead to a variety of problems including unexpected termination. This bug has been fixed, and "mod_nss" now uses a properly sized static array when launching "nss_pcache".

BZ#749401

Due to an incorrect use of the memcpy() function in the "mod_nss" module, running the Apache HTTP Server with this module enabled could cause some requests to fail with the following message written to the error_log file:

```
request failed: error reading the headers
```

This update applies a patch to ensure that the memcpy() function is now used in accordance with the current specification, and using the "mod_nss" module no longer causes HTTP requests to fail.

BZ#749402

Prior to this update, client certificates were only retrieved during the initial SSL handshake if the NSSVerifyClient option was set to "require" or "optional". Also, the FakeBasicAuth option only retrieved Common Name rather than the entire certificate subject. Consequently, it was possible to spoof an identity using that option. This bug has been fixed, the FakeBasicAuth option is now prefixed with "/" and is thus compatible with OpenSSL. Certificates are now retrieved on all subsequent requests beyond the first one.

BZ#749405, BZ#784548

When the NSS library was not initialized and "mod_nss" tried to clear its SSL cache on start-up, "mod_nss" terminated unexpectedly when the NSS library was built with debugging enabled. With this update, "mod_nss" does not try to clear the SSL cache in the described scenario, thus preventing this bug.

BZ#749406

The "Requires: %{_libdir}/libnssckbi.so" directive has been added to the spec file to make "libnssckbi.so" a runtime dependency. This is to prevent symbolic links failing.

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

4.107. mod_python

4.107.1. RHBA-2012:1113 — mod_python bug fix update

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

The mod_python packages provide a module to embed the Python language interpreter within the Apache web server, allowing handlers to be written in Python.

Bug Fix

BZ#431684

Prior to this update, the publisher module did not correctly handle certain authentication variables. As a consequence, the web server could return an "400 Bad Request" error if the "publisher" handler was used with an authentication scheme other than "Basic". This update modifies the publisher.py code to handle the autentication as expected.

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

4.108. mozldap

4.108.1. RHBA-2013:0008 — mozldap bug fix update

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

The mozldap packages provide the Mozilla LDAP C SDK libraries that allow applications to communicate with Lightweight Directory Access Protocol (LDAP) directory servers. These libraries are derived from the University of Michigan and Netscape LDAP libraries and use Mozilla NSPR and NSS for crypto.

Bug Fix

BZ#753014

Prior to this update, the ldapsearch tool could, under certain circumstances, access or free uninitialized memory when following a smart referral entry using anonymous credentials. As a consequence, the ldapsearch tool could encounter a segmentation fault. This update ensures that the memory is initialized. Now, ldapsearch works with anonymous credentials as expected.

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

4.109. mt-st

4.109.1. RHBA-2012:1167 — mt-st bug fix update

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

The mt-st package contains the mt and st tape drive management programs. Mt (for magnetic tape drives) and st (for SCSI tape devices) can control rewinding, ejecting, skipping files and blocks and more.

Bug Fix

BZ#501014

Prior to this update, it was not possible to use a symbolic name for the SILI bit on the command line; the bit could only be specified as a hexadecimal constant (0x4000). With this update, users can use the "sili" symbolic name on the command line.

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

4.110. mutt

4.110.1. RHBA-2012:1143 — mutt bug fix update

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

Mutt is a text-mode mail user agent. Mutt supports color, threading, arbitrary key remapping, and a lot of customization.

Bug Fix

BZ#313291

Prior to this update, the mutt agent failed to allow interruptions during getch calls. As a consequence, the signal "SIGINT" (Ctrl-C) was not handled correctly when waiting for user input. This update modifies the underlying code to allow interruptions.

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

4.111. mysql

4.111.1. RHSA-2013:0121 — Low: mysql security and bug fix update

Updated mysql 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 for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fix

CVE-2012-4452

It was found that the fix for the CVE-2009-4030 issue, a flaw in the way MySQL checked the paths used as arguments for the DATA DIRECTORY and INDEX DIRECTORY directives when the "datadir" option was configured with a relative path, was incorrectly removed when the mysql packages in Red Hat Enterprise Linux 5 were updated to version 5.0.95 via RHSA-2012:0127. An authenticated attacker could use this flaw to bypass the restriction preventing the use of subdirectories of the MySQL data directory being used as DATA DIRECTORY and INDEX DIRECTORY paths. This update re-applies the fix for CVE-2009-4030.

Note: If the use of the DATA DIRECTORY and INDEX DIRECTORY directives were disabled as described in RHSA-2010:0109 (by adding "symbolic-links=0" to the "[mysqld]" section of the "my.cnf" configuration file), users were not vulnerable to this issue.

This issue was discovered by Karel Volný of the Red Hat Quality Engineering team.

Bug Fixes

647223

Prior to this update, the log file path in the logrotate script did not behave as expected. As a consequence, the logrotate function failed to rotate the "/var/log/mysqld.log" file. This update

consequence, the logrotate function failed to rotate the "/var/log/mysqld.log" file. This update modifies the logrotate script to allow rotating the mysqld.log file.

654000

Prior to this update, the mysqld daemon could fail when using the EXPLAIN flag in prepared statement mode. This update modifies the underlying code to handle the EXPLAIN flag as expected.

703476

Prior to this update, the mysqld init script could wrongly report that mysql server startup failed when the server was actually started. This update modifies the init script to report the status of the mysqld server as expected.

806365

Prior to this update, the "--enable-profiling" option was by default disabled. This update enables the profiling feature.

All MySQL users are advised to upgrade to these updated packages, which contain backported patches to resolve these issues. After installing this update, the MySQL server daemon (mysqld) will be restarted automatically.

4.112. net-snmp

4.112.1. RHBA-2012:0674 — net-snmp bug fix update

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

The net-snmp packages provide various libraries and tools for the Simple Network Management Protocol (SNMP), including an SNMP library, an extensible agent, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl Management information Base (MIB) browser.

Bug Fix

BZ#820850

The SNMP daemon (snmpd) did not properly encode a negative Request-ID in outgoing requests (for example during trap operations). As a consequence, a 32-bit value could be encoded in 5 bytes instead of 4, and the outgoing requests could be refused by some implementations of the SNMP protocol as invalid. With this update, a Request-ID can no longer become negative and is always encoded in 4 bytes.

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

4.112.2. RHSA-2013:0124 — Moderate: net-snmp security and bug fix update

Updated net-snmp 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 for each vulnerability from the CVE link(s) associated with each description below.

These packages provide various libraries and tools for the Simple Network Management Protocol (SNMP).

Security Fix

CVE-2012-2141

An out-of-bounds buffer read flaw was found in the net-snmp agent. A remote attacker with read privileges to a Management Information Base (MIB) subtree handled by the "extend" directive (in "/etc/snmp/snmpd.conf") could use this flaw to crash snmpd via a crafted SNMP GET request.

Bug Fix

BZ#754652, BZ#755958, BZ#822061

Devices that used certain file systems were not reported in the "HOST-RESOURCES-MIB::hrStorageTable" table. As a result, the snmpd daemon did not recognize devices using tmpfs, ReiserFS, and Oracle Cluster File System (OCFS2) file systems. This update recognizes these devices and reports them in the "HOST-RESOURCES-MIB::hrStorageTable" table.

BZ#760001

The snmptrapd (8) man page did not correctly describe how to load multiple configuration files using the "-c" option. This update describes correctly that multiple configuration files must be separated by a comma.

BZ#783892

Integers truncated from 64 to 32-bit were not correctly evaluated. As a consequence, the snmpd daemon could enter an endless loop when encoding the truncated integers to network format. This update modifies the underlying code so that snmpd correctly checks truncated 64-bit integers. Now, snmpd avoids an endless loop.

BZ#799699

snmpd did not correctly check for interrupted system calls when enumerating existing IPv6 network prefixes during startup. As a consequence, snmpd could prematurely exit when receiving a signal during this enumeration. This update checks the network prefix enumeration code for interrupted system calls. Now, snmpd no longer terminates when a signal is received.

BZ#803585

snmpd used the wrong length of COUNTER64 values in the AgentX protocol. As a consequence, snmpd could not decode two consecutive COUNTER64 values in one AgentX packet. This update uses the correct COUNTER64 size and can process two or mode COUNTER64 values in AgentX communication.

BZ#805689

snmpd ignored the "-e" parameter of the "trapsess" option in the snmpd configuration file. As a result, outgoing traps were incorrectly sent with the default EngineID of snmpd when configuring "trapsess" with an explicit EngineID. This update modifies the underlying code to send outgoing traps using the EngineID as specified in the "trapsess -e" parameter in the configuration file.

BZ#818259

snmpd did not correctly encode negative Request-IDs in outgoing requests, for example during trap operations. As a consequence, a 32-bit value could be encoded in 5 bytes instead of 4, and the outgoing requests were refused by certain implementations of the SNMP protocol as invalid. With this update, a Request-ID can no longer become negative and is always encoded in 4 bytes.

BZ#828691

snmpd ignored the port number of the "clientaddr" option when specifying the source address of outgoing SNMP requests. As a consequence, the system assigned a random address. This update allows to specify both the port number and the source IP address in the "clientaddr" option. Now, administrators can increase security with firewall rules and Security-Enhanced Linux (SELinux) policies by configuring a specific source port of outgoing traps and other requests.

BZ#830042

snmpd did not correctly process responses to internal queries when initializing monitoring enabled by the "monitor" option in the "/etc/snmp/snmpd.conf" configuration file. As a consequence, snmpd was not fully initialized and the error message "failed to run mteTrigger query" appeared in the system log 30 seconds after the snmpd startup. This update explicitly checks for responses to internal monitoring queries.

Users of net-snmp should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the update, the snmpd and snmptrapd daemons will be restarted automatically.

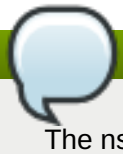
4.113. nss

4.113.1. RHBA-2012:0337 — nss and nspr bug fix and enhancement update

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

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security enabled client and server applications.

Netscape Portable Runtime (NSPR) provides platform independence for non-GUI operating system facilities.



Note

The nss-util package has been upgraded to upstream version 3.13, which provides a number of enhancements over the previous version. (BZ#788670)

The nss packages have been upgraded to upstream version 3.13, which provides a number of bug fixes and enhancements over the previous version. (BZ#788673, BZ#788964, BZ#788672)

The nspr package has been upgraded to upstream version 4.8.9, which provides a number of enhancements over the previous version. (BZ#788674)

Bug Fixes

BZ#789043

A lack of robustness flaw caused crashes in the administration server for Red Hat Directory Server because the mod_nss module made nss calls before initializing nss per documented API. With this update, nss protects itself against being called before it as been properly initialized by the caller.

BZ#786436

Previously, due to a bug in the FreeBL library, Openswan could generate a Key Exchange payload that was one byte shorter than what was required by the Diffie Hellman (DH) protocol. As a consequence, Openswan dropped connections during such payloads. With this update, the size of the payload is set to zero by default, and the Softoken module is queried for the size. Connections

are no longer dropped by Openswan in the described scenario.

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

4.113.2. RHBA-2012:0344 — nss bug fix update

Updated nss packages that fix a bug are now available for Red Hat Enterprise Linux 5 and Red Hat Enterprise Linux 6.

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security enabled client and server applications.

Bug Fix

BZ#798461, BZ#798462

Crashes were reported in the messaging daemon (qpidd) included in Red Hat Enterprise MRG after a recent update to nss. This occurred as qpidd made nss calls before initializing nss. These updated packages prevent qpidd, and other affected processes that call nss without initializing as mandated by the API, from crashing.

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

4.113.3. RHBA-2013:0081 — nss and nspr bug fix and enhancement update

Updated nss and nspr packages that fix two 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#633519

Due to errors in the Netscape Portable Runtime (NSPR) code responsible for thread synchronization, memory corruption sometimes occurred. Consequently, the web server daemon (httpd) sometimes terminated unexpectedly with a segmentation fault after making more than 1023 calls to the NSPR library. With this update, an improvement to the way NSPR frees previously allocated memory has been made and httpd no longer crashes in the scenario described.

BZ#797939

Some Network Security Services (NSS) clients call NSS without initializing first as mandated by the API and NSS did not protect itself against such improper usage. Consequently, this caused unexpected terminations on shutdown as some variables had not been properly initialized. Such crashes were reported in the messaging daemon (qpidd), included in Red Hat Enterprise MRG, after a recent update to the nss package. This occurred as qpidd made NSS calls before initializing NSS. With this update, NSS now protects itself against potential improper use by client code. As a result, NSS prevents qpidd, and other processes that may call NSS without initializing as mandated by the API, from crashing.

Enhancement

BZ#820684

The certutil tool was enhanced to support creation of Elliptic Curve (EC) key pairs on Hardware Security Modules.

All nss and nspr users should upgrade to these updated packages, which fix these bugs and add this enhancement. After installing the update, applications using NSS and NSPR must be restarted for the changes to take effect.

4.113.4. RHSA-2012:1090 — Moderate: nss and nspr security, bug fix, and enhancement update

Updated nss and nspr packages that fix two security issues, several bugs, and add various 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. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

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.

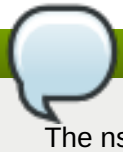
Security Fix

CVE-2012-0441

A flaw was found in the way the ASN.1 (Abstract Syntax Notation One) decoder in NSS handled zero length items. This flaw could cause the decoder to incorrectly skip or replace certain items with a default value, or could cause an application to crash if, for example, it received a specially-crafted OCSP (Online Certificate Status Protocol) response.

It was found that a Certificate Authority (CA) issued a subordinate CA certificate to its customer, that could be used to issue certificates for any name. This update renders the subordinate CA certificate as untrusted. (BZ#798533)

Note: The BZ#798533 fix only applies to applications using the NSS Builtin Object Token. It does not render the certificates untrusted for applications that use the NSS library, but do not use the NSS Builtin Object Token.



Note

The nspr package has been upgraded to upstream version 4.9.1, and the nss package has been upgraded to upstream version 3.13.5. These updates provide a number of bug fixes and enhancements over the previous versions. (BZ#834220, BZ#834219)

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.

4.114. nss_ldap

4.114.1. RHBA-2013:0085 — nss_ldap bug fix update

Updated nss_ldap packages that fix multiple bugs 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 Fixes

BZ#761281

When parsing an ldap.conf file that contained a host and a port definition, the nss_ldap "do_add_hosts()" function always created a URI starting with "ldap://" regardless of SSL being enabled. Consequently, when the response included an "ldaps://..." referral to the same server and port, the libldap library considered this to be a different scheme ("ldaps" vs. the initial "ldap") and opened new connections for each referral lookup instead of reusing the existing persistent connection. The code has been improved and now when the SSL option is enabled the initial URI will be in the format "ldaps://...". As a result, nss_ldap now correctly uses the LDAPS scheme with SSL connections.

BZ#797410

Due to a regression in the configuration parser, the "do_readline()" function did not return the correct exit code when the last line of "/etc/ldap.secret" did not contain a newline. Consequently, the nss_ldap module failed to bind to the LDAP server. With this update the parser now returns the correct exit code when parsing /etc/ldap.secret and nss_ldap works as expected in the scenario described.

BZ#835555

The nss_ldap module used to leak memory when an entry that did not exist on the remote server was requested. The memory leak has been fixed by freeing an internal search structure even in cases where the search does not finish successfully.

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

4.115. OFED

4.115.1. RHBA-2013:0106 — OFED bug fix and enhancement update

Updated OpenFabrics Alliance (*openib*) packages that upgrade the OpenFabrics Enterprise Distribution (OFED) stack, fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The OpenFabrics Enterprise Distribution (OFED) is a collection of InfiniBand and iWARP hardware diagnostic utilities, the InfiniBand fabric management daemon, the Infiniband and iWARP kernel module loader, as well as 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, and RDMA hardware support.

Note

The InfiniBand driver stack in the Red Hat Enterprise Linux 5.9 kernel has been updated to the OpenFabrics Enterprise Distribution (OFED) 1.5.4.1 stack, and this erratum updates the user space packages to work with the updated kernel. The user space packages are updated to the same level as the Red Hat Enterprise Linux 6.3 user space InfiniBand software stack with the exception that in Red Hat Enterprise Linux 5.9 we do not support InfiniBand over Ethernet (IBoE), also known as RDMA over Converged Ethernet (RoCE).

Bug Fixes

BZ#536690

IP over InfinBand (IPoIB) interfaces are artificial constructs created on top of InfiniBand RDMA devices. The **IPoIB** interface has a generated hardware MAC address. The queue pair that the interface is attached to is encoded in the hardware MAC address. However, when unloading and reloading the IPoIB module, it is likely that a different queue pair to the IPoIB queue pair will be assigned. Because the queue pair number is encoded in the MAC address of the IPoIB interface, and because it can change when the IPoIB module is unloaded and reloaded, the final MAC address of IPoIB interfaces can change. Consequently, when users created **`ifcfg-ibX`** files that specified the MAC address of the IPoIB interface, after a reload of the IPoIB kernel module, when the MAC address no longer matched, the IPoIB interface failed to be recognized as a configured interface by the network subsystem. To solve this problem, this update implements custom **`ifup-ib`** and **`ifdown-ib`** network scripts that are aware of the portion of an IPoIB's MAC address that is constant versus the portion that is subject to change. As a result, when a user reloads the IPoIB module, and when the IPoIB interface's MAC address changes, the **`ifup-ib`** and **`ifdown-ib`** scripts will properly match against the portion that did not change and recognize the interface correctly.

BZ#571779

Imperfect argument processing in the **ibv_rc_pingpong** program allowed arguments that were too large to be passed to the program. Consequently, the program terminated unexpectedly with a segmentation fault when attempting to set up transfers using large arguments. The checking of arguments in **ibv_rc_pingpong** has been strengthened. As a result, the program no longer crashes on bad arguments.

BZ#575608

Insufficient state checking in the **`ifup-ib`** script could cause it to create an invalid state on bond devices that had **IPoIB** slaves. Consequently, when the user called **`ifup`** on the IPoIB interface, and expected it to be working, the master bond device was sometimes taken down. A check to make sure that the device is not already present in the bond device before attempting to add it is now made. As a result, the device is now initialized properly.

BZ#578640

The **`libibverbs.spec`** file was missing the **`BuildRequires: valgrind-devel`** line. Consequently, the *libibverbs* package was built without **valgrind** memory allocation debugging support. The required line has been added to the spec file and the *libibverbs* package now supports valgrind memory debugging.

BZ#668913

When passed the **`-r`** flag, the **ibdiagnet** program attempted to free the same memory twice. Consequently, the program would trigger protection built into **glibc** and end the execution. The

program has been fixed to no longer attempt to free the same memory twice and as a result the program completes as expected.

BZ#772602

The **ibnodes** program is a simple shell wrapper script that calls **ibhosts** and **ibswitches**. When passed the **-h** switch to get help for the program, it passed that switch on to both **ibhosts** and **ibswitches**. Consequently, when the user ran **ibnodes -h** they saw help output for **ibhosts** and **ibswitches**. A simple help handler in the **ibnodes** program that outputs ibnodes-specific help information has been implemented and the problem no longer occurs.

BZ#773718

A race condition on handling of completion events could confuse the **ib_send_lat** test program. Consequently, the **ib_send_lat** test program sometimes terminated unexpectedly with a segmentation fault. Completion processing has now been separated into two separate queues, one for send completions and one for receive completions. As a result, out of order and unexpected completions no longer confuse the test program, nor cause crashes.

BZ#783945

An error in thread handling resulted in the **rping** binary freeing resources before all threads that accessed those resources had exited. Consequently, the **rping** binary terminated unexpectedly with a segmentation fault when attempting to access already freed resources. Thread handling has been improved to wait for all threads to exit in various locations before proceeding with freeing memory resources. As a result, the **rping** application no longer crashes on iWARP hardware in the scenario described.

BZ#846162

The **openibd** init script loaded the parent **RDS** module if configured to do so, but did not load either of the RDS transports (**TCP** and **RDMA**). RDS is non-functional without at least one transport module loaded. Consequently, the RDS protocol was listed as available, but was not usable because no suitable interfaces with a supported transport could be found. The openibd init script has been updated to always load the TCP and RDMA transports if the RDS service is configured to be enabled in **/etc/ofed/ofed.conf**. As a result, the RDS protocol is now functional and can find suitable interfaces over which to operate.

BZ#846164

Early versions of the **Qperf** application had the value for the **RDS** address family protocol value hardcoded because it was not specified via the normal system headers at the time. When the RDS protocol was accepted upstream, the preliminary address family value was changed. Qperf did not pick this change up and instead used the incorrect constant. Consequently, when Qperf thought it was attempting to open an RDS protocol socket, it was in fact attempting to open a different, unsupported socket family. This updates removes the old preliminary constant from the *qperf* sources and instead gets the constant from the kernel headers now that it is included. As a result, Qperf will open the correct socket type and operate as expected.

BZ#846574

The **ifup-ib** script did not support naming an **IPoIB** interface anything other than **ib0** or **ib1**. Consequently, it was not possible to give more meaningful names to IPoIB interfaces. The **ifup-ib** script has been updated to match against the MAC address in an **ifcfg-***[name]* file, and if the name of the device as specified in the file is not the same as the name of the device according to

the kernel, then it will use the **iproute** tools to rename the device in the kernel. As a result, it is now possible to create a file **ifcfg-mlx4_1** with a device **HWADDR=[MAC address of mlx4_1 port]**, and **DEVICE=[desired device name]** and have the ifup-ib scripts automatically rename the device to the desired device name.

BZ#847647

Reuse of the outgoing **RDS** ping sockets before the last sent package had received its **ACK** caused the **rds-ping** utility to corrupt its internal data. This happened anytime the user specified a ping interval short enough to result in there being 8 or more outstanding ping packets as there are 8 outgoing sockets used by rds-ping by default. Given that RDS ping times are often in the 20-30 msec range, any value less than 8 or so msec for the ping interval ran a reasonable chance of causing this problem. Consequently, the rds-ping utility would give erratic results and sometimes terminate unexpectedly with a segmentation fault. The rds-ping send path has been reworked to track whether or not the response packet has been received on each socket. When it is time to send the next ping, if all sockets still have outstanding pings lacking a response, the program now waits until a ping response comes back in and frees up a socket for sending again. As a result, the application now works in a reliable manner when given very short ping intervals.

BZ#847938

The **rping** program tried to give an invalid value for the **retry_count** element on newly created queue pairs. Consequently, depending on the particular hardware driver in question, the driver would either refuse to create the queue pair, causing **rping** to fail to create a connection and exit, or it would silently truncate the out-of-bounds value to a smaller value and proceed with the connection. This update changes **rping** to request a valid value for **retry_count**. As a result, regardless of hardware the connection is now accepted and works as expected.

Enhancements

BZ#787610

The *mstflint* package, which provides Mellanox firmware burning and diagnostics tools, now includes support for **Mellanox ConnectX-3** devices.

BZ#802619

The **libcxgb3** library has been updated from upstream version 1.3.0 to the latest upstream version, version 1.3.1. The libcxgb3 library provides a user space driver for **Chelsio cxgb3** hardware to be used with **libibverbs**. This update refreshes the driver for enhanced hardware support and bug fixes.

BZ#802620

The **libcxgb4** library has been updated from upstream version 1.1.1 to the latest upstream version, version 1.2.0. The libcxgb4 library provides a user space driver for **Chelsio cxgb4** hardware to be used with **libibverbs**. This update refreshes the driver for enhanced hardware support and bug fixes.

All users using Infiniband and iWARP hardware are advised to upgrade to these updated *openib* packages, which fix these bugs and add these enhancements.

4.116. openais

4.116.1. RHBA-2012:0553 — openais bug fix update

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

The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais package contains the openais executable, OpenAIS service handlers, default configuration files and an init script.

Bug Fix

BZ#817610

The syslog utility prints data to standard output as a function with a dynamic number of arguments. Previously, a logged string was passed directly as a format string, and if formatting characters were included, stack overflow or underflow could occur. This consequently caused the aisexec process to terminate unexpectedly with a segmentation fault. The underlying source code has been modified so that aisexec no longer crashes in this scenario.

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

4.116.2. RHBA-2012:0558 — openais bug fix update

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

The openais package contains the openais executable, OpenAIS service handlers, default configuration files and an init script. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services during failures.

Bug Fix

BZ#812302

OpenIAS previously performed the incorrect test of the message ID range in the update_aru() function. This could cause OpenAIS to fail to receive multicast packet transmissions with the "FAILED TO RECEIVE" error message. This update removes the incorrect test so that OpenAIS no longer fails in this scenario, and proper checks of the message ID range are performed using the fail_to_recv_const constant.

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

4.116.3. RHBA-2013:0013 — openais bug fix update

Updated openais packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The Application Interface Specification (AIS) is an API and a set of policies for developing applications that maintain services during faults. The OpenAIS Standards Based Cluster Framework is an OSI-certified implementation of the Service Availability Forum AIS. The openais package contains the openais executable, OpenAIS service handlers, default configuration files and an init script.

Bug Fixes

BZ#671575

The FAIL_TO_RECV_CONST constant specifies how many rotations of a token should be received without receiving any messages before a new configuration is formed. Previously, this constant was set to 50, which is low for most modern switch hardware. This could cause processes, such as corosync, to terminate unexpectedly. The FAIL_TO_RECV_CONST constant is now set to 2500, which prevents processes from crashing in this scenario.

BZ#794837

The syslog utility prints data to standard output as a function with a dynamic number of arguments. Previously, a logged string was passed directly as a format string, and if formatting characters were included, stack overflow or underflow could occur. This consequently caused the aisexec process to terminate unexpectedly with a segmentation fault. The underlying source code has been modified so that aisexec no longer crashes in this scenario.

BZ#806901

Previously, the range condition for the update_aru() function could cause incorrect check of message IDs. Due to this, in rare cases, the corosync utility entered the "FAILED TO RECEIVE" state, and so failed to receive multicast packets. With this update, the range value in the update_aru() function is no longer checked for; the fail_to_recv_const constant performs such checks. Now, corosync does not fail to receive packets.

BZ#810250

This update adds support for cluster hearbeat configuration through VLAN network interfaces.

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

4.117. OpenIPMI

4.117.1. RHBA-2012:1406 — OpenIPMI bug fix update

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

The OpenIPMI packages provide command-line tools and utilities to access platform information using Intelligent Platform Management Interface (IPMI). System administrators can use OpenIPMI to manage systems and to perform system health monitoring.

Bug Fix

BZ#867008

In cases of congested network or slow-responding BMC (Baseboard Management Controller), the reply operation timeout triggered the protocol command retry action. Consequently, the ipmitool utility could incorrectly process a LAN session protocol command with the reply from a previous protocol command. This update fixes handling of expected replies for each command alone and cleans up expected replies between commands. Now, the retried reply of the first command is correctly ignored while the later command, which is currently pending, is properly processed in the described scenario.

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

4.117.2. RHSA-2013:0123 — Low: OpenIPMI security, bug fix, and enhancement update

Updated OpenIPMI packages that fix one security issue, multiple 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 low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

The OpenIPMI packages provide command line tools and utilities to access platform information using

Intelligent Platform Management Interface (IPMI). System administrators can use OpenIPMI to manage systems and to perform system health monitoring.

CVE-2011-4339

It was discovered that the IPMI event daemon (ipmievd) created its process ID (PID) file with world-writable permissions. A local user could use this flaw to make the ipmievd init script kill an arbitrary process when the ipmievd daemon is stopped or restarted.

Note: This issue did not affect the default configuration of OpenIPMI as shipped with Red Hat Enterprise Linux 5.

Bug Fixes

BZ#658762

Prior to this update, the ipmitool utility first checked the IPMI hardware for Dell IPMI extensions and listed only supported commands when printing command usage like the option "ipmtool delloem help". On a non-Dell platform, the usage text was incomplete and misleading. This update lists all Dell OEM extensions in usage texts on all platforms, which allows users to check for command line arguments on non-Dell hardware.

BZ#671059, BZ#749796

Prior to this update, the ipmitool utility tried to retrieve the Sensor Data Records (SDR) from the IPMI bus instead of the Baseboard Management Controller (BMC) bus when IPMI-enabled devices reported SDR under a different owner than the BMC. As a consequence, the timeout setting for the SDR read attempt could significantly decrease the performance and no sensor data was shown. This update modifies ipmitool to read these SDR records from the BMC and shows the correct sensor data on these platforms.

BZ#740780

Prior to this update, the exit code of the "ipmitool -o list" option was not set correctly. As a consequence, "ipmitool -o list" always returned the value 1 instead of the expected value 0. This update modifies the underlying code to return the value 0 as expected.

BZ#829705

Prior to this update, the "ipmi" service init script did not specify the full path to the "/sbin/lsmod" and "/sbin/modprobe" system utilities. As a consequence, the init script failed when it was executed if PATH did not point to /sbin, for example, when running "sudo /etc/init.d/ipmi". This update modifies the init script so that it now contains the full path to lsmod and modrpobe. Now, it can be executed with sudo.

BZ#846596

Prior to this update, the ipmitool man page did not list the "-b", "-B", "-l" and "-T" options. In this update, these options are documented in the ipmitool man page.

Enhancement

BZ#797050

Updates to the Dell-specific IPMI extension: A new vFlash command, which allows users to display information about extended SD cards; a new setled command, which allows users to display the backplane LED status; improved error descriptions; added support for new hardware; and updated documentation of the ipmitool delloem commands in the ipmitool manual page.

All users of OpenIPMI are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement.

4.118. openldap

4.118.1. RHBA-2012:1071 — openldap bug fix update

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

OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. LDAP is a set of protocols for accessing directory services (usually phone book style information, but other information is possible) over the Internet, similar to the way DNS (Domain Name System) information is propagated over the Internet. The openldap packages contain configuration files, libraries, and documentation for OpenLDAP.

Bug Fix

BZ#835444

Previously, the OpenLDAP library looked up for an AAAA (IPv6) DNS record while resolving the server IP address even if IPv6 was disabled on the host, which could cause extra delays when connecting. With this update, the AI_ADDRCONFIG flag is set when resolving the remote host address. As a result, the OpenLDAP library no longer looks up for the AAAA DNS record when resolving the server IP address and IPv6 is disabled on the local system.

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

4.119. openmotif

4.119.1. RHBA-2012:0363 — openmotif bug fix update

An updated openmotif package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The openmotif package includes the Motif shared libraries needed to run applications which are dynamically linked against Motif, as well as MWM, the Motif Window Manager.

Bug Fix

BZ#799001

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.

All users of openmotif are advised to upgrade to this updated package, which fixes this bug.

4.120. openoffice.org

4.120.1. RHSA-2012:0411 — Important: openoffice.org security update

Updated openoffice.org 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(s) associated with each description below.

OpenOffice.org is an office productivity suite that includes desktop applications, such as a word processor, spreadsheet application, presentation manager, formula editor, and a drawing program. OpenOffice.org embeds a copy of Raptor, which provides parsers for Resource Description Framework (RDF) files.

Security Fix

CVE-2012-0037

An XML External Entity expansion flaw was found in the way Raptor processed RDF files. If OpenOffice.org were to open a specially-crafted file (such as an OpenDocument Format or OpenDocument Presentation file), it could possibly allow a remote attacker to obtain a copy of an arbitrary local file that the user running OpenOffice.org had access to. A bug in the way Raptor handled external entities could cause OpenOffice.org to crash or, possibly, execute arbitrary code with the privileges of the user running OpenOffice.org.

Red Hat would like to thank Timothy D. Morgan of VSR for reporting this issue.

All OpenOffice.org users are advised to upgrade to these updated packages, which contain backported patches to correct this issue. All running instances of OpenOffice.org applications must be restarted for this update to take effect.

4.120.2. RHSA-2012:0705 — Important: openoffice.org security update

Updated openoffice.org 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 important security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

OpenOffice.org is an office productivity suite that includes desktop applications, such as a word processor, spreadsheet application, presentation manager, formula editor, and a drawing program.

Security Fixes

CVE-2012-2334

An integer overflow flaw, leading to a buffer overflow, was found in the way OpenOffice.org processed an invalid Escher graphics records length in Microsoft Office PowerPoint documents. An attacker could provide a specially-crafted Microsoft Office PowerPoint document that, when opened, would cause OpenOffice.org to crash or, potentially, execute arbitrary code with the privileges of the user running OpenOffice.org.

CVE-2012-1149

Multiple integer overflow flaws, leading to heap-based buffer overflows, were found in the JPEG, PNG, and BMP image file reader implementations in OpenOffice.org. An attacker could provide a specially-crafted JPEG, PNG, or BMP image file that, when opened in an OpenOffice.org application, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

Upstream acknowledges Sven Jacobi as the original reporter of CVE-2012-2334, and Tielei Wang via Secunia SVCRP as the original reporter of CVE-2012-1149.

All OpenOffice.org users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. All running instances of OpenOffice.org applications must be restarted for this update to take effect.

4.120.3. RHSA-2012:1136 — Important: openoffice.org security update

Updated openoffice.org 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. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each description below.

OpenOffice.org is an office productivity suite that includes desktop applications, such as a word processor, spreadsheet application, presentation manager, formula editor, and a drawing program.

Security Fix

CVE-2012-2665

Multiple heap-based buffer overflow flaws were found in the way OpenOffice.org processed encryption information in the manifest files of OpenDocument Format files. An attacker could provide a specially-crafted OpenDocument Format file that, when opened in an OpenOffice.org application, would cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

Upstream acknowledges Timo Warns as the original reporter of these issues.

All OpenOffice.org users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. All running instances of OpenOffice.org applications must be restarted for this update to take effect.

4.121. openssl

4.121.1. RHSA-2012:0426 — Moderate: openssl security and bug fix update

Updated openssl packages that fix two security issues and one bug 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) 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-2012-1165

A NULL pointer dereference flaw was found in the way OpenSSL parsed Secure/Multipurpose Internet Mail Extensions (S/MIME) messages. An attacker could use this flaw to crash an application that uses OpenSSL to decrypt or verify S/MIME messages.

CVE-2012-0884

A flaw was found in the PKCS#7 and Cryptographic Message Syntax (CMS) implementations in OpenSSL. An attacker could possibly use this flaw to perform a Bleichenbacher attack to decrypt an encrypted CMS, PKCS#7, or S/MIME message by sending a large number of chosen ciphertext messages to a service using OpenSSL and measuring error response times.

This update also fixes a regression caused by the fix for CVE-2011-4619, released via RHSA-2012:0060 and RHSA-2012:0059, which caused Server Gated Cryptography (SGC) handshakes to fail.

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.

4.121.2. RHSA-2012:0518 — Important: openssl security update

Updated openssl, openssl097a, and openssl098e 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(s) 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 Fix

CVE-2012-2110

Multiple numeric conversion errors, leading to a buffer overflow, were found in the way OpenSSL parsed ASN.1 (Abstract Syntax Notation One) data from BIO (OpenSSL's I/O abstraction) inputs. Specially-crafted DER (Distinguished Encoding Rules) encoded data read from a file or other BIO input could cause an application using the OpenSSL library to crash or, potentially, execute arbitrary code.

All OpenSSL users should upgrade to these updated packages, which contain a backported patch to resolve this issue. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

4.121.3. RHSA-2012:0699 — Moderate: openssl security and bug fix update

Updated openssl packages that fix one security issue and one bug 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 for each vulnerability from the CVE link(s) 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 Fix

CVE-2012-2333

An integer underflow flaw, leading to a buffer over-read, was found in the way OpenSSL handled DTLS (Datagram Transport Layer Security) application data record lengths when using a block cipher in CBC (cipher-block chaining) mode. A malicious DTLS client or server could use this flaw to crash its DTLS connection peer.

Red Hat would like to thank the OpenSSL project for reporting this issue. Upstream acknowledges Codenomicon as the original reporter.

On Red Hat Enterprise Linux 6, this update also fixes an uninitialized variable use bug, introduced by the fix for CVE-2012-0884 (released via RHSA-2012:0426). This bug could possibly cause an attempt to create an encrypted message in the CMS (Cryptographic Message Syntax) format to fail.

All OpenSSL users should upgrade to these updated packages, which contain a backported patch to resolve these issues. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

4.122. openswan

4.122.1. RHBA-2013:0077 — openswan bug fix and enhancement update

Updated openswan packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

Openswan is a free implementation of IPsec and IKE (Internet Key Exchange) for Linux. This 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.x also supports IKEv2 (RFC4306).

Bug Fix

BZ#807772

The openswan packages have been upgraded to incorporate a number of backported patches which provide a number of bug fixes and enhancements over the previous version.

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

4.123. pam

4.123.1. RHBA-2013:0032 — pam bug fix and enhancement update

Updated pam packages that fix three bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

Pluggable Authentication Modules (PAM) provide a system to set up authentication policies without the need to recompile programs to handle authentication.

Bug Fixes

BZ#614765

Due to an error in the %post script, the /var/log/faillog and /var/log/tallylog files were truncated on PAM upgrade. Consequently, the user authentication failure records were lost. The %post script has been fixed, and the user authentication failure records are now preserved during the pam package upgrade.

BZ#768087

When the "remember" option was used, the pam_unix and pam_cracklib modules were matching usernames incorrectly while searching for the old password entries in the /etc/security/opasswd file. Due to this bug, the old password entries could be mixed; the users whose usernames were a substring of another username could have the passwords entries of another user. With this update, the string that is used to match usernames has been fixed. Now only the exact same usernames are matched and the entries about old passwords are no longer mixed in the described scenario.

BZ#824858

Prior to this update, using the pam_pwhistory module caused an error when changing user's password. It was not possible to choose any password, that was in user's password history, as a new password. With this update, root can change the password regardless of whether it is in the user's history or not.

Enhancements

BZ#551312

Prior to this update, the pam_listfile module was searching through all group entries using the getgrent command when looking for group matches. Due to this implementation, getgrent took too much time on systems using central identity servers such as LDAP for storing large number of groups. This feature has been replaced by more efficient implementation, which does not require to look up through all groups on the system. As a result, pam_listfile is now much faster in the described scenario.

BZ#675835

Previously, the pam_access module did not include the nodefgroup option. Consequently, it was impossible to differentiate between users and groups using this module. This enhancement adds backported support for the nodefgroup option of pam_access. When using this option, the user field of the entries in the access.conf file is not matched against groups on the system. The group matches have to be explicitly marked with parentheses "(" and ")".

BZ#554518

Prior to this update, when the pam_exec module ran an external command, the environment variables such as PAM_USER or PAM_HOST were not exported. This enhancement adds support for exporting environment variables, including those which contains common PAM item values from the PAM environment to the script that is executed by the pam_exec module.

BZ#809247

This update improved the pam_cracklib module, which is used to check properties of a new password entered by the user and reject it if it does not meet the specified limits. The pam_cracklib module now allows to check whether a new password contains the words from the GECOS field entries in the "/etc/passwd" file. It also allows to specify the maximum allowed number of consecutive characters of the same class (lowercase, uppercase, number, and special characters) in a password.

All pam users are advised to upgrade to these updated packages, which fix these bugs and adds these enhancements.

4.124. parted

4.124.1. RHBA-2013:0048 — parted bug fix

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

The parted packages provide tools to create, destroy, resize, move, and copy hard disk partitions. The parted program can be used for creating space for new operating systems, reorganizing disk usage, and copying data to new hard disks.

Bug Fix

BZ#750396

Prior to this update, the libparted partition_duplicate() function did not correctly copy all GPT partition flags. This update modifies the underlying code so that all flags are correctly copied.

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

4.125. pdksh

4.125.1. RHBA-2012:1193 — pdksh bug fix update

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

The pdksh package contains a public domain implementation the Korn shell (ksh-88). The ksh shell is a command interpreter intended for both interactive and shell script use.

Bug Fix

BZ#848078

Prior to this update, the pdksh binary file was installed as "/bin/pdksh" but the path written to the /etc/shells file was "/usr/bin/pdksh". As a consequence, some audit tools reported errors. This update fixes the path written to /etc/shells and audit tools no longer report errors in the described scenario.

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

4.126. perl

4.126.1. RHBA-2012:1411 — perl bug fix update

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

Perl is a high-level programming language commonly used for system administration utilities and web programming.

Bug Fix

BZ#865709

Previously, certain Perl scripts using modules, which use the overload() function in a specific way, could be impacted by a performance regression. Consequently, users could observe slower operation of such scripts after an upgrade from perl packages of version 5.8.5. This update removes an upstream patch from these perl packages that was responsible for the regression, thus preventing this bug.

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

4.127. perl-IO-Socket-SSL

4.127.1. RHBA-2012:0567 — perl-IO-Socket-SSL bug fix update

An updated perl-IO-Socket-SSL package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The perl-IO-Socket-SSL package is a 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.

Bug Fix

BZ#815335

Prior to this update, check_crl routines could, under certain circumstances, cause a segmentation fault. This update modifies the underlying code so that the correct function is now called and the check_crl routine works as expected.

All users of perl-IO-Socket-SSL are advised to upgrade to this updated package, which fixes this bug.

4.128. perl-LDAP

4.128.1. RHBA-2012:1303 — perl-LDAP bug fix update

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

The perl-LDAP package provide a collection of modules that implements a LDAP services API for Perl programs. The module may be used to search directories or perform maintenance functions such as adding, deleting, or modifying entries.

Bug Fix

BZ#858699

Previously, errors in LDAP communication occurred when the sent data was too large. Consequently, user could not send data bigger than 15,000 bytes over SSL. With this update, backported upstream patches have been provided, which modify the syswrite() call to use smaller chunks of data passed to the IO::Socket::SSL module, thus fixing this bug.

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

4.129. perl-XML-SAX

4.129.1. RHBA-2012:1184 — perl-XML-SAX bug fix update

An updated perl-XML-SAX package that fixes one bug is now available for Red Hat Enterprise Linux 5.

XML::SAX is a SAX parser access API for Perl. It includes classes and APIs required for implementing SAX drivers, along with a factory class for returning any SAX parser installed on the user's system.

Bug Fix

BZ#846814

Prior to this update, the presence of a comment in an XML file could cause the XML::SAX parser to terminate unexpectedly with an "End tag mismatch" error. This update adapts the algorithm for finding a closing tag to process comments properly. As a result, XML files that contain comments can now be parsed without errors, as expected.

All users of perl-XML-SAX are advised to upgrade to this updated package, which fixes this bug.

4.130. php

4.130.1. RHSA-2012:0546 — 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 for each vulnerability from the CVE link(s) associated with each description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fix

CVE-2012-1823

A flaw was found in the way the php-cgi executable processed command line arguments when running in CGI mode. A remote attacker could send a specially-crafted request to a PHP script that would result in the query string being parsed by php-cgi as command line options and arguments. This could lead to the disclosure of the script's source code or arbitrary code execution with the privileges of the PHP interpreter.

Red Hat is aware that a public exploit for this issue is available that allows remote code execution in affected PHP CGI configurations. This flaw does not affect the default configuration in Red Hat Enterprise Linux 5 and 6 using the PHP module for Apache httpd to handle PHP scripts.

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.

4.130.2. RHSA-2012:1045 — Moderate: php security update

Updated php 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. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fixes

CVE-2012-0057

It was discovered that the PHP XSL extension did not restrict the file writing capability of libxslt. A remote attacker could use this flaw to create or overwrite an arbitrary file that is writable by the user running PHP, if a PHP script processed untrusted eXtensible Style Sheet Language Transformations (XSLT) content.

CVE-2012-1172

Note: This update disables file writing by default. A new PHP configuration directive, "xsl.security_prefs", can be used to enable file writing in XSLT.

A flaw was found in the way PHP validated file names in file upload requests. A remote attacker could possibly use this flaw to bypass the sanitization of the uploaded file names, and cause a PHP script to store the uploaded file in an unexpected directory, by using a directory traversal attack.

CVE-2012-2336

It was discovered that the fix for CVE-2012-1823, released via RHSA-2012:0546, did not properly filter all php-cgi command line arguments. A specially-crafted request to a PHP script could cause the PHP interpreter to output usage information that triggers an Internal Server Error.

CVE-2012-0789

A memory leak flaw was found in the PHP strtotime() function call. A remote attacker could possibly use this flaw to cause excessive memory consumption by triggering many strtotime() function calls.

CVE-2011-4153

It was found that PHP did not check the zend_strndup() function's return value in certain cases. A remote attacker could possibly use this flaw to crash a PHP application.

All php users should upgrade to these updated packages, which contain backported patches to resolve these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.131. php53

4.131.1. RHSA-2012:0547 — 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 for each vulnerability from the CVE link(s) associated with each description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fix

CVE-2012-1823

A flaw was found in the way the php-cgi executable processed command line arguments when running in CGI mode. A remote attacker could send a specially-crafted request to a PHP script that would result in the query string being parsed by php-cgi as command line options and arguments. This could lead to the disclosure of the script's source code or arbitrary code execution with the privileges of the PHP interpreter.

Red Hat is aware that a public exploit for this issue is available that allows remote code execution in affected PHP CGI configurations. This flaw does not affect the default configuration using the PHP module for Apache httpd to handle PHP scripts.

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.

4.131.2. RHSA-2012:1047 — Moderate: php53 security update

Updated php53 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. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fixes

CVE-2012-0057

It was discovered that the PHP XSL extension did not restrict the file writing capability of libxslt. A remote attacker could use this flaw to create or overwrite an arbitrary file that is writable by the user running PHP, if a PHP script processed untrusted eXtensible Style Sheet Language Transformations (XSLT) content.

CVE-2012-1172

Note: This update disables file writing by default. A new PHP configuration directive, "xsl.security_prefs", can be used to enable file writing in XSLT.

A flaw was found in the way PHP validated file names in file upload requests. A remote attacker could possibly use this flaw to bypass the sanitization of the uploaded file names, and cause a PHP script to store the uploaded file in an unexpected directory, by using a directory traversal attack.

CVE-2012-2386

Multiple integer overflow flaws, leading to heap-based buffer overflows, were found in the way the PHP phar extension processed certain fields of tar archive files. A remote attacker could provide a specially-crafted tar archive file that, when processed by a PHP application using the phar extension, could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running PHP.

CVE-2010-2950

A format string flaw was found in the way the PHP phar extension processed certain PHAR files. A remote attacker could provide a specially-crafted PHAR file, which once processed in a PHP application using the phar extension, could lead to information disclosure and possibly arbitrary code execution via a crafted phar:// URI.

CVE-2012-2143

A flaw was found in the DES algorithm implementation in the crypt() password hashing function in PHP. If the password string to be hashed contained certain characters, the remainder of the string was ignored when calculating the hash, significantly reducing the password strength.

CVE-2012-2336

Note: With this update, passwords are no longer truncated when performing DES hashing. Therefore, new hashes of the affected passwords will not match stored hashes generated using vulnerable PHP versions, and will need to be updated.

It was discovered that the fix for CVE-2012-1823, released via RHSA-2012:0547, did not properly filter all php-cgi command line arguments. A specially-crafted request to a PHP script could cause the PHP interpreter to execute the script in a loop, or output usage information that triggers an Internal Server Error.

CVE-2012-0789

A memory leak flaw was found in the PHP strtotime() function call. A remote attacker could possibly use this flaw to cause excessive memory consumption by triggering many strtotime() function calls.

CVE-2011-4153

It was found that PHP did not check the zend_strndup() function's return value in certain cases. A remote attacker could possibly use this flaw to crash a PHP application.

Upstream acknowledges Rubin Xu and Joseph Bonneau as the original reporters of CVE-2012-2143.

All php53 users should upgrade to these updated packages, which contain backported patches to resolve these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

4.132. pidgin

4.132.1. RHSA-2012:1102 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) 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-2012-1178

A flaw was found in the way the Pidgin MSN protocol plug-in processed text that was not encoded in UTF-8. A remote attacker could use this flaw to crash Pidgin by sending a specially-crafted MSN message.

CVE-2012-2318

An input validation flaw was found in the way the Pidgin MSN protocol plug-in handled MSN notification messages. A malicious server or a remote attacker could use this flaw to crash Pidgin by sending a specially-crafted MSN notification message.

CVE-2012-3374

A buffer overflow flaw was found in the Pidgin MXit protocol plug-in. A remote attacker could use this flaw to crash Pidgin by sending a MXit message containing specially-crafted emoticon tags.

Red Hat would like to thank the Pidgin project for reporting the CVE-2012-3374 issue. Upstream acknowledges Ulf Härnhammar as the original reporter of CVE-2012-3374.

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.

4.133. piranha

4.133.1. RHBA-2013:0065 — piranha bug fix update

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

Piranha provides high-availability and load balancing services for Red Hat Enterprise Linux. The piranha packages contains various tools to administer and configure the Linux Virtual Server (LVS), as well as the heartbeat and failover components. LVS is a dynamically-adjusted kernel routing mechanism that provides load balancing, primarily for Web and FTP servers.

Bug Fixes

BZ#786364

Previously, the lvsd daemon did not correctly identify the existence of a new virtual server when re-reading the configuration file. As a consequence, the lvsd daemon could terminate unexpectedly with a segmentation fault when the pulse service was reloaded. With this update, the lvsd daemon correctly determines if a virtual server has been added to the configuration file when the pulse service is reloaded.

BZ#739223

Previously, the lvsd daemon exited if a nanny process encountered an error as a result of executing the ipvsadm command to add or remove a real server. If a nanny process attempted to delete a real server that was not defined for a virtual service, or if a nanny process attempted to add a real server that was already defined for a virtual service, nanny encountered an error from ipvsadm and exited abnormally. With this update, a nanny process does not exit if it fails to add or remove a real server.

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

4.134. pirut

4.134.1. RHBA-2013:0069 — pirut bug fix update

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

The pirut (Package Install, Remove, and Update Tool) packages provide a set of graphical tools for managing software.

Bug Fix

BZ#472606

When pirut was used to edit a repository that did not have a ".repo" file but was instead provided by a yum plug-in, such as RHN, pirut terminated unexpectedly. This update provides a patch that ensures an error message is displayed for repositories that cannot be edited and pirut no longer crashes in the described scenario.

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

4.135. pm-utils

4.135.1. RHBA-2012:1145 — pm-utils bug fix update

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

The pm-utils packages contain a set of utilities and scripts for tasks related to power management.

Bug Fixes

BZ#481811

Prior to this update, the pm-utils set listed files without listing the directories for those files. As a consequnce, pm-utils only created but did not own the directories "/usr/lib/pm-utils/bin", "/usr/lib/pm-utils/power.d," and "/usr/lib/pm-utils/sleep.d". This update modifies pm-utils so that all directories are correctly listed in the package. Now, pm-utils owns the created directories.

BZ#675268

Prior to this update, the x86emu code could cause problems for certain hardware. As a consequence, systems that used NVIDIA Quadro FX 1700 video cards and the nv driver did not correctly resume after suspending the system. This update modifies the x86emu code so that all systems resume as expected.

BZ#817421

Prior to this update, the RPM description contained wrong product names. This update removes all wrong information.

All users of pm-utils are advised to upgrade to these updated packages, which fix these bugs.

4.136. postfix

4.136.1. RHBA-2013:0054 — postfix bug fix and enhancement update

Updated postfix packages that fix multiple bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

The postfix packages provide a Mail Transport Agent (MTA), which supports protocols like LDAP, SMTP AUTH (SASL), and TLS.

Bug Fixes

BZ#251677

Prior to this update, upstream example scripts were not included. This update adds these upstream example scripts to the postfix package.

BZ#474541

Prior to this update, the recipient duplicate elimination did not work correctly. As a consequence, users with multiple virtual aliases could receive multiple copies of emails. This update modifies the underlying code so that the recipient duplicate elimination will work as expected if the "enable_original_recipient" configuration option is set to "no". Now, users will no longer receive multiple copies of emails.

BZ#514948

Prior to this update, the postconf documentation contained ambiguous information about "reject_invalid_helo_hostname" restrictions. This update modifies the postconf documentation and the "reject_invalid_helo_hostname" parameter is now documented without ambiguity .

BZ#617069

Prior to this update, the milter (mail filter) communication failed for headers that are larger than 64 kB. Further milter processing of the email was blocked. Now, this update modifies the underlying code so that the long headers are truncated to 60000 characters or less before milter processing. Now, milter processes these large headers as expected.

BZ#645348

Prior to this update, the postfix init script looked for any process named "master" when checking whether the postfix daemon was running. As a consequence, the script could be tricked by any other process named "master", which could lead to problems. This update modifies the init script to check for the process ID (PID) which is more robust.

BZ#664627

Prior to this update, the manual pages for the command line tools "mailq", "newaliases", "sendmail" and "aliases" were not supported by alternatives. As a consequence, these man pages could not be displayed. This update adds support for these manual pages to the alternatives list.

BZ#766499

Prior to this update, the biff notification code did not set the FD_CLOEXEC file descriptor flag on created UDP sockets. As a consequence, the postfix agent could leak file descriptors (FD) to the local delivery agent (LDA) and to other processes spawned by LDA. This update modifies the underlying code to set the FD_CLOEXEC as expected.

Enhancement

BZ#502412

Prior to this update, the postfix agent did not support MySQL. This update adds MySQL support to postfix.

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

4.137. postgresql

4.137.1. RHSA-2012:0677 — Moderate: postgresql security update

Updated postgresql 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

PostgreSQL is an advanced object-relational database management system (DBMS).

Security Fixes

CVE-2012-0868

The pg_dump utility inserted object names literally into comments in the SQL script it produces. An unprivileged database user could create an object whose name includes a newline followed by an SQL command. This SQL command might then be executed by a privileged user during later restore of the backup dump, allowing privilege escalation.

CVE-2012-0866

CREATE TRIGGER did not do a permissions check on the trigger function to be called. This could possibly allow an authenticated database user to call a privileged trigger function on data of their choosing.

All PostgreSQL users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. If the postgresql service is running, it will be automatically restarted after installing this update.

4.137.2. RHSA-2012:0678 — Moderate: postgresql and postgresql84 security update

Updated postgresql84 and postgresql packages that fix three security issues are now available for Red Hat Enterprise Linux 5 and 6 respectively.

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 for each vulnerability from the CVE link(s) associated with each description below.

PostgreSQL is an advanced object-relational database management system (DBMS).

Security Fixes

CVE-2012-0868

The pg_dump utility inserted object names literally into comments in the SQL script it produces. An unprivileged database user could create an object whose name includes a newline followed by an SQL command. This SQL command might then be executed by a privileged user during later restore of the backup dump, allowing privilege escalation.

CVE-2012-0867

When configured to do SSL certificate verification, PostgreSQL only checked the first 31 characters of the certificate's Common Name field. Depending on the configuration, this could allow an attacker to impersonate a server or a client using a certificate from a trusted Certificate Authority issued for a different name.

CVE-2012-0866

CREATE TRIGGER did not do a permissions check on the trigger function to be called. This could possibly allow an authenticated database user to call a privileged trigger function on data of their choosing.

These updated packages upgrade PostgreSQL to version 8.4.11, which fixes these issues as well as several data-corruption issues and lesser non-security issues. Refer to the PostgreSQL Release Notes for a full list of changes:

http://www.postgresql.org/docs/8.4/static/release.html

All PostgreSQL users are advised to upgrade to these updated packages, which correct these issues. If the postgresql service is running, it will be automatically restarted after installing this update.

4.137.3. RHSA-2012:1036 — Moderate: postgresql security update

Updated postgresql 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 for each vulnerability from the CVE link(s) associated with each description below.

PostgreSQL is an advanced object-relational database management system (DBMS).

Security Fix

CVE-2012-2143

A flaw was found in the way the crypt() password hashing function from the optional PostgreSQL pgcrypto contrib module performed password transformation when used with the DES algorithm. If the password string to be hashed contained the 0x80 byte value, the remainder of the string was ignored when calculating the hash, significantly reducing the password strength. This made brute-force guessing more efficient as the whole password was not required to gain access to protected resources.

Note: With this update, the rest of the string is properly included in the DES hash; therefore, any previously stored password values that are affected by this issue will no longer match. In such cases, it will be necessary for those stored password hashes to be updated.

Upstream acknowledges Rubin Xu and Joseph Bonneau as the original reporters of this issue.

All PostgreSQL users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. If the postgresql service is running, it will be automatically restarted after installing this update.

4.137.4. RHSA-2012:1037 — Moderate: postgresql and postgresql84 security update

Updated postgresql84 and postgresql packages that fix two security issues are now available for Red Hat Enterprise Linux 5 and 6 respectively.

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 for each vulnerability from the CVE link(s) associated with each description below.

PostgreSQL is an advanced object-relational database management system (DBMS).

Security Fixes

CVE-2012-2143

A flaw was found in the way the crypt() password hashing function from the optional PostgreSQL pgcrypto contrib module performed password transformation when used with the DES algorithm. If the password string to be hashed contained the 0x80 byte value, the remainder of the string was ignored when calculating the hash, significantly reducing the password strength. This made brute-force guessing more efficient as the whole password was not required to gain access to protected resources.

CVE-2012-2655

Note: With this update, the rest of the string is properly included in the DES hash; therefore, any previously stored password values that are affected by this issue will no longer match. In such cases, it will be necessary for those stored password hashes to be updated.

A denial of service flaw was found in the way the PostgreSQL server performed a user privileges check when applying SECURITY DEFINER or SET attributes to a procedural language's (such as PL/Perl or PL/Python) call handler function. A non-superuser database owner could use this flaw to cause the PostgreSQL server to crash due to infinite recursion.

Upstream acknowledges Rubin Xu and Joseph Bonneau as the original reporters of the CVE-2012-2143 issue.

These updated packages upgrade PostgreSQL to version 8.4.12, which fixes these issues as well as several non-security issues. Refer to the PostgreSQL Release Notes for a full list of changes:

http://www.postgresql.org/docs/8.4/static/release.html

All PostgreSQL users are advised to upgrade to these updated packages, which correct these issues. If the postgresql service is running, it will be automatically restarted after installing this update.

4.137.5. RHSA-2012:1263 — Moderate: postgresql and postgresql84 security update

Updated postgresql84 and postgresql packages that fix two security issues are now available for Red Hat Enterprise Linux 5 and 6 respectively.

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 for each vulnerability from the CVE link(s) associated with each description below.

PostgreSQL is an advanced object-relational database management system (DBMS).

Security Fixes

CVE-2012-3488

It was found that the optional PostgreSQL xml2 contrib module allowed local files and remote URLs to be read and written to with the privileges of the database server when parsing Extensible Stylesheet Language Transformations (XSLT). An unprivileged database user could use this flaw to read and write to local files (such as the database's configuration files) and remote URLs they would otherwise not have access to by issuing a specially-crafted SQL query.

CVE-2012-3489

It was found that the "xml" data type allowed local files and remote URLs to be read with the privileges of the database server to resolve DTD and entity references in the provided XML. An unprivileged database user could use this flaw to read local files they would otherwise not have access to by issuing a specially-crafted SQL query. Note that the full contents of the files were not returned, but portions could be displayed to the user via error messages.

Red Hat would like to thank the PostgreSQL project for reporting these issues. Upstream acknowledges Peter Eisentraut as the original reporter of CVE-2012-3488, and Noah Misch as the original reporter of CVE-2012-3489.

These updated packages upgrade PostgreSQL to version 8.4.13. Refer to the PostgreSQL Release Notes for a list of changes:

http://www.postgresql.org/docs/8.4/static/release-8-4-13.html

All PostgreSQL users are advised to upgrade to these updated packages, which correct these issues. If the postgresql service is running, it will be automatically restarted after installing this update.

4.137.6. RHSA-2012:1264 — Moderate: postgresql security update

Updated postgresql 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 for each vulnerability from the CVE link(s) associated with each description below.

PostgreSQL is an advanced object-relational database management system (DBMS).

Security Fix

CVE-2012-3488

It was found that the optional PostgreSQL xml2 contrib module allowed local files and remote URLs to be read and written to with the privileges of the database server when parsing Extensible Stylesheet Language Transformations (XSLT). An unprivileged database user could use this flaw to read and write to local files (such as the database's configuration files) and remote URLs they would otherwise not have access to by issuing a specially-crafted SQL query.

Red Hat would like to thank the PostgreSQL project for reporting this issue. Upstream acknowledges Peter Eisentraut as the original reporter.

All PostgreSQL users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. If the postgresql service is running, it will be automatically restarted after installing this update.

4.138. ppc64-utils

4.138.1. RHBA-2012:0691 — ppc64-utils bug fix update

Updated ppc64-utils packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The ppc64-utils packages are a collection of utilities for Linux running on 64-bit PowerPC platform.

Bug Fix

BZ#821850

Previously, due to errors in the source code, the lparstat utility displayed incorrect values for the "smt", "ent" and "lcpu" items, and undefined values (XXX) for the "entc" and "phint" items. The underlying source code has been modified so that correct values are now displayed when running lparstat.

All users of ppc64-utils are advised to upgrade to these updated packages, which fix this bug.

4.139. procps

4.139.1. RHBA-2013:0062 — procps bug fix and enhancement update

Updated procps packages that fix several bugs and add one enhancement 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#598561

Due to an inaccurate internal evaluation of the CPU utilization, the "ps --sort" command did not work as expected in some cases. Consequently, some of the values in the final sorted sequence were in an incorrect order. This bug has been fixed and these values are sorted correctly in the described scenario.

BZ#730724

Prior to this update, the description of the SWAP field in the top(1) man page could be misleading and confusing. The man page has been fixed by using the SWAP field description from the man page of the successor project procps-ng.

BZ#757734

Descriptions for some of the top command switches were missing in the top(1) man page. Switches "-m", "-M", and "-V", which represent sorting by memory usage, memory units detection, and version/help, respectively, have been added to these updated procps packages.

BZ#839340

Previously, values shown in the "si" and "so" columns were always zero for the "m" or "M" conversion units. The evaluation has been modified to prevent losses of the arithmetic precision and zero values no longer appears in this situation.

Enhancement

BZ#586742

This update introduces a new enhancement in using of the "w" command. Users can switch the value shown in the FROM field to represent IP addresses instead of hostnames. This behavior can be achieved with the "-i" switch.

All users of procps are advised to upgrade to these updated packages that fix these bugs and add this enhancement.

4.140. psmisc

4.140.1. RHBA-2013:0118 — psmisc bug fix update

Updated psmisc packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The psmisc package contains the pstree, killall, and fuser utilities to manage system processes.

Bug Fixes

BZ#479345

Prior to this update, the fuser utility incorrectly used the "/proc/net/tcp" socket table to list processes. As a consequence, the fuser tool did not list processes that use a UDP port as expected. This update modifies the underlying code to parse the correct "/proc/net/udp" socket table, and fuser now lists processes for UDP ports as expected.

BZ#666213

Prior to this update, memory was not correctly allocated. As a consequence, the "killall -g" option could fail to kill a process group. This update modifies the memory allocation. Now, the killall utility works as expected.

BZ#693476

Prior to this update, IPv6 addresses were not correctly handled. As a consequence, the fuser command could return empty output for IPv6 sockets. This update modifies the code to handle IPv6 addresses as expected. Now, IPv6 sockets are identified correctly.

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

4.141. python

4.141.1. RHBA-2013:0045 — python bug fix and enhancement update

Updated python packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC).

Bug Fixes

BZ#573782

Prior to this update, calling the logging.config.fileConfig() function failed when the logging handlers already existed. Consequently, a KeyError occured in the atexit() call to the logging.shutdown() function. With this update, a fix has been added into logging.config.fileConfig() in order to lose previously existing handlers. As a result, the KeyError no longer occurs.

BZ#638514

IDLE is an integrated development environment for Python. With this update, support to run multiple instances of IDLE on a server has been added. As a result, multiple users can now use IDLE at the same time.

BZ#640523

Previously, the os.chown() function failed on 32-bit architectures when the UID and GID parameters contained numeric values greater than 2147483647 (0x7fffffff). Consequently, an error occurred with the following message:

OverflowError: signed integer is greater than maximum

This bug has been fixed and the os.chown function now handles larger identification numbers correctly.

BZ#822072

Previously, the fcntl.ioctl() function failed on 32-bit architectures when the op parameter contained a numeric value greater than 2147483647 (0x7fffffff). Consequently, an error occurred with the following message:

OverflowError: signed integer is greater than maximum

This bug has been fixed and the fcntl.ioctl function now handles larger request codes correctly.

BZ#701277

Due to a flaw in the Makefile.pre.in file, occasional compilation or link errors appeared when Python was rebuilt on systems with more than one CPU core. This bug has been fixed, and Python can now be rebuilt on multiple-core processing units without the aforementioned errors.

BZ#701569

Previously, a memory leak occurred when Python was used with the _japanese_codecs module

Previously, a memory leak occurred when Python was used with the _japanese_codecs module. This bug has been fixed, and the memory leak no longer occurs in the described scenario.

Enhancement

BZ#644661

The gdb debugger has been enhanced to allow more effective debugging of Python code. The added hooks enable gdb to display human-readable representations of Python objects within the process being debugged. As a result, backtraces involving Python are now easier to read, and the new hooks enhance the effectiveness of the debugging process.

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

4.141.2. RHSA-2012:0745 — Moderate: python security update

Updated python 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. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Python is an interpreted, interactive, object-oriented programming language.

Security Fixes

CVE-2012-1150

A denial of service flaw was found in the implementation of associative arrays (dictionaries) in Python. An attacker able to supply a large number of inputs to a Python application (such as HTTP POST request parameters sent to a web application) that are used as keys when inserting data into an array could trigger multiple hash function collisions, making array operations take an excessive amount of CPU time. To mitigate this issue, randomization has been added to the hash function to reduce the chance of an attacker successfully causing intentional collisions.

Note: The hash randomization is not enabled by default as it may break applications that incorrectly depend on dictionary ordering. To enable the protection, the new "PYTHONHASHSEED" environment variable or the Python interpreter's "-R" command line option can be used. Refer to the python(1) manual page for details.

The RHSA-2012:0731 expat erratum must be installed with this update, which adds hash randomization to the Expat library used by the Python pyexpat module.

CVE-2011-4940

A flaw was found in the way the Python SimpleHTTPServer module generated directory listings. An attacker able to upload a file with a specially-crafted name to a server could possibly perform a cross-site scripting (XSS) attack against victims visiting a listing page generated by SimpleHTTPServer, for a directory containing the crafted file (if the victims were using certain web browsers).

CVE-2011-4944

A race condition was found in the way the Python distutils module set file permissions during the creation of the .pypirc file. If a local user had access to the home directory of another user who is running distutils, they could use this flaw to gain access to that user's .pypirc file, which can contain usernames and passwords for code repositories. (CVE-2011-4944)

Red Hat would like to thank oCERT for reporting CVE-2012-1150. oCERT acknowledges Julian Wälde and Alexander Klink as the original reporters of CVE-2012-1150.

All Python users should upgrade to these updated packages, which contain backported patches to correct these issues.

4.142. python-iniparse

4.142.1. RHBA-2012:1128 — python-iniparse bug fix update

An updated python-iniparse package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The python-iniparse package contains an INI parser for Python which is API-compatible with the standard library's ConfigParser, preserves structure of INI files (order of sections and options, indentation, comments, and blank lines is preserved when data is updated), and is more convenient to use.

Bug Fix

BZ#753891

Due to errors in the defaults() method, python-iniparse failed with a traceback and the "ValueError: too many values to unpack" message was printed when using the method. The underlying source code has been revised, and the traceback no longer occurs when the defaults() method is used.

All users of python-iniparse are advised to upgrade to this updated package, which fixes this bug.

4.143. python-rhsm

4.143.1. RHBA-2013:0039 — python-rhsm bug fix update

Updated python-rhsm packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The python-rhsm packages provide a library for communicating with the representational state transfer (REST) interface of Red Hat's subscription and content service. The Subscription Management tools use this interface to manage system entitlements, certificates, and content access.

Bug Fixes

BZ#806958, BZ#830767, BZ#842885

Prior to this update, the python-rhsm library used unimplemented methods in certain error classes. As a consequence, messages contained a traceback obscuring actual error messages. This update implements the missing methods in the error classes. Now, the error message is reported as expected.

BZ#833537

Prior to this update, malformed requests were sent to the content delivery network (CDN). As a consequence, clients could not get a list of releases. This update modifies the underlying code to format the requests to CDN as expected. Now, clients can get a list of releases.

BZ#834108

Prior to this update, the httplib library used the default timeout setting of several minutes. As a consequence, clients that used the python-rhsm library appeared to be suspended. This update shortens the default setting for the timeout to 60 seconds.

BZ#848742

Prior to this update, the python-rhsm library did not support arbitrary bit length certificate serial numbers. As a consequence, certificates could be created with incorrect file names. This update supports arbitrary length certificate serial numbers to ensure that certificates are created with the correct file name.

BZ#851644

Prior to this update, the python-rhsm library did not decode logging messages using the Japanese locale as expected. As a consequence, python-rhsm logged tracebacks instead of messages. This update configures python-rhsm to handle messages in the Japanese locale correctly.

BZ#857426

Prior to this update, post data was set as "None" due to an invalid "if" statement. As a consequence, python-rhsm failed to set an empty JSON structure as the body of the request. This update modifies the "if" statement to explicitly check that the data is not "None". Now, empty mapping of hypervisors can pass as expected and is correctly sent to candlepin.

All users of python-rhsm are advised to upgrade to these updated packages, which fix these bugs.

4.144. qt

4.144.1. RHBA-2012:1176 — qt bug fix update

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

The qt packages contain a software toolkit that simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System.

Bug Fix

BZ#758386

When building multilib RPM packages, Qt's moc preprocessor inserted different timestamps in their source files. As a consequence, attempting to install debuginfo multilib packages failed because of conflicts between the packages. With this update, the timestamp-insertion code has been removed, so that the source files are identical and multilib packages can be installed as expected.

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

4.145. quagga

4.145.1. RHBA-2013:0050 — quagga bug fix update

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

The quagga packages contain Quagga, the free network-routing software suite that manages TCP/IP based protocols. Quagga supports the BGP4, BGP4+, OSPFv2, OSPFv3, RIPv1, RIPv2, and RIPng protocols, and is intended to be used as a Route Server and Route Reflector.

Bug Fixes

BZ#528583

Previously, several function declarations were missing in the zebra.h header file. As a consequence, a zebra server terminated unexpectedly with a segmentation fault when commands, such as "show ip protocol", calling these functions were issued on the zebra server. With this update, the missing function declarations have been added and zebra servers no longer crash in this scenario.

BZ#604620

Previously on system update, Quagga marked obsolete any other routing packages that provide the same functionality as Quagga, such as the bird package that provides a TCP/IP routing daemon. Consequently, such packages were removed from the system. With this update, the quagga spec file has been modified so that it no longer obsoletes other routing packages.

BZ#508800

Previously, Quagga init scripts did not locate PID files of Quagga daemons correctly. Consequently, these PID files were not removed during service shutdown. With this update, Quagga init scripts have been modified to locate the respective PID files correctly and the PID files now no longer remain on the system after the service is stopped.

BZ#716324

Previously, Quagga init scripts ignored the QCONFDIR variable specified in the /etc/sysconfig/quagga file and used an explicit path to the configuration files instead. This could cause problems if the location of the configuration changed. This update modifies Quagga init scripts to use the QCONFDIR variable as expected.

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

4.146. quota

4.146.1. RHSA-2013:0120 — Low: quota security and bug fix update

An updated quota package that fixes one security issue and multiple 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 for each vulnerability from the CVE link(s) associated with each description below.

The quota package provides system administration tools for monitoring and limiting user and group disk usage on file systems.

Security Fix

CVE-2012-3417

It was discovered that the rpc.rquotad service did not use tcp_wrappers correctly. Certain hosts access rules defined in "/etc/hosts.allow" and "/etc/hosts.deny" may not have been honored, possibly allowing remote attackers to bypass intended access restrictions.

This issue was discovered by the Red Hat Security Response Team.

Bug Fixes

BZ#667360

Prior to this update, values were not properly transported via the remote procedure call (RPC) and interpreted by the client when querying the quota usage or limits for network-mounted file systems if the quota values were 2^32 kilobytes or greater. As a consequence, the client reported mangled values. This update modifies the underlying code so that such values are correctly interpreted by the client.

BZ#680429

Prior to this update, warnquota sent messages about exceeded quota limits from a valid domain name if the warnquota tool was enabled to send warning e-mails and the superuser did not change the default warnquota configuration. As a consequence, the recipient could reply to invalid addresses. This update modifies the default warnquota configuration to use the reserved example.com. domain. Now, warnings about exceeded quota limits are sent from the reserved domain that inform the superuser to change to the correct value.

BZ#689822

Previously, quota utilities could not recognize the file system as having quotas enabled and refused to operate on it due to incorrect updating of /etc/mtab. This update prefers /proc/mounts to get a list of file systems with enabled quotas. Now, quota utilities recognize file systems with enabled quotas as expected.

BZ#831520

Prior to this update, the setquota(8) tool on XFS file systems failed to set disk limits to values greater than 2^31 kilobytes. This update modifies the integer conversion in the setquota(8) tool to use a 64-bit variable big enough to store such values.

All users of quota are advised to upgrade to this updated package, which contains backported patches to resolve these issues.

4.147. redhat-release

4.147.1. RHEA-2013:0021 — redhat-release enhancement update

A new redhat-release package is now available for Red Hat Enterprise Linux 5.9.

The redhat-release package contains licensing information regarding, and identifies the installed version of, Red Hat Enterprise Linux.

This new package reflects changes made for the release of Red Hat Enterprise Linux 5.9.

Users of Red Hat Enterprise Linux 5.9 are advised to install this new package.

4.148. redhat-release-notes

4.148.1. RHEA-2013:0109 — redhat-release-notes enhancement update

An updated redhat-release-notes package is now available for Red Hat Enterprise Linux 5.9 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 5.9 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 5.9.

The online Red Hat Enterprise Linux 5.9 Release Notes, which are located online at https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/5/h tml-single/5.9_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.

4.149. rgmanager

4.149.1. RHBA-2012:1044 — 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 provides the ability to create and manage high-availability server applications in the event of system downtime.

Bug Fix

BZ#827390

The filesystem and clusterfs resource agents were, in some cases, unable to unmount file systems that were exported using the nfsd utility. This update adds a new configuration option, "nfsrestart", as a workaround which ensures that the system is successfully unmounted. This new option is not compatible with the nfsserver resource agent, and requires the "force_unmount" option to be enabled.

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

4.149.2. RHBA-2012:1092 — 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 provides the ability to create and manage high-availability server applications in the event of system downtime.

Bug Fix

BZ#839195

Under rare conditions, rgmanager could attempt to free memory that had previously been freed. When this occurred, rgmanager terminated unexpectedly with a segmentation fault. This bug has been fixed and rgmanager no longer attempts to free previously-freed memory.

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

4.149.3. RHBA-2012:1230 — 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 allows to create and manage high-availability server applications in the event of system downtime.

Bug Fix

BZ#852865

If the contents of the /proc/mounts file changed during a status check operation of the file system resource agent, the status check could incorrectly detect that a mount was missing. Consequently, a healthy service could have incorrectly be marked as having failed. This bug has been fixed and rgmanager's file system resource agent no longer reports false failures in the described scenario.

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

4.149.4. RHBA-2012:1333 — 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 allows to create and manage high-availability server applications in the event of system downtime.

Bug Fix

BZ#859999

Due to a regression in the filesystem resource agent as part of the bug fix related to reading the /proc/mounts file, the filesystem resource agent status operations failed if the name of a file system resource contained the "/" character. This bug has been fixed and resources with "/" in their name no longer cause rgmanager to report failure for status operations.

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

4.149.5. RHBA-2012:1513 — 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 allows to create and manage high-availability server applications in the event of system downtime.

Bug Fix

BZ#876962

When rgmanager received a remote start message for a particular service while already in the process of starting that service locally, a deadlock could occur. This sometimes happened during recovery of a service that had failed its start operation. This bug has been fixed and rgmanager works as expected.

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

4.149.6. RHBA-2013:0026 — rgmanager bug fix update

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

The rgmanager packages contain the Red Hat Resource Group Manager, which provides the ability to create

and manage high-availability server applications in the event of system downtime.

Bug Fixes

BZ#693855

A mirror device failure during the relocation of the High Availability LVM service (HA-LVM) could cause, under certain circumstances, the service to fail. This bug has been fixed and now the mirror device failure no longer affects the HA-LVM service in such a case.

BZ#723819

The orainstance.sh resource agent did not detect all startup failures properly. The underlying source code has been modified and all failures are now detected correctly.

BZ#756180

LVM resource agent could not update logical volume tags if there were missing physical volumes. This bug has been fixed and the logical volume tags are forcibly removed if the physical volumes are missing.

BZ#769730

If the cman service was stopped while the rgmanager service was running, rgmanager sometimes exited uncleanly without releasing its Distributed Lock Manager (DLM) lock space. Consequently, it was impossible to shut down rgmanager and cman. Now if the user mistakenly attempts to stop cman service while rgmanager is still running, rgmanager no longer stops in this situation.

BZ#773372

If the /etc/lvm/lvm.conf file was changed after the last initrd (initial ramdisk) rebuild, the LVM resource agent failed. This agent has been modified to generate a warning message and no longer fails in such a case.

BZ#789366

If a service with a relocate failover policy failed and the relocation operation failed as well, the service could be restarted locally. Due to an error in the source code, the service afterwards stopped, even if the local restart succeeded. This error has been fixed, and these services no longer stop after a successful local restart.

BZ#819595

When the root file system was full, rgmanager randomly killed applications when trying to force-unmount. The underlying source code has been modified and applications are stopped instead of killed in this case.

BZ#820632

Under rare conditions, rgmanager attempted to free memory that had been previously freed. As a consequence, rgmanager terminated unexpectedly with a segmentation fault. This bug has been fixed and rgmanager no longer attempts to free previously-freed memory.

BZ#834459

When rgmanager received a remote start message for a particular service while already in the process of starting that service locally, a deadlock could occur. This sometimes happened during recovery of a service that had failed its start operation. This bug has been fixed and rgmanager works as expected.

BZ#847125

If the contents of the /proc/mounts file changed during a status check operation of the file system resource agent, the status check could incorrectly detect that a mount was missing and mark a service as failed. This bug has been fixed and rgmanager's file system resource agent no longer reports false failures in the described scenario.

Enhancements

BZ#819494

A new "prefer_interface" parameter has been added to the rgmanager ip.sh resource agent. This parameter is used for adding an IP address to a particular network interface if a cluster node has multiple active interfaces that have IP addresses on the same subnetwork.

BZ#822066

In some cases, "fs unmount" command and clustersfs resource agents were unable to unmount the file systems which were exported by the nfsd utility. The new nfsrestart option to enable a last resort workaround prior to failing to unmount the file system has been added. The new option requires force_unmount="" to be enabled and it is not compatible with nfsserver resource agent.

All users of rgmanager should upgrade to these updated packages, which fix these bugs and add these enhancements.

4.150. rhn-client-tools

4.150.1. RHBA-2013:0104 — 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.

The rhn-client-tools packages provide programs and libraries that allow a system to receive software updates from Red Hat Network.

Bug Fixes

BZ#761489

Previously, when the rhn-virtualization-host package was installed and the libvirtd service was not running, the exit status of the rhnreg_ks utility would incorrectly indicate an error even if it succeeded in registering the system. This update corrects this error and the rhnreg_ks utility now terminates with the exist status of 0 in this situation.

BZ#771749

Prior to this update, an attempt to use the rhn-channel tool to manage a non-existent channel failed with a traceback. With this update, the user is presented with an informative error message.

BZ#781336

When the user attempted to register a system with RHN Classic and provided invalid credentials, the rhn_register utility for the graphical user interface previously reported the following error at the very end of the registration process: "You have no active subscriptions available in your account". This update adapts the rhn_register utility to report invalid credentials as expected.

BZ#798181

Previously, an error message that had no effect and mentioned Subscription Manager could appear if the user was registering the system with Red Hat Network or Red Hat Network Satellite. With this update, this message is no longer presented to the user.

BZ#865641

In the beta version of Red Hat Enterprise Linux 5.9, certain parts of the rhn_register utility and the firstboot application were not fully translated to all supported languages. This update ensures that both these tools are translated as expected.

BZ#827076

When the server failover mechanism was enabled and rhnplugin failed to connect to the primary server, it did not correctly fall back to the secondary Red Hat Network Satellite or Red Hat Network Proxy server. This update ensures that when the primary server is unavailable and secondary servers are configured, rhnplugin correctly attempts to connect to these servers instead.

Enhancement

BZ#823549

The rhn_register utility for the graphical user interface and the "Set Up Software Updates" part of the firstboot application have been adapted to mention Subscription Manager.

All users of rhn-client-tools are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

4.151. rhnsd

4.151.1. RHBA-2013:0097 — rhnsd bug fix update

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

The rhnsd packages provide the Red Hat Network Services Daemon, a system service that automatically queries the Red Hat Network servers, determines which packages on the machine need to be updated, and performs appropriate actions.

Bug Fix

BZ#800127

The /etc/sysconfig/rhn/rhnsd configuration file allows the system administrator to specify how many minutes the rhnsd service waits before checking the Red Hat Network for available updates and actions again. The previous version of the rhnsd service would incorrectly log a message telling the user that this interval is specified in seconds. This update corrects the wording of this log message.

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

4.152. rp-pppoe

4.152.1. RHBA-2012:0726 — rp-pppoe bug fix update

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

The rp-pppoe packages provide the Roaring Penguin PPPoE client, a user-mode program that does not require any kernel modifications. This client is fully compliant with RFC 2516, the official PPPoE (Point-to-Point Protocol over Ethernet) specification.

Bug Fix

BZ#606403

Prior to this update, the pppoe-server did not correctly calculate the value of the Access Concentrator (AC) Cookie on Intel 64 and AMD64 platforms. As a consequence, the pppoe-server did not return a PPPoE active discovery session-confirmation (PADS) packet to the client. This update modifies the pppoe-server code so that a PADS packet is returned.

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

4.153. rpm

4.153.1. RHBA-2013:0061 — 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#620570

RPM treated systems which were using Geode processors as compatible with the i686 architecture. Consequently, installation of i686 packages failed on this systems. This compatibility issue has been resolved by setting the architecture to i686, and installation of the i686 architecture packages works as expected.

BZ#760552

Previously, the Japanese version of the rpm(8) manual page contained multiple typos. This update corrects those typos.

BZ#783451

The Python bindings provided by the rpm-python package incorrectly added a new line character at the end of the group tag when retrieving it from a Python program. This bug has been fixed and the tag is now returned unaltered.

BZ#808547

Due to the lack of DWARF 3 and 4 format support, the rpmbuild utility was not able to produce usable debug packages with newer compilers. This update adds the required support for the debugedit utility to RPM, and DWARF 3 and 4 formats are now supported as expected.

BZ#813282

The "freshen" (rpm -F/--freshen) operation did not consider the architecture the packages were built for when selecting update candidates, which caused either misleading error messages or packages being updated to a different architecture inappropriately on multilib systems. RPM now requires an exact architecture match between packages on multilib systems to perform the freshen operation.

BZ#814602

Descriptions of the "--define" and "--eval" parameters were missing in the rpm(8) manual page. This update adds these missing descriptions.

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

4.153.2. RHSA-2012:0451 — Important: rpm security update

Updated rpm packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5 and 6; Red Hat Enterprise Linux 3 and 4 Extended Life Cycle Support; Red Hat Enterprise Linux 5.3 Long Life; and Red Hat Enterprise Linux 5.6, 6.0 and 6.1 Extended Update Support.

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

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

Security Fix

CVE-2012-0060, **CVE-2012-0061**, **CVE-2012-0815**

Multiple flaws were found in the way RPM parsed package file headers. An attacker could create a specially-crafted RPM package that, when its package header was accessed, or during package signature verification, could cause an application using the RPM library (such as the rpm command line tool, or the yum and up2date package managers) to crash or, potentially, execute arbitrary code.

Note: Although an RPM package can, by design, execute arbitrary code when installed, this issue would allow a specially-crafted RPM package to execute arbitrary code before its digital signature has been verified. Package downloads from the Red Hat Network are protected by the use of a secure HTTPS connection in addition to the RPM package signature checks.

All RPM users should upgrade to these updated packages, which contain a backported patch to correct these issues. All running applications linked against the RPM library must be restarted for this update to take effect.

4.154. ruby

4.154.1. RHSA-2013:0129 — Moderate: ruby security and bug fix update

Updated ruby packages that fix two security issues and one bug 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each 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 Fixes

CVE-2012-4522

It was found that certain methods did not sanitize file names before passing them to lower layer routines in Ruby. If a Ruby application created files with names based on untrusted input, it could result in the creation of files with different names than expected.

CVE-2012-4481

It was found that the RHSA-2011:0909 update did not correctly fix the CVE-2011-1005 issue, a flaw in the method for translating an exception message into a string in the Exception class. A remote attacker could use this flaw to bypass safe level 4 restrictions, allowing untrusted (tainted) code to modify arbitrary, trusted (untainted) strings, which safe level 4 restrictions would otherwise prevent.

The CVE-2012-4481 issue was discovered by Vit Ondruch of Red Hat.

Bug Fix

BZ#834381

Prior to this update, the "rb_syck_mktime" option could, under certain circumstances, terminate with a segmentation fault when installing libraries with certain gems. This update modifies the underlying code so that Ruby gems can be installed as expected.

All users of Ruby are advised to upgrade to these updated packages, which contain backported patches to resolve these issues.

4.155. perl-DBD-Pg

4.155.1. RHSA-2012:1116 — Moderate: perl-DBD-Pg security update

An updated perl-DBD-Pg package that fixes two 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 moderate security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Perl DBI is a database access Application Programming Interface (API) for the Perl language. perl-DBD-Pg allows Perl applications to access PostgreSQL database servers.

Security Fix

CVE-2012-1151

Two format string flaws were found in perl-DBD-Pg. A specially-crafted database warning or error message from a server could cause an application using perl-DBD-Pg to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

All users of perl-DBD-Pg are advised to upgrade to this updated package, which contains a backported patch to fix these issues. Applications using perl-DBD-Pg must be restarted for the update to take effect.

4.156. samba

4.156.1. RHSA-2012:0465 — Critical: samba security update

Updated samba packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6; Red Hat Enterprise Linux 5.3 Long Life; and Red Hat Enterprise Linux 5.6, 6.0 and 6.1 Extended Update Support.

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 for each vulnerability from the CVE link(s) associated with each description below.

Samba is an open-source implementation of the Server Message Block (SMB) or Common Internet File System (CIFS) protocol, which allows PC-compatible machines to share files, printers, and other information.

Security Fix

CVE-2012-1182

A flaw in the Samba suite's Perl-based DCE/RPC IDL (PIDL) compiler, used to generate code to handle RPC calls, resulted in multiple buffer overflows in Samba. A remote, unauthenticated attacker could send a specially-crafted RPC request that would cause the Samba daemon (smbd) to crash or, possibly, execute arbitrary code with the privileges of the root user.

Users of Samba are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the smb service will be restarted automatically.

4.156.2. RHSA-2012:0533 — Important: samba and samba3x security update

Updated samba3x and samba packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6 respectively.

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(s) associated with each description below.

Samba is an open-source implementation of the Server Message Block (SMB) or Common Internet File System (CIFS) protocol, which allows PC-compatible machines to share files, printers, and other information.

Security Fix

CVE-2012-2111

A flaw was found in the way Samba handled certain Local Security Authority (LSA) Remote Procedure Calls (RPC). An authenticated user could use this flaw to issue an RPC call that would modify the privileges database on the Samba server, allowing them to steal the ownership of files and directories that are being shared by the Samba server, and create, delete, and modify user accounts, as well as other Samba server administration tasks.

Red Hat would like to thank the Samba project for reporting this issue. Upstream acknowledges Ivano Cristofolini as the original reporter.

Users of Samba are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the smb service will be restarted automatically.

4.156.3. RHSA-2012:0332 — Critical: samba security update

Updated samba packages that fix one security issue are now available for Red Hat Enterprise Linux 4 and 5, and Red Hat Enterprise Linux 5.3 Long Life, and 5.6 Extended Update Support.

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 for each vulnerability from the CVE link(s) associated with each description below.

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

Security Fix

CVE-2012-0870

An input validation flaw was found in the way Samba handled Any Batched (AndX) requests. A remote, unauthenticated attacker could send a specially-crafted SMB packet to the Samba server, possibly resulting in arbitrary code execution with the privileges of the Samba server (root).

Red Hat would like to thank the Samba team for reporting this issue. Upstream acknowledges Andy Davis of NGS Secure as the original reporter.

Users of Samba are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the smb service will be restarted automatically.

4.157. samba3x

4.157.1. RHBA-2012:1126 — samba3x bug fix update

Updated samba3x packages that fix a bug are now available for Red Hat Enterprise Linux 5.

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.

Bug Fix

BZ#841374

Previously, newer versions of the Microsoft Windows operating system could not properly set Access Control Lists (ACLs) on a Samba share. Consequently, the "Access denied" error messages were returned and the share could not be configured in this regard. This bug has been fixed and the ACLs can now be fully managed as expected.

All users of samba3x are advised to upgrade to these updated packages, which fix this bug.

4.157.2. RHBA-2013:0064 — samba3x bug fix and enhancement update

Updated *samba3x* packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

Samba is an open-source implementation of the Server Message Block (SMB) or Common Internet File System (CIFS) protocol, which allows PC-compatible machines to share files, printers, and other information.

Note

The *samba3x* packages have been upgraded to upstream version 3.6, which provides a number of bug fixes and enhancements over the previous version. In particular, support for the SMB2 protocol has been added. SMB2 support can be enabled with the following parameter in the [global] section of the **/etc/samba/smb.conf** file:

```
max protocol = SMB2
```

Warning

Warning, the updated *samba3x* packages also change the way ID mapping is configured. Users are advised to modify their existing **Samba** configuration files. For more information, refer to the Release Notes for Samba 3.6.0, the **smb.conf** man page and the individual IDMAP backend man pages.

Note

Also note that several *Trivial Database* (TDB) files have been updated and printing support has been rewritten to use the actual registry implementation. This means that all TDB files are upgraded as soon as you start the new **Samba** server daemon (**smbd**) version. You cannot downgrade to an older *samba3x* version unless you have backups of the TDB files. (BZ#803457, BZ#839383).

Bug Fixes

BZ#738185

When the connection to a *Domain Controller* was lost, for example if a network cable was removed, the *Remote Procedure Call* (RPC) connection timed out and was not reset. Consequently, all subsequent RPC calls to the Domain Controller timed out. With this update, the *Winbind daemon* (winbindd) now resets the connection if an RPC timeout occurs. As a result, the connection is reestablished and new RPC commands can be issued.

BZ#782168

The man page for the Winbind information query tool “wbinfo” described the “-h” switch which is not present. The documentation has been changed and the options are now correctly documented.

BZ#790384

Samba sometimes generated many debug messages such as “Could not find child XXXX -- ignoring” that were written to syslog. Consequently, although these messages are not critical, syslog could be flooded by the large amount of these messages. Samba has been fixed to no longer issue this message to syslog automatically and syslog is no longer flooded by these Samba debug messages.

BZ#790845

When using **Samba** with the “password server” configuration setting and when the given name for that parameter was a hostname that resolved to multiple IP addresses, Samba did not correctly handle the returned addresses. Consequently, Samba failed to use one of the password servers

and terminated unexpectedly. This update fixes Samba to correctly process multiple IP addresses when using a hostname with the “password server” parameter. Samba now works correctly with multiple IP addresses in the scenario described.

BZ#816871

If “winbind normalize names = yes” was set and “winbind separator” was set to something other than the default separator, users were unable to login to Samba. The relevant check for the winbind separator has been changed to read it from the config file instead of using a hardcoded value. As a result, users are able to login to Samba again in the scenario described.

BZ#802546

Packages requiring *samba* did not recognize *samba3x* as an updated samba version. With this update, dependent packages recognize *samba3x* as the new *samba* version.

BZ#828113, BZ#830944

Due to a regression, the previous release changed the behavior of resolving domain local groups and the Winbind daemon (winbindd) could not find them. The original behavior for resolving the domain local groups has been restored. As a result, the ID command resolves domain local groups in its own domain correctly again.

BZ#838892

Samba 3.6 failed to migrate existing printers from the *Trivial Database* (TDB) to the registry due to a *Network Data Representation* (NDR) alignment problem. Consequently, printers from 3.5 could not be migrated and the Samba server daemon (smbd) stopped with an error. The NDR parser has been fixed to correctly parse printing entries from **Samba** 3.5. As a result, printers are correctly migrated from 3.5 TDB to 3.6 registry.

BZ#855831

When there was no connection to the trusted domain and an attempt was made to lookup a user, a null-pointer dereference occurred. Consequently, the Winbind daemon (winbindd) terminated unexpectedly with a segmentation fault. The code has been improved to make sure that the connection to the domain controller is set up before attempting to resolve a username. As a result, Winbind no longer crashes and logs useful error messages in the scenario described.

Users of *samba3x* should upgrade to these updated packages, which fix these bugs and add these enhancements.

4.157.3. RHSA-2012:0466 — Critical: samba3x security update

Updated samba3x packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and Red Hat Enterprise Linux 5.6 Extended Update Support.

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 for each vulnerability from the CVE link(s) associated with each description below.

Samba is an open-source implementation of the Server Message Block (SMB) or Common Internet File System (CIFS) protocol, which allows PC-compatible machines to share files, printers, and other information.

Security Fix

CVE-2012-1182

A flaw in the Samba suite's Perl-based DCE/RPC IDL (PIDL) compiler, used to generate code to

handle RPC calls, resulted in multiple buffer overflows in Samba. A remote, unauthenticated attacker could send a specially-crafted RPC request that would cause the Samba daemon (smbd) to crash or, possibly, execute arbitrary code with the privileges of the root user.

Users of Samba are advised to upgrade to these updated packages, which contain a backported patch to resolve this issue. After installing this update, the smb service will be restarted automatically.

4.158. scim-bridge

4.158.1. RHBA-2012:0578 — scim-bridge bug fix update

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

SCIM (Smart Common Input Method) Bridge is a C implementation of a GTK IM module for SCIM.

Bug Fix

BZ#805753

Prior to this update, the message "The lockfile is destroyed" was incorrectly logged as an error message. This update modifies the message logging level so that this message is now correctly logged as a info message.

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

4.159. selinux-policy

4.159.1. RHBA-2013:0060 — selinux-policy bug fix and enhancement update

Updated *selinux-policy* packages that fix a number of bugs and add various enhancements 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#682856, BZ#841178

When SELinux was running in enforcing mode, it incorrectly prevented the Postfix mail transfer agent from re-sending queued email messages. This update adds a new security file context for the **`/var/spool/postfix/maildrop/`** directory to make sure Postfix is allowed to re-send queued email messages in enforcing mode.

BZ#738995

Previously, the **`cyrus-master`** process could not run as an NNTP server because **`cyrus-master`** was unable to use the **`indd`** port. With this update, the SELinux policy rules have been updated, and the problem with **`cyrus-master`** running as an NNTP server no longer occurs.

BZ#751385

Previously, the **`condor_vm-gahp`** service running in the **`initrc_t`** SELinux domain returned AVC (Access Vector Cache) messages. This update labels **`condor_vm-gahp`** the **`virtd_exec_t`** SELinux security context, thus fixing this bug.

BZ#784197

When SELinux was running in enforcing mode, the **cimserver** command was unable to rename its own **cimserver_current.conf** file. This update fixes the relevant policy and **cimserver** program can now rename its configuration file as expected.

BZ#785076

When SELinux was running in enforcing mode and Kerberos+NSS was configured to use the **coolkey** module, AVC messages were returned. This update fixes the relevant SELinux policy so that the AVC messages are no longer returned in the described scenario.

BZ#803704

Previously, when a file was created by the **/usr/bin/R** command in user home directories, these directories got an incorrect SELinux security context because of missing SELinux policy rules. With this update, the relevant SELinux policy has been amended to ensure that correct SELinux security context is set in the described scenario.

BZ#807686

When OpenMPI (Open Message Passing Interface) was configured to use the parallel universe environment in the Condor server, a large number of AVC messages was returned when an OpenMPI job was submitted. Consequently, the job failed. This update fixes the appropriate SELinux policy and OpenMPI jobs now pass successfully and no longer cause AVC messages to be returned.

BZ#833843

With SELinux in enforcing mode, missing SELinux policy rules prevented the **freeradius2** server to communicate with the **postgresql** database. With this update, appropriate SELinux rules have been added and **freeradius2** is now able to communicate with the **postgresql**.

BZ#834621

SSSD (System Security Services Daemon) sometimes handles systems with more than four thousand processes running simultaneously. This requires the **CAP_SYS_RESOURCE** Linux capability to be set with a higher limit for open file descriptors but SELinux did not previously allow it. With this update, an appropriate SELinux rule has been added to prevent this bug.

BZ#838511

Previously, with SELinux in enforcing mode, the **clamd** command was unable to create its own PID file in the **/var/run/amavis/** directory. With this update, the **amavis_create_pid_files()** SELinux policy interface has been fixed to allow this action.

BZ#843443

With SELinux running in enforcing mode, the **snmpd** daemon was unable to connect to the **modcluster** service over the **Unix** stream socket. This bug has been fixed and the updated SELinux policy rules now allow these operations.

BZ#844701

When SELinux was running in enforcing mode, the **httpd** daemon running in the **piranha_web_t** SELinux domain was unable to read from the random number generator device (**/dev/random**). This update adds appropriate SELinux rules to grant **httpd** running in the **piranha_web_t** domain access to **/dev/random**.

BZ#848693

Previously, security contexts for the **sesh** shell installed in different directories did not match. This update adds a SELinux security context for the **/usr/libexec/sesh** command to be the same as the context for the **/usr/sbin/sesh** command.

BZ#848727

Due to an error in a SELinux policy, SELinux incorrectly prevented the **netplugd** service from starting. Now, updated SELinux policy rules have been provided that allow **netplugd** execute the **brctl** command in the **brctl** SELinux domain, thus fixing this bug.

BZ#849155

Due to an incorrect file context specification, correct labeling for 64-bit Oracle libraries was missing from the SELinux policy. This bug has been fixed and the *selinux-policy* packages now provide this missing labeling.

BZ#833843

Previously, when the **etc-pam-d-radiusd-uses-non-existent-password-auth** test was run, the **radiusd** service was disallowed the **ptrace** system call, resulting in an AVC message being returned. This update adds an appropriate SELinux policy rule to allow **radiusd** this system call, thus fixing this bug.

BZ#851658

Previously, OCSP (Online Certificate Status Protocol) requests from the Kerberos KDC (Key Distribution Center) failed in enforcing mode. Consequently, attempts to obtain Kerberos credentials by running the **kinit** from a smart card were not successful. This update allows the **krb5kdc** utility to connect to the **tcp/9180** port, thus fixing this problem.

BZ#854194

With SELinux in enforcing mode, the following scenario did not work and generated AVC messages to the **/var/log/audit/audit.log** file:

1. append the following line to **/etc/sysconfig/snmptrapd.options** file:

```
OPTIONS="-Lsd -x /var/agentx/master"
```

2. append following line to **/etc/snmp/snmpd.conf** file:

```
master agentx
```

3. run the **service snmpd restart** and **service snmptrapd restart** commands.

With this update, an appropriate SELinux rule has been added and this scenario now succeeds.

BZ#855035

Due to incorrect SELinux policy rules, the **nmbd** service was unable to create the **/var/nmbd/unexpected/** directory for its operation. Consequently, the following command failed:

```
nmblookup -U 127.0.0.1 MACHINE-nmb
```

Now, the SELinux policy rules have been updated and the problem with the above command no longer occurs.

BZ#855324

With SELinux in enforcing mode, when the **openswan** service was started and stopped in quick succession on a freshly-booted system, the AVC denial messages were logged to the **/var/log/audit/audit.log** file. With this update, SELinux policy has been amended to ensure that SELinux no longer logs AVC messages in the described scenario.

BZ#859338

When SELinux was running in enforcing mode, the **pulse** daemon failed to start the **IPVS** synchronization daemon at startup and a large number of AVC messages was logged to the **/var/log/audit/audit.log** file. This bug has been fixed and SELinux now allows **IPVS** to be started by **pulse** as expected.

BZ#863155

Due to an incorrect SELinux policy, the **swat** utility was unable to write into the **unexpected** samba socket. This update provides a new SELinux policy rule, which prevent this bug.

Enhancements

BZ#839608, BZ#849071

A new SELinux policy rule has been added to allow the CUPS back end to send D-Bus messages to the system bus, thus allowing the *hplip3* package to work with SELinux running in enforcing mode.

BZ#843841

The rebased *rsyslogd* package in Red Hat Enterprise Linux 5.9 required additional SELinux policy updates to allow running the **getschedule**, **setschedule**, and **sys_nice** operations. These *selinux-policy* packages add the required policy.

BZ#810239

With this update, labels of all files that are processed by the **logrotate** utility are preserved.

BZ#845672

The **zarafa** SELinux policy has been updated by the **zarafa** SELinux policy from Red Hat Enterprise Linux 6.

BZ#772205

Support for the **mod_ban** module in the **proftpd** service has been added.

BZ#773042

A new **fenced_selinux.8** man page has been added.

BZ#750588

A new **virtd_selinux.8** man page has been added.

Users of *selinux-policy* are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.160. setroubleshoot

4.160.1. RHBA-2012:0146 — setroubleshoot bug fix update

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

The setroubleshoot packages provide tools to help diagnose SELinux problems. When Access Vector Cache (AVC) messages are generated, an alert can be displayed that provides information about the problem and helps track its resolution. Alerts are user-configurable. The same tools can be run on existing log files.

Bug Fix

BZ#789143

Due to a memory leak in the rpm underlying code, the setroubleshoot tool consumed extensive memory resources. This update applies a patch that reduces memory consumption significantly, however, the problem has not been fixed completely and has to be resolved in the rpm utility.

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

4.161. shadow-utils

4.161.1. RHBA-2013:0040 — shadow-utils bug fix update

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

The shadow-utils package includes the necessary programs for converting UNIX password files to the shadow password format, plus programs for managing user and group accounts. The pwconv command converts passwords to the shadow password format. The pwunconv command converts shadow passwords and generates an npasswd file (a standard UNIX password file). The pwck command checks the integrity of password and shadow files. The lastlog command prints out the last login times for all users. The useradd, userdel, and usermod commands are used for managing user accounts. The groupadd, groupdel, and groupmod commands are used for managing group accounts.

Bug Fix

BZ#787736

A structural bug in a delete routine meant /etc/shadow (or /etc/gshadow) files containing bad entries were not updated properly by pwconv (or grpconv). Specifically if /etc/shadow (or /etc/gshadow) contained two consecutive bad entries, the second of the two bad entries was skipped when pwconv (or grpconv) was run on the file. This left the file improperly updated. With this update, the loop that iterates through /etc/shadow (or /etc/gshadow) was reworked. No bad lines (consecutive or otherwise) are now skipped and /etc/shadow (or /etc/gshadow) files are properly updated by pwconv (or grpconv).

All shadow-utils users should install this update which fixes this bug.

4.162. smartmontools

4.162.1. RHBA-2013:0041 — smartmontools bug fix and enhancement update

Updated smartmontools packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

The smartmontools packages contain the smartctl and the smartd utilities to control and monitor storage systems using the Self-Monitoring, Analysis and Reporting Technology System (SMART) built into most modern ATA and SCSI hard disks. In many cases, these utilities will provide advanced warning of disk degradation and failure.

The smartmontools packages have been upgraded to version 5.42, which provides a number of bug fixes and enhancements over the previous version. This update also features improved support of SATA disks on 3ware 9750 RAID controllers, improved support of SSD devices, and a much larger database of supported devices. (BZ#714123)

Bug Fix

BZ#706782

Prior to this update, the smartd utility failed to handle multiple /dev/sgX devices, which were provided by the mptsas controller. As a consequence, the devices were not SMART self-check capable. This update modifies the underlying code so that smartd can now handle multiple /dev/sgX devices. Now, all devices pass the SMART self-check.

Enhancement

BZ#519261

This update adds improved MegaRAID support to the smartmontools packages for Red Hat Enterprise Linux 5.

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

4.163. specspo

4.163.1. RHBA-2012:1159 — specspo bug fix update

Updated specspo packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The specspo packages contain the portable object catalogs used to internationalize packages.

Bug Fixes

BZ#520378

Previously, translation of the Summary and Description fields for the Deployment_Guide package contained incorrect information. The information has been corrected with this update.

BZ#636195

Translation of the Summary and Description fields for the flash-plugin package contained outdated version information that changed with every update of flash-plugin. Except for English, there is currently no other translation available for the flash-plugin package, so this information has been removed.

BZ#698881

Translation of the libvirt package's Description and Summary contained incorrect information. This has been updated and the information is now correct.

BZ#835096

Previously, translation of the Summary and Description fields for the pm-utils and specspo packages contained an incorrect product name. The name has been fixed with this update.

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

4.164. spice-client

4.164.1. RHBA-2012:0147 — spice-client bug fix update

An updated spice-client package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The spice-client package provides the Simple Protocol for Independent Computing Environments (SPICE) client application. SPICE is a remote display protocol designed for virtual environments. SPICE users can access a virtualized desktop or server from the local system or any system with network access to the server. SPICE is used in Red Hat Enterprise Linux for viewing virtualized guests running on the KVM hypervisor or on Red Hat Enterprise Virtualization Hypervisors.

Bug Fix

BZ#790894

The SPICE client did not correctly handle an exception which was raised when trying to connect to a guest operating system with no running SPICE agent. Consequently, the SPICE client application terminated unexpectedly after the 30-second timeout. With this update, the SPICE client correctly handles this situation and successfully connects to the guest system without unnecessary waiting.

All users of spice-client are advised to upgrade to this updated package, which fixes this bug.

4.164.2. RHBA-2013:0096 — spice-client bug fix update

An updated spice-client package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The spice-client package provides the Simple Protocol for Independent Computing Environments (SPICE) client application. SPICE is a remote display protocol designed for virtual environments.

Bug Fix

BZ#789331

Prior to this update, the SPICE client did not correctly handle an exception which was raised when trying to connect to a guest operating system with no running SPICE agent. As a consequence, the SPICE client application terminated unexpectedly after a 30-second timeout. With this update, the SPICE client correctly handles this situation and successfully connects to the guest system without unnecessary waiting.

All users of spice-client are advised to upgrade to this updated package, which fixes this bug.

4.165. spice-xpi

4.165.1. RHBA-2013:0100 — spice-xpi bug fix update

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

The spice-xpi package provides the Simple Protocol for Independent Computing Environments (SPICE) extension for Mozilla that allows the SPICE client to be used from a web browser.

Bug Fixes

BZ#795513

Prior to this update, the spice-xpi utility incorrectly assumed sole ownership of the /usr/lib{,64}/mozilla/plugins ({_libdir}/mozilla/plugins/) directory and all files in it. As a consequence, also files that belonged to other packages were removed when spice-xpi was uninstalled. This update modifies the specifications to remove only files that belong to the spice-xpi package.

BZ#817470

Prior to this update, the spice-xpi packages did not compile correctly with the xulrunner runtime environment. This update modifies the underlying code to allow spice-xpi to compile successfully.

All users of spice-xpi are advised to upgrade to these updated packages, which fix these bugs.

4.166. sqlite

4.166.1. RHBA-2013:0063 — sqlite bug fix

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

SQLite is a C library that implements an SQL database engine.

Bug Fix

BZ#504634

Prior to this update, the "PRAGMA user_version" query returned a NULL value as the column heading, which caused PHP to terminate unexpectedly with a segmentation fault. With this update, the underlying source code has been modified and the "PRAGMA user_version" query now works correctly.

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

4.167. squirrelmail

4.167.1. RHSA-2013:0126 — Low: squirrelmail security and bug fix update

An updated squirrelmail package that fixes one security issue 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. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

SquirrelMail is a standards-based webmail package written in PHP.

Security Fix

CVE-2012-2124

The SquirrelMail security update RHSA-2012:0103 did not, unlike the erratum text stated, correct the CVE-2010-2813 issue, a flaw in the way SquirrelMail handled failed log in attempts. A user preference file was created when attempting to log in with a password containing an 8-bit character, even if the username was not valid. A remote attacker could use this flaw to eventually consume all hard disk space on the target SquirrelMail server.

Bug Fixes

BZ#241861

Prior to this update, SquirrelMail could not decode multi-line subjects properly. Consequently, the decode header internationalization option did not properly handle new lines or tabs at the beginning of the lines. This bug has been fixed and SquirrelMail now works correctly in the described scenario.

BZ#359791

Due to a bug, attachments written in HTML code on the Windows operating system were not displayed properly when accessed with SquirrelMail; the "!=null" string was trimmed to "!ull". This bug has been fixed and the attachments are now displayed correctly in such a case.

BZ#450780

Previously, e-mail messages with a Unique Identifier (UID) larger than 2^31 bytes were unreadable when using the squirrelmail package. With this patch the squirrelmail package is able to read all messages regardless of the UIDs size.

BZ#475188

Due to a bug, a PHP script did not assign the proper character set to requested variables. Consequently, SquirrelMail could not display any e-mails. The underlying source code has been modified and now the squirrelmail package assigns the correct character set.

BZ#508686

Due to the incorrect internationalization option located at the i18n.php file, the squirrelmail package could not use the GB 2312 character set. The i18n.php file has been fixed and the GB 2312 character set works correctly in the described scenario.

BZ#528758

Previously, the preg_split() function contained a misspelled constant, PREG_SPLIT_NI_EMPTY, which could cause SquirrelMail to produce error messages. The name of the constant has been corrected to PREG_SPLIT_NO_EMPTY, and SquirrelMail no longer produces error messages in this scenario.

BZ#745380

Due to Security-Enhanced Linux (SELinux) settings, sending e-mails from the SquirrelMail web interface was blocked. This update adds a note to the SquirrelMail documentation that describes how to set the SELinux options to allow sending e-mails from the SquirrelMail web interface.

BZ#745469

Previously, the squirrelmail package did not comply with the RFC 2822 specification about line length limits. Consequently, attachments with lines longer than 998 characters could not be forwarded using SquirrelMail. This patch modifies the underlying source code and now SquirrelMail complies with the RFC 2822 specification as expected.

BZ#789353

Prior to this update, the squirrelmail package required the php-common script instead of the mod_php script during installation or upgrade of the package, which led to a dependency error. As a result, attempting to install or upgrade the squirrelmail package failed on systems using the php53 packages. With this update, the dependencies of the squirrelmail package were changed and the installation or upgrade now works correctly in the described scenario.

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

4.168. sssd

4.168.1. RHBA-2012:0440 — sssd bug fix update

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

The sssd packages contain a set of daemons to manage access to remote directories and authentication mechanisms.

Bug Fix

BZ#806765

If an LDAP server had the paging control module installed but not enabled or if a highly loaded LDAP server was restricted to a single page search operation at the time, SSSD could unexpectedly deny simple paged search requests with the following error message:

Unexpected result from ldap: Server is unwilling to perform(53), Simple Paged Results Search already in progress on this connection.

This update implements the "ldap_disable_paging" option, which allows SSSD to disable the LDAP paging control. With this option set, the number of SSSD lookups is limited to the maximum defined by the LDAP server and SSSD no longer fails with aforementioned error in this scenario.

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

4.168.2. RHBA-2012:1342 — sssd bug fix update

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

The sssd packages contain a set of daemons to manage access to remote directories and authentication mechanisms.

Bug Fix

BZ#860788

If a single group was present in two different places in the LDAP group hierarchy, the sssd daemon skipped the whole nesting level that contained the group when it was processing the group for the second time. With this update, sssd only skips the single group that was already processed and moves to other groups on the same nesting level, thus fixing this bug.

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

4.168.3. RHBA-2013:0047 — sssd bug fix update

Updated sssd packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

SSSD (System Security Services Daemon) provides daemons to manage access to remote directories and authentication mechanisms. It provides NSS (Name Service Switch) and PAM (Pluggable Authentication Modules) interfaces and a pluggable back end system to connect to multiple different account sources.

Bug Fixes

BZ#782221

Previously, the SSSD daemon could deny simple paged search requests, if an LDAP (Lightweight Directory Access Protocol) server had the paging control module installed but not enabled or if a highly loaded LDAP server was restricted to a single page search operation. With this update, the "ldap_disable_paging" option disables the LDAP paging control to limit the number of SSSD lookups defined by the LDAP server.

BZ#783081

Previously, a segmentation fault could occur when the IPA HBAC (Host-Based Access Control) code iterated over the list of groups with an entity that formed the HBAC rule without checking its validity. This update creates an empty array to allow the HBAC code to loop safely.

BZ#797272

Previously, the SSSD daemon did not have a versioned dependency on the DBus library. Now, a versioned dependency on the DBus library is added to enable SSSD also on older versions of the DBus library.

BZ#797300

Previously, the IPA provider checked only IPA access control policies and ignored additional access control policies when the access provider was configured to use IPA access control policies. Users could get access when the LDAP access provider denied access. Now, LDAP access control policies are checked before the IPA access control policies.

BZ#811912

Previously, provider-specific data was freed before data that was transported between different SSSD processes. A segmentation fault could occur on shutdown when already freed memory was accessed. This update changes the order of free operations.

BZ#815154

Previously, the SSSD daemon was limited to 1024 open files by default. Further logins were rejected if the number of simultaneous connections exceed the limit. This update sets the limit to 8000 open files or the maximum from limits.conf, whichever is less.

BZ#817073

Previously, the SSSD daemon went offline when set to encrypt the communication with the LDAP server using GSSAPI if the first Kerberos server was down. Now, SSSD retries all key distribution centers (KDC) before going offline.

BZ#828190

Previously, the status of a server that was unreachable was reset to neutral after a 30-seconds timeout. The server list marked a server for another retry and the cycle looped if the server list was too long. This update performs only one loop and stops when encountering a server that was checked before.

BZ#833169

Previously, the SSSD daemon kept connections to client applications open for the lifetime of the application. SSSD could use too many file descriptors and refused new connections if many long-running applications were running simultaneously. Now, SSSD keeps a connection to a client application open only for a default interval of 60 seconds.

BZ#841677

Previously, the SSSD daemon did not contain an option to disable source hosts processing. The LDAP query to retrieve hosts could reach the administration limit of the LDAP server and abort if the IPA server contained a large number of hosts. Now, the ipa_hbac_support_srchost option defaults to "False" to switch off source hosts support.

BZ#846664

Previously, the SSSD daemon could skip a complete level of nesting processes when SSSD processed a group that was already encountered on another nesting level. SSSD incorrectly reported group memberships. This update modifies the logic in the LDAP back end to skip only already processed groups.

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

4.169. strace

4.169.1. RHBA-2012:0326 — strace bug fix update

An updated strace package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The strace program intercepts and records the system calls called and received by a running process. It can print a record of each system call, its arguments and its return value. The strace utility is useful for diagnosing, debugging and instructional purposes.

Bug Fix

BZ#788666

The strace utility did not properly track switches between 32-bit and 64-bit process execution domains (so called "personalities") when tracing multiple processes with multiple "personalities". This caused strace to output the wrong system call names and arguments for the traced processes. This update corrects personality tracking in strace so that it now prints system call names and arguments as expected.

All users of strace are advised to upgrade to this updated package, which fixes this bug.

4.169.2. RHBA-2013:0010 — strace bug fix update

Updated strace packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The strace packages provide a utility to intercept and record the system calls called and received by a running process. The strace utility can print a record of each system call, its arguments and its return value. The strace utility is useful for diagnosing, debugging and instructional purposes.

Bug Fixes

BZ#495935

Prior to this update, the strace utility incorrectly decoded system calls when tracing a 32 bit process on a 64 bit machine, because strace on IBM System z platforms is not multi-arch aware. This update provides an additional strace executable (strace32) which can be used to trace 32 bit processes on 64 bit machines.

BZ#509152

Prior to this update, the strace utility incorrectly exited a system call loop when the child process was interrupted. As a consequence, strace reported that the last system call exited with a ERESTART_RESTARTBLOCK condition. This update modifies the loop exit so that strace now correctly reports that the interrupted system call is unfinished.

BZ#512692

Prior to this update, the kernel could, under certain circumstances, fail to send a SIGTRAP signal to the strace utility. As a consequence, the strace utility could become suspended if the target process blocked the debugging signal SIGTRAP. With this update, strace now checks for this situation and re-synchronizes with system call notifications when necessary.

BZ#552964

Prior to this update, traces were not detached but forcefully terminated when the SIGTERM signal terminated the strace process while the trace executed a fork or a cloned system call. This update modifies the underlying code to cleanly detach traces when a strace process is terminated.

BZ#571437

Prior to this update, the strace utility incorrectly printed 64 bit arguments for certain system calls such as "fadvise". This update modifies the underlying code so that the correct "fadvise" arguments are printed as expected.

BZ#580211

Prior to this update, a misinterpreted status caused strace to leave the traced process in a stopped state when detaching from a process. This update modifies the underlying code to leave the process in the correct state after detaching.

BZ#759566

Prior to this update, the strace utility extracted arguments for the "semtimedop" system call from the wrong location on the IBM System z platforms. As a consequence, arguments for the "semtimedop" system call were incorrectly displayed. This update modifies strace to extract the arguments from the correct memory location so that the arguments for the "semtimedop" system call are displayed as expected.

BZ#768203

Prior to this update, the strace utility did not correctly track switches between 32-bit and 64-bit process execution domains, so called "personalities", when tracing multiple processes with multiple "personalities". As a consequence, strace logged the wrong system call names and arguments for the traced processes. This update corrects personality tracking in strace so that it now prints system call names and arguments as expected.

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

4.170. subscription-manager

4.170.1. RHBA-2012:0148 — subscription-manager bug fix update

Updated subscription-manager packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

The subscription-manager package provides programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat Entitlement platform.

Bug Fix

BZ#788661

On Red Hat Enterprise Linux 5, subscription management does not support software channels for 64-bit PowerPC architectures. Therefore, the "install-num-migrate-to-rhsm" utility did not work on these architectures, and users were not able to migrate their systems to the Certificate-based Red Hat Network (RHN). With this update, the "install-num-migrate-to-rhsm" utility has been modified to use the supported PowerPC product certificates instead. Systems installed on 64-bit PowerPC architectures can now be migrated properly from Classic RHN to Certificate-based RHN.

BZ#788665

Previously, the "rhn-migrate-classic-to-rhsm" utility did not correctly handle a situation when a Red Hat Network (RHN) software channel supported more than one product. Consequently, the utility installed superfluous product certificates when client systems were subscribed to particular RHN channels. This update corrects "rhn-migrate-classic-to-rhsm" so that only the proper product certificate is now installed under these circumstances.

BZ#790437

Previously, the "install-num-migrate-to-rhsm" utility did not work correctly for certain products. Consequently, the utility installed also a superfluous Desktop product certificate when the system was provided with an installation number for a Workstation product and vice versa. With this update, "install-num-migrate-to-rhsm" has been fixed and only the correct product certificate is now installed under these circumstances.

All users of subscription-manager are advised to upgrade to these updated packages, which fix these bugs.

4.170.2. RHBA-2012:1074 — subscription-manager bug fix update

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

The subscription-manager package provides programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat Entitlement platform.

Bug Fix

BZ#838091

Client ID certificates expire after one year, and previously could be regenerated only manually by the user. With this update, the client can automatically retrieve an updated client ID certificate from the entitlement server if this is supported by the target instance.

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

4.170.3. RHBA-2013:0033 — subscription-manager bug fix and enhancement update

Updated *subscription-manager* packages that fix numerous bugs and add various enhancements are now available for Red Hat Enterprise Linux 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.

Bug Fixes

BZ#842170

Due to an incorrect logic in **Subscription Manager**, a "None" value was printed for service levels where an empty string should have been printed instead. This behavior has been fixed to recognize that an empty string represents a valid service level and the empty string is now printed for the service level if appropriate.

BZ#752316, BZ#771751

Due to an improper handling of multi-byte Unicode characters in a dependent library, some of these characters were not being rendered properly. This incorrect handling of multi-byte characters has been overridden by subclassing the dependent library and these characters are now rendered as expected.

BZ#853233

Due to an improper logic in the **rhn-migrate-classic-to-rhsm** tool, the Desktop (68.pem) and the Workstation (71.pem) certificates could both be installed on the system. However, these certificates cannot be installed simultaneously. Logic of this behavior has been fixed to prevent Desktop and Workstation certificates from coexisting.

BZ#849644

The **`--no-auto`** option in the **rhn-migrate-classic-to-rhsm** tool is used to prevent to auto-subscribing during the registration to the Subscription Manager service. Previously, user systems were not registered when the script was called with this option. This bug has been fixed, and the **`--no-auto`** option now works as expected in the described scenario.

BZ#849494

Previously, a variable name was used for two different variables in the **rhn-migrate-classic-to-rhsm** script. Consequently, when *Red Hat Network* (RHN) was configured to use a proxy, migration from RHN Classic to Certificate-based Red Hat Network failed. This script has been fixed to prevent the variable name collision and migration through a proxy now works as expected.

BZ#849483

Due to an incomplete implementation of migration from a standalone System Engine server, the migration failed when the organization name was required but not specified during registration. This bug has been fixed by soliciting the user to specify the organization name if necessary and the **rhn-migrate-classic-to-rhsm** tool works correctly now.

BZ#842768

Previously, the **`--baseurl`** and **`--serverurl`** options were being provided for a wide number of subcommands where they had no meaning. This overly broad options parsing has been fixed and these options are now only allowed where appropriate.

BZ#840169

When attempting to migrate a system from RHN to Red Hat Subscription Management using the **rhn-migrate-classic-to-rhsm** tool, the system was registered but did not have its service level set correctly. This bug has been fixed and the service level is now set before registration.

BZ#789182

Due to logging of Unicode strings, using the subscription-manager **`identity --regenerate`** command with a wrong username or a password caused a traceback to be printed to the console. This bug has been fixed by properly handling logging messages as Unicode strings and the tracebacks are no longer produced in such a case.

BZ#852001

The **`subscription-manager identity`** command is used to get the **`org name`** and **`org id`** values. Previously, this command reported the **`database id`** value instead of **`org id`**, which was then being misinterpreted by the user as the **`org key`**. Consequently, the user could try to register with the **`--org`** option passing in an unknown value. The value reported by **`subscription-manager identity`** has been changed to actually report the **`org key`** as the **`org id`**. As a result, users can now register using the reported **`org id`** value.

BZ#859811

When a consumer has been deleted on a Candlepin server, the client was left in an inconsistent state with the old consumer and entitlement certificates, which were no longer valid. This bug has been fixed and the **`rhsmcert`** daemon recognizes this inconsistent state, cleans the old entitlements, makes a backup of the old consumer certificate, and allows the client to register with the **`--force`** option.

BZ#862099

Closing some of the dialog boxes within **Subscription Manager** using the ESC key or the window manager's **`Close`** button led to those dialog boxes failing to open properly if the users attempted to use them again. With this update, default GTK **`destroy`** signals have been correctly hooked up and all dialog boxes can now be opened, closed and re-opened, regardless of how they are closed.

BZ#865954

Previously, **Subscription Manager** handled invalid system names incorrectly. Consequently, when an invalid system name was used, firstboot could become unresponsive.The handling of invalid system names has been fixed and the **`firstboot`** utility now works correctly in the described scenario.

BZ#803442

Previously, the **rhn-migrate-classic-to-rhsm** tool failed to migrate the RHN proxy settings from the **`/etc/sysconfig/rhn/up2date`** file. Consequently, post-migration configuration lacked the proxy settings and therefore could not connect. This bug has been fixed by including the **RHN up2date** proxy settings during the migration from the RHN Classic channel to **Subscription manager** and post-migration connection through the original proxy server is now maintained.

BZ#785203

Previously, the **subscription-manager-gui** utility did not have a convenient way to close. The toolbar buttons have been replaced by menus that include a **Quit** option.

BZ#773539

Due to incorrect logging of Unicode strings, using the **`orgs`** modules with a wrong username or a password caused a traceback to be printed to the console. This bug has been fixed by properly handling logging messages as Unicode strings and the tracebacks are no longer produced in such a case.

BZ#773527

Due to incorrect logging of Unicode strings, using the **`subscription-manager redeem --email`** command with a wrong username or a password caused a traceback to be printed to the console. This bug has been fixed by properly handling logging messages as Unicode strings and the tracebacks are no longer produced in such a case.

BZ#854467

An attempt to register with an activation key when an organization is required but not provided caused **Subscription Manager** to abort with an incorrect error message. The handling of the error condition has been corrected and an appropriate error message is now displayed in the described scenario.

BZ#853876

When a consumer was deleted using the subscription management application on www.redhat.com, the client was left in an inconsistent state with the old consumer and entitlement certificates, which were no longer valid. This bug has been fixed and the **`rhsmcert`** daemon recognizes this inconsistent state, cleans the old entitlements, makes a backup of the old consumer certificate, and allows the client to register with the **`--force`** option.

BZ#854312

The Candlepin server did not delete expired certificates until the next refresh operation. As a consequence, **Subscription Manager** could re-install any expired entitlement certificates that were reported by Candlepin, leaving the UI in an invalid state. This bug has been fixed and the **`rhsmcert`** daemon now checks any new entitlement certificates it receives from the Candlepin server to make sure that they are not expired before installing.

BZ#861443

Previously, an exception was ignored after it was issued. As a consequence, the healing process errors were never logged to the **`rhasmcertd`** log file. Handling of any exceptions has been fixed, so they are logged by the **`rhsmcert`** daemon and the proper exit status is now generated for the healing process.

Enhancements

BZ#821065

This enhancement introduces a progress spinner that is now shown during the auto-subscribe process so that the applications no longer appear to be unresponsive during this process.

BZ#790938

With this update, users can set a service-level preference, which is useful during an auto-subscribe process. Entitlements are granted from *Stock-keeping units* (SKUs) that provide the desired *Service-level agreement* (SLA).

BZ#790939

The **rhn-migrate-classic-to-rhsm** migration tool can now migrate a system and provide a service level for that system, so that the user can specify the SLA. Previously, the SLA was chosen automatically.

BZ#822706

The **`Register`** button is now shown on the **`Installed Software Tab`** when the system is not registered. The **`Auto-subscribe`** button is displayed once the system is registered.

Users of *subscription-manager* are advised to upgrade to these updated packages, which fix these bugs and add these enhancements.

4.171. subscription-manager-migration-data

4.171.1. RHBA-2013:0055 — subscription-manager-migration-data bug fix update

An updated subscription-manager-migration-data package that fixes several bugs and adds one enhancement is now available for Red Hat Enterprise Linux 5.

The subscription-manager-migration-data package provides Subscription Management tooling, which allows users to understand the specific products, which have been installed on their machines, and the specific subscriptions, which their machines consume.

Bug Fixes

BZ#786140

All *debuginfo channels were missing in the channel-cert-mapping.txt file. These channels have been added to this file.

BZ#786203

Previously, all *beta channels in the channel-cert-mapping.txt file were mapped to "none" instead of a valid product ID. The channel-cert-mapping.txt file has been modified and *beta channels are mapped to a proper ID as expected.

BZ#786278

Channels for -rhev- and -vt- in the channel-cert-mapping.txt file were not mapped to a product ID. The channel-cert-mapping.txt file has been fixed and subscription-manager-migration-data now includes mappings for these channels.

BZ#847069

Previously, the rhel-x86_64-server-eucjp-5* channels were not mapped to the Server-EUCJP-x86_64-e07b2fcd8a01-181.pem file due to missing certificates. The missing certificates have been added with this update, and the channels are now mapped correctly.

BZ#849274

The subscription-manager-migration-data package mapped the "JBoss Enterprise Application Platform" products incorrectly. The channel-cert-mapping.txt file has been fixed and the JBoss products are now mapped properly.

BZ#849305

Previously, the rhel-i386-rhev-agent-5-* channels in the channel-cert-mapping.txt file did not match the proper product ID in the content delivery network (CDN) Product Baseline. These channels matched product with identifier 150 instead of products with identifiers 68 and 69. This bug has been fixed and the product ID is now matched as expected.

BZ#852551

Prior to this update, mappings for the "Red Hat Developer Toolset" and "Red Hat Beta" products were missing. These missing mappings have been added to the channel-cert-mapping.txt file, and now all of the expected "Red Hat Developer Toolset" and "Red Hat Beta" product certifications and mappings are accounted for in the subscription-manager-migration-data.

BZ#861420

The product certificates and the mapping for the "Red Hat Enterprise Virtualization 3.0" (rhev 3.0) were missing. These certificates and this mapping have been added to subscription-manager-data.

BZ#861470

The product certificates and the mapping for the "JBoss Enterprise Application Platform - ELS" (jbappplatform-4.2.0) were missing. These certificates and this mapping have been added to subscription-manager-data.

BZ#865566

Additional *debuginfo channels (the rhel-x86_64-rhev-mgmt-agent-5-debuginfo and rhel-x86_64-rhev-mgmt-agent-5-beta-debuginfo channels) have been added to subscription-manager-data.

Enhancement

BZ#835964

The channel-cert-mapping.txt file has been updated to map Red Hat Network channels to the correct product certificates for Red Hat Enterprise Linux 5.9.

All subscription-manager-migration-data users are advised to upgrade to this updated package, which fixes these bugs and adds this enhancement.

4.172. subversion

4.172.1. RHBA-2012:0574 — subversion bug fix update

Updated subversion packages that resolve an issue are now available.

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.

Bug Fix

BZ#809384

The "svn" command unnecessarily required access to the parent directory during certain types of merge operations, which could have been denied by the server's authorization policy. This update corrects the svn command's behavior so that it no longer attempts to access a repository's parent folder during operations, with the result that it is no longer denied by access control or authorization policies.

All users of subversion are advised to upgrade to these updated packages, which resolve this issue.

4.173. sudo

4.173.1. RHBA-2012:1160 — sudo bug fix update

Updated sudo packages that fix one bug 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 Fix

BZ#846974

The RHSA-2012:1149 sudo security update introduced a regression that caused the permissions of the /etc/nsswitch.conf file to change during the installation or upgrade of the sudo package. This could cause various services to be unable to access the file. In reported cases, this bug prevented PostgreSQL from starting. This update fixes the bug and the file's permissions are no longer changed in the described scenario.

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

4.173.2. RHBA-2012:1270 — sudo bug fix update

Updated sudo packages that fix one bug 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 Fix

BZ#854513

Due to an previous enhancement update, the sudo behavior changed to run a command as a new child process using the fork() and execve() functions, rather than using execve() directly and replace the sudo process. This change in behavior caused various problems with custom scripts. This update adds a new option to restore the old behavior. This option can be activated by adding "Defaults cmnd_no_wait" to the /etc/sudoers file, which fixes this bug.

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

4.173.3. RHBA-2013:0112 — sudo bug fix and enhancement update

Updated sudo packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

The sudo (superuser do) utility allows system administrators to give specific users the ability to run commands as root.

Bug Fixes

BZ#806073

Previously, sudo escaped non-alphanumeric characters in commands using "sudo -s" or "sudo -" at the wrong place and interfered with the authorization process. Some valid commands were not permitted. Now, non-alphanumeric characters are escaped immediately before the command is executed and no longer interfere with the authorization process.

BZ#814508

Prior to this update, the sudo utility could fail to receive the SIGCHLD signal when it was executed from a process that blocked the SIGCHLD signal. As a consequence, sudo could become suspended and fail to exit. This update modifies the signal process mask so that sudo can exit and sends the correct output.

BZ#818585

The sudo update RHSA-2012:0309 introduced a regression that caused the SELinux context of the /etc/nsswitch.conf file to change during installation or upgrade of the sudo package. This could cause that various services confined by SELinux were no longer permitted to access the file. In reported cases, this issue prevented PostgreSQL and Postfix from starting.

BZ#829263

Prior to this update, a race condition bug existed in sudo. When a program was executed with sudo, it could exit successfully before sudo started waiting for it. In this situation, the program became a defunct process and sudo waited for it endlessly as it expected the program was still running.

BZ#840971

The sudo update RHSA-2012:0309 changed the behavior of sudo; it now runs commands as a child process instead of executing them directly and replacing the running process. This change could cause errors in some external scripts. A new cmnd_no_wait configuration option was added to restore the old behavior. To apply this option, add the following line to the /etc/sudoers file:

```
        Defaults cmnd_no_wait
```

BZ#841070

Updating the sudo package resulted in the "sudoers" line in /etc/nsswitch.conf being removed. This update corrects the bug in the sudo package's post-uninstall script that caused this issue.

BZ#846631

The RHSA-2012:1149 sudo security update introduced a regression that caused the permissions of the /etc/nsswitch.conf file to change during the installation or upgrade of the sudo package. This could cause various services to be unable to access the file. In reported cases, this bug prevented PostgreSQL from starting. This update fixes the bug and the file's permissions are no longer changed in the described scenario.

BZ#846694

The policycoreutils package dependency, which includes the restorecon utility, was set to Requires only. Consequently, the installation proceeded in the incorrect order and restorecon was required before it was installed. This bug has been fixed by using a context marked dependency "Requires(post)" and "Requires(postun)", and the installation now proceeds correctly.

Enhancement

BZ#840097

The sudo utility is able to consult the /etc/nsswitch.conf file for sudoers entries and look them up in files or in LDAP. Previously, when a match was found in the first database of sudoers entries, the look-up operation still continued in other databases. This update adds an option to the /etc/nsswitch.conf file that allows specifying a database. Once a match was found in the specified database, the search is finished. This eliminates the need to query any other databases; thus, improving the performance of sudoers entry look ups in large environments. This behavior is not enabled by default and must be configured by adding the "[SUCCESS=return]" string after a selected database. When a match is found in a database that directly precedes this string, no other databases are queried.

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

4.173.4. RHSA-2012:1149 — Moderate: sudo security and bug fix update

An updated sudo package that fixes one security issue and several bugs is 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 for each vulnerability from the CVE link(s) 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 Fix

CVE-2012-3440

An insecure temporary file use flaw was found in the sudo package's post-uninstall script. A local attacker could possibly use this flaw to overwrite an arbitrary file via a symbolic link attack, or modify the contents of the "/etc/nsswitch.conf" file during the upgrade or removal of the sudo package.

Bug Fixes

BZ#844418

Previously, sudo escaped non-alphanumeric characters in commands using "sudo -s" or "sudo -" at the wrong place and interfered with the authorization process. Some valid commands were not permitted. Now, non-alphanumeric characters escape immediately before the command is executed and no longer interfere with the authorization process.

BZ#844419

Prior to this update, the sudo utility could, under certain circumstances, fail to receive the SIGCHLD signal when it was executed from a process that blocked the SIGCHLD signal. As a consequence, sudo could become suspended and fail to exit. This update modifies the signal process mask so that sudo can exit and sends the correct output.

BZ#842759

The sudo update RHSA-2012:0309 introduced a regression that caused the Security-Enhanced Linux (SELinux) context of the "/etc/nsswitch.conf" file to change during the installation or upgrade of the sudo package. This could cause various services confined by SELinux to no longer be permitted to access the file. In reported cases, this issue prevented PostgreSQL and Postfix from starting.

BZ#844420

Updating the sudo package resulted in the "sudoers" line in "/etc/nsswitch.conf" being removed. This update corrects the bug in the sudo package's post-uninstall script that caused this issue.

BZ#844978

Prior to this update, a race condition bug existed in sudo. When a program was executed with sudo, the program could possibly exit successfully before sudo started waiting for it. In this situation, the program would be left in a zombie state and sudo would wait for it endlessly, expecting it to still be running.

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

4.173.5. RHSA-2012:1081 — Moderate: sudo security update

An updated sudo 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 for each vulnerability from the CVE link(s) 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 Fix

CVE-2012-2337

A flaw was found in the way the network matching code in sudo handled multiple IP networks listed in user specification configuration directives. A user, who is authorized to run commands with sudo on specific hosts, could use this flaw to bypass intended restrictions and run those commands on hosts not matched by any of the network specifications.

All users of sudo are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

4.174. symlinks

4.174.1. RHBA-2012:1134 — symlinks bug fix update

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

The symlinks utility is used for maintenance of symbolic links.

Bug Fix

BZ#578597

On 32-bit systems, support for files larger than 2 GB was not enabled. This caused failures when running the symlinks utility in directories containing symbolic links to large files. This update enables large file support so that the utility works as expected in this scenario.

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

4.175. syslinux

4.175.1. RHBA-2013:0086 — syslinux bug fix update

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

The syslinux packages provide a utility, which is responsible for booting the operating system kernel.

Bug Fixes

BZ#471067

Prior to this update, the syslinux utility used an inappropriate timeout value. As a consequence, the timeout took longer than expected. This update modifies the underlying code to remove this limitation. Now, syslinux timeouts work as expected.

BZ#844250

Prior to this update, the syslinux-perl package contained unresolved Perl dependencies. As a consequence, syslinux-perl failed to build. This update modifies the underlying code to resolve these dependencies. Now, syslinux-perl builds as expected.

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

4.176. sysstat

4.176.1. RHBA-2012:1219 — sysstat bug fix update

Updated sysstat packages that fix four bugs are now available for Red Hat Enterprise Linux 5.

The sysstat packages provide a set of utilities which enable system monitoring of disks, network, and other I/O activity.

Bug Fixes

BZ#706333

Prior to this update, the cifsiostat utility did not report the correct number of open files on CIFS file systems. This update modifies the underlying code to output the correct number of open files on CIFS file systems.

BZ#725266

Prior to this update, the argument for the "-i" option of the "sar" command used intervals of quarter seconds instead of seconds. This update modifies the underlying code to print the output in the chosen time interval.

BZ#801701

Prior to this update, the device minor number was limited to 256. As a consequence, the "-p" option of the "sar" command incorrectly displayed device names greater than 256 as "nodev" or "dev-[major number]-[minor number]". This update increases the value of the IOC_MAXNIMOR constant. Now, devices names with minor numbers greater than 256 are displayed correctly in the "sar" output.

BZ#805635

Prior to this update, both disks and partitions were considered for full statistics. As a consequence, the "-b" option of the "sar" command could, under certain circumstances, double the actual value. This update adds a test to check whether a name is a device or a partition before summing. Now, the output represents the actual values.

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

4.177. system-config-bind

4.177.1. RHBA-2013:0037 — system-config-bind bug fix update

Updated system-config-bind packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The system-config-bind packages provide a graphical user interface (GUI) to configure the Berkeley Internet Name Domain (BIND) Domain Name System (DNS) server.

Bug Fix

BZ#669757

Prior to this update, the system-config-bind tool did not correctly handle IPv6 addresses without at least one zero sequence. As a consequence, system-config-bind could fail to start with the error "string index out of range" when the full IPv6 address in a configuration file did not contain any zero sequence. This update modifies the underlying code to handle IPv6 addresses without a zero-sequence as expected. Now, all IPv6 addresses can be used.

All users of system-config-bind are advised to upgrade to these updated packages, which fix this bug.

4.178. system-config-cluster

4.178.1. RHBA-2013:0046 — system-config-cluster bug fix update

An updated system-config-cluster package that fixes several bugs is 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#741292

When a cluster service with the "__independent_subtree" attribute was edited, this attribute was stripped after saving the cluster configuration using the system-config-cluster utility. This bug has been fixed and the "__independent_subtree" attribute is no longer removed from services in this situation.

BZ#808498, BZ#824451

The cluster schema bundled with the system-config-cluster utility was missing the "suborg" attribute for fence_cisco_ucs, and the following attributes for fence_ipmilan: "cipher", "privlvl", "delay", "power_wait", and "timeout". As a consequence, any cluster configuration that included these attributes failed validation. This update adds the missing attributes to the cluster schema.

BZ#837045

The system-config-cluster utility did not allow users to configure fencing when an unknown fencing device which was supported by the cluster, but not by system-config-cluster was defined in the cluster configuration. Consequently, having such a fence device in the cluster.conf file caused system-config-cluster to produce a non-fatal traceback and refuse to show any configuration options for that device, or for fencing devices in general. This bug has been fixed and system-config-cluster works as expected in such a case.

All users are advised to upgrade to this updated system-config-cluster package, which fixes these bugs.

4.179. system-config-lvm

4.179.1. RHBA-2013:0070 — system-config-lvm bug fix update

An updated system-config-lvm package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The system-config-lvm package contains a utility for configuring logical volumes (LVs) using a graphical user interface.

Bug Fixes

BZ#834231

The system-config-lvm utility did not start correctly when there were too many existing LVs and returned a traceback. This was due to a bug in the best_fit function, which tried to fit all existing LVs into the display area. This update modifies the underlying source code to make the system-config-lvm utility fully functional even when there are more then 350 LVs existing on the system.

BZ#700253

Initializing a disk via the system-config-lvm utility with an EFI GPT partition table did not work correctly because the fdisk utility, which is used by system-config-lvm to manipulate disk partition tables, does not support EFI GPT partition tables. With this update, attempting to initialize a disk using an EFI GPT partition table returns an informative error message. Support for EFI GPT partition tables was not added.

All users of system-config-lvm are advised to upgrade to this updated package, which fixes these bugs.

4.180. system-config-netboot

4.180.1. RHBA-2012:1147 — system-config-netboot bug fix update

Updated system-config-netboot packages that that fix one bug are now available for Red Hat Enterprise Linux 5.

System-config-netboot is a utility which allows the configuration of diskless environments and network installations.

Bug Fix

BZ#772950

Prior to this update, deletion of a pxeos entry only removed its description from the pxeos.xml file and not from the default pxe configuration file as described in the pxeos manual page. With this update, the change is reflected in both the pxeos.xml file and the default pxe configuration file.

All users of system-config-netboot are advised to upgrade to these updated packages, which fix this bug.

4.181. system-config-printer

4.181.1. RHBA-2013:0051 — system-config-printer bug fix update

Updated system-config-printer packages that fix three bugs are now available for Red Hat Enterprise Linux 5.

The system-config-printer packages provide a print queue configuration tool with a graphical user interface.

Bug Fixes

BZ#472398

Prior to this update, the system-config-printer tool did not allow to keep the Server Settings page selected. As a consequence, a blank window was displayed after adjusting the server settings. This update modifies the underlying code so that the Server Settings page remains visible after changes have been applied.

BZ#651854

Prior to this update, the system-config-printer tool failed to check correctly whether all components of the driver were present when the generic PostScript driver was used. As a consequence, the PostScript printer could fail to start with the error "local variable 'exe' referenced before assignment". This update modifies the underlying code to check for the driver components and the postscript printer now starts as expected.

BZ#719459

Prior to this update, the authentication details of a queue that was configured for printing to an SMB share were not correctly encoded in the device URI if the password contained an "@" symbol. As a consequence, CUPS could not parse the Device URI correctly and the "Add Printer" operation failed. This update uses percent-encoding for the "@" symbol. Now, the "Add Printer" operation works as expected.

All users of system-config-printer are advised to upgrade to these updated packages, which fix these bugs.

4.182. systemtap

4.182.1. RHBA-2013:0058 — systemtap bug fix and enhancement update

Updated systemtap packages that fix multiple bugs and add various enhancements are now available for Red Hat Enterprise Linux 5.

SystemTap is a tracing and probing tool to analyze and monitor activities of the operating system, including the kernel. It provides a wide range of filtering and analysis options.

Note

The systemtap packages have been upgraded to upstream version 1.8, which provides a number of bug fixes and enhancements over the previous version. (BZ#751479)

Bug Fix

BZ#843392

Prior to this update, updating the systemtap package on client machines could fail because the systemap-testsuite is not designed for these machines. To work around this problem, remove the systemtap-testsuite subpackage before upgrading the systemtap package on client machines.

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

4.182.2. RHSA-2012:0376 — Moderate: systemtap security update

Updated systemtap 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 for each vulnerability from the CVE link(s) associated with each description below.

SystemTap is an instrumentation system for systems running the Linux kernel. The system allows developers to write scripts to collect data on the operation of the system.

Security Fix

CVE-2012-0875

An invalid pointer read flaw was found in the way SystemTap handled malformed debugging information in DWARF format. When SystemTap unprivileged mode was enabled, an unprivileged user in the stapusr group could use this flaw to crash the system or, potentially, read arbitrary kernel memory. Additionally, a privileged user (root, or a member of the stapdev group) could trigger this flaw when tricked into instrumenting a specially-crafted ELF binary, even when unprivileged mode was not enabled.

SystemTap users should upgrade to these updated packages, which contain a backported patch to correct this issue.

4.183. tar

4.183.1. RHBA-2012:0580 — tar bug fix update

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

The GNU tar program saves many files together in one archive and can restore individual files (or all of the files) from that archive.

Bug Fix

BZ#813245

Previously, the tar utility was unable to extract (using the "-x" or "--extract" option) or list (using the "-t" or "list" option) files from an archive in an older GNU format if the archive contained files with long paths and if the length of the member name was divisible by the block size of 512. This happened because tar read an extra block of data after a long name header and the file pointer was consequently set off. An upstream patch has been applied to address this problem, and the tar utility now lists and extracts files as expected under these circumstances.

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

4.184. tcl

4.184.1. RHSA-2013:0122 — Moderate: tcl security and bug fix update

Updated tcl packages that fix two security issues and one bug 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Tcl (Tool Command Language) provides a powerful platform for creating integration applications that tie together diverse applications, protocols, devices, and frameworks. When paired with the Tk toolkit, Tcl provides a fast and powerful way to create cross-platform GUI applications.

Security Fix

CVE-2007-4772, CVE-2007-6067

Two denial of service flaws were found in the Tcl regular expression handling engine. If Tcl or an application using Tcl processed a specially-crafted regular expression, it would lead to excessive CPU and memory consumption.

Bug Fix

BZ#478961

Due to a suboptimal implementation of threading in the current version of the Tcl language interpreter, an attempt to use threads in combination with fork in a Tcl script could cause the script to stop responding. At the moment, it is not possible to rewrite the source code or drop support for threading entirely. Consequent to this, this update provides a version of Tcl without threading support in addition to the standard version with this support. Users who need to use fork in their Tcl scripts and do not require threading can now switch to the version without threading support by using the alternatives command.

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

4.185. tcsh617

4.185.1. RHBA-2013:0052 — tcsh617 bug fix update

Updated tcsh617 package that fixes three bugs is now available for Red Hat Enterprise Linux 5.

The tcsh617 package is a mutually-exclusive replacement for the tcsh package. Tcsh is a command language interpreter compatible with the C shell (csh), which can be used as an interactive login shell, as well as a shell script command processor.

Bug Fixes

BZ#648592

Prior to this update, the tcsh617 processes were not handling the ".history" file exclusively. Consequently, when running several tcsh617 processes simultaneously, the .history file got malformed. This behavior, apart from corrupting .history content, slowed down the startup of the tcsh617 scripts. With this update, the .history file locking mechanism has been introduced. As a result, the file is merged correctly after modification by several processes.

BZ#759132

The tcsh617 package introduced a change in the default value of the $status variable for lists and pipelines. This change was made to provide compatibility with POSIX-compliant shells, like bash, ksh, resh, etc. However, the modification affected existing applications, which relied on previous

csh behavior, present for many years. With this update, the $status value has been reverted to the csh default. In addition, the $tcsh_posix_status variable has been added to opt-in the POSIX-like behavior. As a result, compliance with both csh and POSIX is made possible within tcsh617.

BZ#858281

Due to a syntax error in the tcsh617 package, the source command failed to function correctly when a single-line if-statement was used. This bug has been fixed and the source command now works properly in the described scenario.

All users of tcsh617 are advised to upgrade to this updated package, which fixes these bugs.

4.186. telnet

4.186.1. RHBA-2012:1035 — telnet bug fix update

Updated telnet packages that fix four bugs are now available for Red Hat Enterprise Linux 5.

Telnet is a popular protocol for logging in to remote systems over the Internet. The telnet service is disabled by default.

Bug Fixes

BZ#440614

Prior to this update, the telnet.spec file used the "%{dist}" macro instead of the "%{?dist}", which violated packaging guidelines. This update replaces the macro with the correct one.

BZ#678336

Prior to this update, the telnet utility used the sockaddr structure as storage for IPv6 addresses. As a consequence, telnet could emit incomplete IPv6 addresses because the sockaddr structure is to small to hold an IPv6 address. This update modifies telnet to use the sockaddr_storage structure as IPv6 address storage and now emits complete IPv6 addresses.

BZ#772860

Prior to this update, the telnet utility could enter an infinite loop when the user specified the "-b" parameter with a non-existing network interface. This update modifies the telnet command to print errors when users specify a non-existing network interface.

BZ#825946

Prior to this update, the in.telnetd daemon could fail to update information in the /var/run/utmp directory when a deadlock occured in a telnet session. This update modifies telnetd to update /var/run/utmp correctly.

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

4.187. tomcat5

4.187.1. RHBA-2013:0014 — tomcat5 bug fix update

Updated tomcat5 packages that fix various bugs are available for Red Hat Enterprise Linux 5.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

Bug Fixes

BZ#493007

Symbolic links to system libraries could be lost rendering Tomcat unusable if a problem occurred during Tomcat start while the RELINK script was running. The event triggering the problem could have been any kind of start interruption, such as closing Tomcat with CTRL+C, driver crash, power outage, and so on. With this update, to provide a workaround for this issue, the RELINK script is called only if explicitly required by the user as the problem is caused by a subordinate utility script, which does not belong to Tomcat.

BZ#530089

When the tomcat server parsed a cookie whose name contained either single- or double-quotes and then passed that cookie name and value to a servlet, any quotes were removed from the cookie name as expected; however, the cookie values were empty. This update corrects the parsing so that single- or double-quotes can be used inside cookie names and the correct cookie values are returned.

BZ#543995

The OPTION request did not return the TRACE method as an allowed method and incorrectly reported TRACE as an allowed method. With this update, the information returned to the OPTION request has been corrected.

BZ#689924

Previously, context.xml files that did not specify the Document Base (docBase) property caused Tomcat to fail on startup with a NullPointerException. With this update, if the docBase property is not defined, it is handled gracefully and the path name to the context is used as docBase. Note that when deploying a context, the docBase attribute is mandatory.

BZ#578648

On IBM S/390 and 64-bit PowerPC architectures, Tomcat Administration Tool terminated unexpectedly and accessing failed with HTTP Status 404 as JSP pre-compilation was disabled. With this update, JSP has been pre-compiled so that compilation at runtime is not needed and Tomcat Administration Tool can be accessed in this scenario.

BZ#691833

When a context was deployed with a web application and the etc/localhost/[webapp].xml file existed, tomcat threw a NullPointerException. With this update, the bug no longer occurs.

BZ#548961

Previously, java.util.logging was not working due to the missing tomcat-juli.jar library in Tomcat. The library has been added and the Tomcat logging works as expected.

BZ#587215

The /etc/init.d/tomcat5 script returned an incorrect exit status when stopped. With this update, the correct exit value is returned on stop.

Users are advised to upgrade to these updated tomcat5 packages, which fix these bugs.

4.187.2. RHSA-2012:0474 — Moderate: tomcat5 security update

Updated tomcat5 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Apache Tomcat is a servlet container for the Java Servlet and JavaServer Pages (JSP) technologies.

Security Fixes

CVE-2011-4858

It was found that the Java hashCode() method implementation was susceptible to predictable hash collisions. A remote attacker could use this flaw to cause Tomcat to use an excessive amount of CPU time by sending an HTTP request with a large number of parameters whose names map to the same hash value. This update introduces a limit on the number of parameters processed per request to mitigate this issue. The default limit is 512 for parameters and 128 for headers. These defaults can be changed by setting the org.apache.tomcat.util.http.Parameters.MAX_COUNT and org.apache.tomcat.util.http.MimeHeaders.MAX_COUNT system properties.

CVE-2012-0022

It was found that Tomcat did not handle large numbers of parameters and large parameter values efficiently. A remote attacker could make Tomcat use an excessive amount of CPU time by sending an HTTP request containing a large number of parameters or large parameter values. This update introduces limits on the number of parameters and headers processed per request to address this issue. Refer to the CVE-2011-4858 description for information about the org.apache.tomcat.util.http.Parameters.MAX_COUNT and org.apache.tomcat.util.http.MimeHeaders.MAX_COUNT system properties.

Red Hat would like to thank oCERT for reporting CVE-2011-4858. oCERT acknowledges Julian Wälde and Alexander Klink as the original reporters of CVE-2011-4858.

Users of Tomcat should upgrade to these updated packages, which correct these issues. Tomcat must be restarted for this update to take effect.

4.188. tzdata

4.188.1. RHEA-2012:0412 — tzdata enhancement update

An updated tzdata package that brings Daylight Saving Time observations in four locales up-to-date is now available.

The tzdata package contains data files with rules for various time zones around the world.

This updated package adds the following time-zone changes to the zone info database:

BZ#802460, BZ#802541, BZ#802542, BZ#802543,

On 2012-03-15, Morocco announced it will switch to daylight savings time (DST) on the last Sunday in April (29th April) and not the 25th of March. The earlier date was announced as the daylight savings switch date on 2012-03-09. The change was made "after discussion of proposals to consider the demands of schooling", according to Mustapha El Khalfi, the Morocco Minister of Communications. The switch back to standard Moroccan time will still occur at 03:00 on the last Sunday in September, 2012-09-30. This update reflects the later switching date announced on 2012-03-15.

Note: the 2012-03-09 announcement also noted Morocco DST will run to September 30, 2012 "except the month of Ramadan". Relative to the Gregorian calendar, Ramadan runs from 2012-07-

20 to 2012-08-18 this year. Specific times for this temporary switching to Morocco standard time and then back to Morocco DST were not available as of this errata's publication, however. Consequently this mooted exception is not yet included in the tzdata package.

BZ#802460, BZ#802541, BZ#802542, BZ#802543,

Armenia announced it will abolish local daylight savings time observance. This update reflects this: the Armenian time-zone will not advance an hour on 2012-03-24 as was previously set.

BZ#802460, BZ#802541, BZ#802542, BZ#802543,

The Falkland Islands announced it will remain on Falklands Summer Time for the rest of 2012 and will likely remain so for future years. This update assumes a permanent summer time for the Falkland Islands until advised differently.

BZ#802460, BZ#802541, BZ#802542, BZ#802543,

Cuba has delayed the 2012 DST switch by three weeks. Originally set to switch at 01:00 2012-03-11, Cuba will now switch to local DST at 01:00 2012-04-01. The switch back to standard time remains unchanged at 2012-11-13. This update incorporates the delayed DST switch for Cuba.

Note: other changes noted in the bug reports referenced above (for example, the changes to Chile’s DST observance for 2012 and 2013) were previously incorporated into the tzdata package.

All users, especially those in the locale affected by these time changes, and users interacting with people or systems in the affected locale, are advised to upgrade to this updated package, which adds these enhancements.

4.188.2. RHEA-2012:0356 — tzdata enhancement update

An updated tzdata package that updates Daylight Saving Time observations is now available.

The tzdata package contains data files with rules for various time zones around the world.

This updated package addresses the following changes in zone info database:

BZ#782174, BZ#782173, BZ#782172, BZ#773755

The leap second database now includes the leap second that will occur at the end of June 2012. Note that only zones in the subdirectory called "right/" are affected. Unless you set up your system to specifically use "right" time zones, this change will not affect you in any way. Normally, the information about leap seconds is distributed via the NTP protocol, and the NTP client should update your system properly even without this update.

BZ#796569, BZ#796747, BZ#796748, BZ#796749

This update changes the Daylight Saving Time rules for Chile, which decided to exit DST on March 11 2012 instead of the previous date of April 28th 2012

* This update retroactively changes the Daylight Saving Time rules for Cuba, which left the period of DST in November.

* This update retroactively changes the Daylight Saving Time rules for Fiji, which entered DST in January.

All users, especially those in the locale affected by these time changes, and users interacting with people or systems in the affected locale, are advised to upgrade to this updated package, which adds this enhancement.

4.188.3. RHEA-2012:0689 — tzdata enhancement update

Updated tzdata packages that add several enhancements are now available for Red Hat Enterprise Linux.

The tzdata packages contain data files with rules for various time zones around the world.

Enhancements

BZ#820689, BZ#820732, BZ#821326, BZ#821327

The following time-zone changes have been added to the zone info database: Haiti entered a period of Daylight Saving Time (DST) on March 11; Gaza Strip, West Bank and Syria entered a period of DST on March 30.

All users, especially those in the locale affected by these time changes, and users interacting with people or systems in the affected locale, are advised to upgrade to these updated packages, which add these enhancements.

4.188.4. RHEA-2012:1101 — tzdata enhancement update

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

The tzdata packages contain data files with rules for various time zones around the world.

Enhancement

BZ#839271, BZ#839934, BZ#839937, BZ#839938

Daylight Saving Time will be interrupted during the holy month of Ramadan in Morocco (that is July 20 - August 19, 2012 in the Gregorian Calendar). This update incorporates the exception so that Daylight Saving Time is turned off and the time setting returned back to the standard time during Ramadan.

All users of tzdata are advised to upgrade to these updated packages, which add this enhancement.

4.188.5. RHEA-2012:1338 — tzdata enhancement update

Updated tzdata packages that add two enhancements are now available for Red Hat Enterprise Linux.

The tzdata packages contain data files with rules for various time zones around the world.

Enhancements

BZ#857904, BZ#857905, BZ#857906, BZ#857907

Daylight saving time in Fiji will start at 2:00 a.m. on Sunday, 21st October 2012, and end at 3 am or Sunday, 20th January 2013.

BZ#857904, BZ#857905, BZ#857906, BZ#857907

Tokelau was listed in an incorrect time zone for as long as the Zoneinfo project was in existence. The actual zone was supposed to be GMT-11 hours before Tokelau was moved to the other side of the International Date Line at the end of year 2011. The local time in Tokelau is now GMT+13.

All users of tzdata are advised to upgrade to these updated packages, which add these enhancements.

4.188.6. RHEA-2012:1488 — tzdata enhancement update

A new tzdata package that updates Daylight Saving Time observations for several countries is now available.

The tzdata packages contain data files with rules for various time zones around the world.

This updated package adds the following time-zone changes to the zone info database:

BZ#871993, BZ#871791, BZ#871994, BZ#871995

On October 24 2012, the Jordanian Cabinet rescinded a 2012-10-14 instruction to switch from daylight saving time (DST) to standard time on 2012-10-26. Instead, Jordan will remain on local DST (ITC +3) for the 2012-2013 Jordanian winter.

BZ#871993, BZ#871791, BZ#871994, BZ#871995

Cuba, which was scheduled to move back to standard time on 2012-11-12, switched to standard time on 2012-11-04.

* In Brazil, the North Region state, Tocantins, will observe DST in 2012-2013. This is the first time Tocantins has observed DST since 2003. By contrast, Bahia, a Northeast Region state, will not observe DST in 2012-2013. Like Tocantins, Bahia stopped observing DST in 2003. Bahia re-introduced DST on October 16 2011. On October 17 2012, however, Bahia Governor, Jaques Wagner, announced DST would not be observed in 2012, citing public surveys showing most Bahia residents were opposed to it.

BZ#871993, BZ#871791, BZ#871994, BZ#871995

Israel has new DST rules as of 2013. DST now starts at 02:00 on the Friday before the last Sunday in March. DST now ends at 02:00 on the first Sunday after October 1, unless this day is also the second day of (Rosh Hashanah). In this case, DST ends a day later, at 02:00 on the first Monday after October 2.

* The Palestinian territories, which were scheduled to move back to standard time on 2012-09-28, switched to standard time on 2012-09-21.

* Although Western Samoa has observed DST for two consecutive seasons (2010-2011 and 2011-2012), there is no official indication of DST continuing according to a set pattern for the foreseeable future. On 2012-09-04, the Samoan Ministry of Commerce, Industry, and Labour announced Samoa would observe DST from Sunday, 2012-09-30 until Sunday 2012-04-07.

All users, especially those in the locale affected by these time changes, and users interacting with people or systems in the affected locale, are advised to upgrade to this updated package, which includes these updates.

4.189. udev

4.189.1. RHBA-2013:0091 — udev bug fix update

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

The udev packages implement a dynamic device directory, exposing the devices currently present on the system. The directory runs in user space, dynamically creates and removes devices, ensures consistent naming, and provides a user-space API.

Bug Fixes

BZ#736475

On system boot, the udev helper application, pam_console_apply, was called for every disk on the system. This was unnecessary for example for SCSI disks, which do not have default pam console permissions. As a consequence, the boot process was significantly slowed down if the system

contained a large number of disks. To fix this problem, the /etc/udev/rules.d/95-pam-console.rules file has been marked as a configuration file and it will not be automatically updated with newer udev versions. System administrators should now comment out the pam_console_apply call in this file on systems that do not need non-root user access to devices.

BZ#758205

Previously, the udev helper tool for loading firmware into drivers was logging to syslog only. Consequently, there was no output in the early boot stage when the syslog daemon was not running. With this update, if the udevd daemon is running in debug mode, the firmware_helper also logs to the console, which helps to debug firmware loading problems.

BZ#769169

The WAIT_FOR_SYSFS variable in the udev rules was set to wait 3 seconds for a file in the sysfs file system to appear. This timeout was too low for some hot-added SCSI disks that need at least 6 seconds to spin up. Therefore no symbolic links in the /dev/disk/ directory were created. The WAIT_FOR_SYSFS variable has been set to 10 seconds, which is enough for most disks. This results in proper udev database entries and symbolic links.

BZ#812286

Prior to this update, udev used the target's port identifier instead of the initiator's PHY identifier in the /dev/disk/by-path symbolic link. Consequent to this, when the disk was hot-removed and hot-added, the symbolic link used a different pathname. This bug has been fixed and udev now uses the correct initiator's PHY identifier in the symbolic link, which remains the same for re-added disks.

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

4.190. util-linux

4.190.1. RHBA-2012:1437 — util-linux bug fix update

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

The util-linux packages contain a set of low-level system utilities that are necessary for a Linux operating system to function.

Bug Fix

BZ#865791

Due to a regression, the fdisk utility did not provide kernel with updated information about new partition table on some systems. Consequently, fdisk failed to partition a disk not in use at the time. A patch has been provided to address this issue and fdisk now works as expected in the described scenario.

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

4.191. vim

4.191.1. RHBA-2013:0066 — vim bug fix update

Updated vim packages that fix various bugs are now available for Red Hat Enterprise Linux 5.

Vim (Vi IMproved) is an updated and improved version of the vi editor.

Bug Fixes

BZ#591578

Previously, when using the VimExplorer file manager with the locale set to Simplified Chinese (zh_CN), the netrw.vim script inserted an unwanted "e" character in front of file names. The underlying code has been modified so that file names are now displayed correctly, without unwanted characters.

BZ#681108

Under certain circumstances, when doing completion in Vim, the text editor entered a recursive function call without returning and stopped responding to user input. With this update, a patch has been applied to prevent such a recursive loop.

BZ#825307

When using the file explorer in a subdirectory of the root directory, the "vim .." command displayed only part of the root directory's content. A patch has been applied to address this issue, and the "vim .." command now lists the content of the root directory properly in the described scenario.

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

4.192. virt-who

4.192.1. RHBA-2013:0072 — virt-who bug fix and enhancement update

Updated virt-who packages that fix several bugs and add two enhancements are now available for Red Hat Enterprise Linux 5.

The virt-who packages provide an agent that collects information about virtual guests present in the system and reports them to the Red Hat Subscription Manager tool.

Bug Fixes

BZ#806226

Previously, when executing the "service virt-who restart" command on a virtual machine via the secure shell (SSH) network protocol, the security lock prevented the service from reconnecting after the restart. Therefore, when running two virtual machines simultaneously, restarting the first machine reported the following message in the output of the "virt-who service status" command executed on the second machine:

virt-who dead but pid file exists

The bug has been fixed, and the virt-who agent now handles the aforementioned situation properly.

BZ#812736

Prior to this update, the virt-who agent failed to monitor the guest start event after performing a specific set of user operations. Consequently, the virt.uuid of the guest could not be reported. The bug has been fixed, and the virt.uuid identifications are now provided correctly regardless of previous operations.

BZ#848777

Previously, when starting the virt-who service with the "virt-who -d" command, the background loop was created, even though the virt-who agent was not in the background mode. With this update, the background loop is no longer accidentally initiated in the described scenario.

BZ#848788

Previously, when the virt-who agent was started as a service in the background, the debug log appeared in the shell prompt. This behavior has been corrected, and the debug log is no longer displayed in the aforementioned case.

BZ#849921

In the virt-who configuration file, setting the "VIRTWHO_INTERVAL" option to any number enables sending a list of virtual guests to a log file automatically at the given time interval. Due to a bug, this functionality was blocked, therefore the log file was not updated as expected. The bug has been fixed, and now the log file is updated as frequently as set in the "VIRTWHO_INTERVAL" option.

BZ#853371

Previously, when the virt-who agent was running in debug mode, it failed to create or recover a connection to a virtual machine. Consequently, the following message was displayed:

ERROR: Unable to create connection

With this update, the bug has been fixed and the virt-who agent properly connects with the debug mode enabled.

BZ#859841

Previously, when running the virt-who service in vdsm mode, unregistering the system from the SAM (Red Hat Subscription Asset Manager) server caused the service to crash with the following message:

virt-who dead but subsys locked

This bug has been fixed and virt-who now works properly in the described case.

BZ#861563

Previously, when running the "service virt-who restart" command repeatedly in very short time intervals, the command failed to stop the virt-who process, but started a new process successfully. Consequently, many virt-who processes could have ended up running simultaneously. This bug has been fixed, and running "service virt-who restart" repeatedly no longer results in multiple processes being started.

Enhancements

BZ#808061

With this update, the virt-who agent has been modified to start as a foreground process and to print error messages or debugging output (the "-d" command line option) to standard error. Moreover, the following command line options have been enhanced: the "-o" option provides the one-shot mode and exits after sending the list of guests; the "-b" option and the "service virt-who start" command equivalently start on the background and send data to the /var/log/ directory.

BZ#848781

With this update, a man page has been added to the virt-who package. As a result, a proper description of virt-who is provided.

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

4.193. vsftpd

4.193.1. RHBA-2012:0537 — vsftpd bug fix update

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

The vsftpd package includes a Very Secure FTP (File Transfer Protocol) daemon.

Bug Fix

BZ#813567

Previously, the vsftpd daemon did not correctly handle a situation when it received the EADDRINUSE error from a TCP port which vsftpd was listening on. In such a case, vsftpd immediately sent an error message to an FTP client instead of retrying to use the port. This update modifies error handling of vsftpd so that the daemon now retries to use the port before sending the error message to the FTP client in this scenario.

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

4.193.2. RHBA-2013:0025 — vsftpd bug fix update

Updated vsftpd packages that fix multiple bugs are now available for Red Hat Enterprise Linux 5.

The vsftpd packages provide the VSFTP (Very Secure File Transfer Protocol) daemon.

Bug Fixes

BZ#795393

Prior to this update, the "local_max_rate" option did not work as expected. As a consequence, the transmission speed was significantly lower. This update extends the types of variables for calculating and accumulating the amount of transferred data and postpones the start of evaluation after the tenth.

BZ#799245

Prior to this update, the "ls" command failed to handle the wildcard character "?" correctly. This update modifies the "ls" code so that the "ls" command can now uses the wildcard character "?" as expected.

BZ#804078

Prior to this update, the file transfer on a TLS connection failed after transferring the first files when the "ssl_request_cert" option used the default setting "YES". This update modifies the underlying code so that the file transfer completes as expected.

BZ#809450

Prior to this update, the vsftpd daemon did not correctly handle "EADDRINUSE" errors received from a TCP port on which vsftpd was listening. As a consequence, vsftpd immediately sent an error message to an FTP client instead of retrying to use the port. This update modifies the error handling of vsftpd so that the daemon now retries the port before sending the error message to the

FTP client.

BZ#845051

Prior to this update, the vsftpd daemon failed with the message "500 OOPS: vsf_sysutil_bind" when the ports from the range configured for passive mode were occupied. This could occur when repeating the "ls" command on the empty sub-directory in the FTP client. The updated daemon is able to reuse ports from the approved range that are in the state TIME_WAIT and the described failure is no more observed.

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

4.194. wget

4.194.1. RHBA-2012:0438 — wget bug fix update

An updated wget package that fixes one bug is now available for Red Hat Enterprise Linux 5.

GNU Wget is a file retrieval utility which can use either the HTTP of FTP protocols.

Bug Fix

BZ#802438

Previously, the wget utility failed with the "Connection timed out" message when running the utility to get data from Microsoft Windows Server 2003 that had returned an error for the "PORT" request. This was because wget did not correctly handle the error in the accept_connection() function and therefore did not attempt to retry upon the connection timeout. The underlying source code has been modified to ensure that wget retries the connection in the described scenario.

All users of wget are advised to upgrade to this updated package, which fixes this bug.

4.194.2. RHBA-2012:0560 — wget bug fix update

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

GNU Wget is a file retrieval utility which can use either the HTTP, HTTPS or FTP protocol. Wget provides various useful features, such as the ability to work in the background while the user is logged out, recursive retrieval of directories, file name wildcard matching or updating files in dependency on file timestamp comparison.

Bug Fix

BZ#815418

The wget utility did not previously work as intended with the "-T, --timeout" option set. As a consequence, if the HTTPS server accepted a wget session but did not respond to the SSL handshake, the timeout could not take effect and Wget did not terminate the session after a given time. With this update, the underlying source code has been modified to ensure that Wget aborts the connection in this scenario.

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

4.195. wireshark

4.195.1. RHSA-2013:0125 — Moderate: wireshark security, bug fix, and enhancement update

Updated wireshark packages that fix several security issues, three 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Wireshark, previously known as Ethereal, is a network protocol analyzer. It is used to capture and browse the traffic running on a computer network.

Security Fixes

CVE-2011-4102

A heap-based buffer overflow flaw was found in the way Wireshark handled Endace ERF (Extensible Record Format) capture files. If Wireshark opened a specially-crafted ERF capture file, it could crash or, possibly, execute arbitrary code as the user running Wireshark.

CVE-2011-1958, **CVE-2011-1959**, **CVE-2011-2175**, **CVE-2011-2698**, **CVE-2012-0041**, **CVE-2012-0042**, **CVE-2012-0066**, **CVE-2012-0067**, **CVE-2012-4285**, **CVE-2012-4289**, **CVE-2012-4290**, **CVE-2012-4291**

Several denial of service flaws were found in Wireshark. Wireshark could crash or stop responding if it read a malformed packet off a network, or opened a malicious dump file.

The CVE-2011-1958, CVE-2011-1959, CVE-2011-2175, and CVE-2011-4102 issues were discovered by Huzaifa Sidhpurwala of the Red Hat Security Response Team.

Bug Fixes

BZ#438473

When Wireshark starts with the X11 protocol being tunneled through an SSH connection, it automatically prepares its capture filter to omit the SSH packets. If the SSH connection was to a link-local IPv6 address including an interface name (for example ssh -X [ipv6addr]%eth0), Wireshark parsed this address erroneously, constructed an incorrect capture filter and refused to capture packets. The "Invalid capture filter" message was displayed. With this update, parsing of link-local IPv6 addresses is fixed and Wireshark correctly prepares a capture filter to omit SSH packets over a link-local IPv6 connection.

BZ#493693

Previously, Wireshark's column editing dialog malformed column names when they were selected. With this update, the dialog is fixed and no longer breaks column names.

BZ#580510

Previously, TShark, the console packet analyzer, did not properly analyze the exit code of Dumpcap, Wireshark's packet capturing back end. As a result, TShark returned exit code 0 when Dumpcap failed to parse its command-line arguments. In this update, TShark correctly propagates the Dumpcap exit code and returns a non-zero exit code when Dumpcap fails.

BZ#580513

Previously, the TShark "-s" (snapshot length) option worked only for a value greater than 68 bytes. If a lower value was specified, TShark captured just 68 bytes of incoming packets. With this update, the "-s" option is fixed and sizes lower than 68 bytes work as expected.

Enhancement

BZ#484999

In this update, support for the "NetDump" protocol was added.

All users of Wireshark are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement. All running instances of Wireshark must be restarted for the update to take effect.

4.196. tetex

4.196.1. RHSA-2012:1201 — Moderate: tetex security update

Updated tetex 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. Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

teTeX is an implementation of TeX. TeX takes a text file and a set of formatting commands as input, and creates a typesetter-independent DeVice Independent (DVI) file as output.

Security Fixes

CVE-2010-2642, **CVE-2011-0433**

teTeX embeds a copy of t1lib to rasterize bitmaps from PostScript Type 1 fonts. The following issues affect t1lib code:

Two heap-based buffer overflow flaws were found in the way t1lib processed Adobe Font Metrics (AFM) files. If a specially-crafted font file was opened by teTeX, it could cause teTeX to crash or, potentially, execute arbitrary code with the privileges of the user running teTeX.

CVE-2011-0764

An invalid pointer dereference flaw was found in t1lib. A specially-crafted font file could, when opened, cause teTeX to crash or, potentially, execute arbitrary code with the privileges of the user running teTeX.

CVE-2011-1553

A use-after-free flaw was found in t1lib. A specially-crafted font file could, when opened, cause teTeX to crash or, potentially, execute arbitrary code with the privileges of the user running teTeX.

CVE-2011-1554

An off-by-one flaw was found in t1lib. A specially-crafted font file could, when opened, cause teTeX to crash or, potentially, execute arbitrary code with the privileges of the user running teTeX.

CVE-2011-1552

An out-of-bounds memory read flaw was found in t1lib. A specially-crafted font file could, when opened, cause teTeX to crash.

CVE-2010-3702

teTeX embeds a copy of Xpdf, an open source Portable Document Format (PDF) file viewer, to allow adding images in PDF format to the generated PDF documents. The following issues affect

Xpdf code:

An uninitialized pointer use flaw was discovered in Xpdf. If pdflatex was used to process a TeX document referencing a specially-crafted PDF file, it could cause pdflatex to crash or, potentially, execute arbitrary code with the privileges of the user running pdflatex.

CVE-2010-3704

An array index error was found in the way Xpdf parsed PostScript Type 1 fonts embedded in PDF documents. If pdflatex was used to process a TeX document referencing a specially-crafted PDF file, it could cause pdflatex to crash or, potentially, execute arbitrary code with the privileges of the user running pdflatex.

Red Hat would like to thank the Evince development team for reporting CVE-2010-2642. Upstream acknowledges Jon Larimer of IBM X-Force as the original reporter of CVE-2010-2642.

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

4.197. thunderbird

4.197.1. RHSA-2012:0388 — Critical: thunderbird security update

An updated thunderbird package that fixes multiple 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2012-0461, **CVE-2012-0462**, **CVE-2012-0464**

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-2012-0456, **CVE-2012-0457**

Two flaws were found in the way Thunderbird parsed certain Scalable Vector Graphics (SVG) image files. An HTML mail message containing a malicious SVG image file could cause an information leak, or cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0455

A flaw could allow malicious content to bypass intended restrictions, possibly leading to a cross-site scripting (XSS) attack if a user were tricked into dropping a "javascript:" link onto a frame.

CVE-2012-0458

It was found that the home page could be set to a "javascript:" link. If a user were tricked into setting such a home page by dragging a link to the home button, it could cause Firefox to repeatedly crash, eventually leading to arbitrary code execution with the privileges of the user running Firefox. A similar flaw was found and fixed in Thunderbird.

CVE-2012-0459

A flaw was found in the way Thunderbird parsed certain, remote content containing "cssText". Malicious, remote content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0460

It was found that by using the DOM fullscreen API, untrusted content could bypass the mozRequestFullscreen security protections. Malicious content could exploit this API flaw to cause user interface spoofing.

CVE-2012-0451

A flaw was found in the way Thunderbird handled content with multiple Content Security Policy (CSP) headers. This could lead to a cross-site scripting attack if used in conjunction with a website that has a header injection flaw.

Note: All issues except CVE-2012-0456 and CVE-2012-0457 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 contains Thunderbird version 10.0.3 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.197.2. RHSA-2012:0516 — Critical: thunderbird security update

An updated thunderbird package that fixes multiple 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2011-3062

A flaw was found in Sanitiser for OpenType (OTS), used by Thunderbird to help prevent potential exploits in malformed OpenType fonts. Malicious content could cause Thunderbird to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0467, **CVE-2012-0468**, **CVE-2012-0469**

Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0470

Content containing a malicious Scalable Vector Graphics (SVG) image file could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0472

A flaw was found in the way Thunderbird used its embedded Cairo library to render certain fonts. Malicious content could cause Thunderbird to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0478

A flaw was found in the way Thunderbird rendered certain images using WebGL. Malicious content could cause Thunderbird to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-0471

A cross-site scripting (XSS) flaw was found in the way Thunderbird handled certain multibyte character sets. Malicious content could cause Thunderbird to run JavaScript code with the permissions of different content.

CVE-2012-0473

A flaw was found in the way Thunderbird rendered certain graphics using WebGL. Malicious content could cause Thunderbird to crash.

CVE-2012-0474

A flaw in the built-in feed reader in Thunderbird allowed the Website field to display the address of different content than the content the user was visiting. An attacker could use this flaw to conceal a malicious URL, possibly tricking a user into believing they are viewing a trusted site, or allowing scripts to be loaded from the attacker's site, possibly leading to cross-site scripting (XSS) attacks.

CVE-2012-0477

A flaw was found in the way Thunderbird decoded the ISO-2022-KR and ISO-2022-CN character sets. Malicious content could cause Thunderbird to run JavaScript code with the permissions of different content.

CVE-2012-0479

A flaw was found in the way the built-in feed reader in Thunderbird handled RSS and Atom feeds. Invalid RSS or Atom content loaded over HTTPS caused Thunderbird to display the address of said content, but not the content. The previous content continued to be displayed. An attacker could use this flaw to perform phishing attacks, or trick users into thinking they are visiting the site reported by the Website field, when the page is actually content controlled by an attacker.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Mateusz Jurczyk of the Google Security Team as the original reporter of CVE-2011-3062; Aki Helin from OUSPG as the original reporter of CVE-2012-0469; Atte Kettunen from OUSPG as the original reporter of CVE-2012-0470; wushi of team509 via iDefense as the original reporter of CVE-2012-0472; Ms2ger as the original reporter of CVE-2012-0478; Anne van Kesteren of Opera Software as the original reporter of CVE-2012-0471; Matias Juntunen as the original reporter of CVE-2012-0473; Jordi Chancel and Eddy Bordi, and Chris McGowen as the original reporters of CVE-2012-0474; Masato Kinugawa as the original reporter of CVE-2012-0477; and Jeroen van der Gun as the original reporter of CVE-2012-0479.

Note: All issues except CVE-2012-0470, CVE-2012-0472, and CVE-2011-3062 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.

4.197.3. RHSA-2012:0715 — Critical: thunderbird security update

An updated thunderbird package that fixes multiple 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2011-3101, **CVE-2012-1937**, **CVE-2012-1938**, **CVE-2012-1939**, **CVE-2012-1940**, **CVE-2012-1941**, **CVE-2012-1946**, **CVE-2012-1947**

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-2012-1944

Note: CVE-2011-3101 only affected users of certain NVIDIA display drivers with graphics cards that have hardware acceleration enabled.

It was found that the Content Security Policy (CSP) implementation in Thunderbird no longer blocked Thunderbird inline event handlers. Malicious content could possibly bypass intended restrictions if that content relied on CSP to protect against flaws such as cross-site scripting (XSS).

CVE-2012-1945

If a web server hosted content that is stored on a Microsoft Windows share, or a Samba share, loading such content with Thunderbird could result in Windows shortcut files (.lnk) in the same share also being loaded. An attacker could use this flaw to view the contents of local files and directories on the victim's system. This issue also affected users opening content from Microsoft Windows shares, or Samba shares, that are mounted on their systems.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Ken Russell of Google as the original reporter of CVE-2011-3101; Igor Bukanov, Olli Pettay, Boris Zbarsky, and Jesse Ruderman as the original reporters of CVE-2012-1937; Jesse Ruderman, Igor Bukanov, Bill McCloskey, Christian Holler, Andrew McCreight, and Brian Bondy as the original reporters of CVE-2012-1938; Christian Holler as the original reporter of CVE-2012-1939; security researcher Abhishek Arya of Google as the original reporter of CVE-2012-1940, CVE-2012-1941, and CVE-2012-1947; security researcher Arthur Gerkis as the original reporter of CVE-2012-1946; security researcher Adam Barth as the original reporter of CVE-2012-1944; and security researcher Paul Stone as the original reporter of CVE-2012-1945.

Note: None of the issues in this advisory can 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 10.0.5 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.197.4. RHSA-2012:1351 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2012-3982, CVE-2012-3988, CVE-2012-3990, CVE-2012-3995, CVE-2012-4179, CVE-2012-4180, CVE-2012-4181, CVE-2012-4182, CVE-2012-4183, CVE-2012-4185, CVE-2012-4186, CVE-2012-4187, CVE-2012-4188

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-2012-3986, CVE-2012-3991

Two flaws in Thunderbird could allow malicious content to bypass intended restrictions, possibly leading to information disclosure, or Thunderbird executing arbitrary code. Note that the information disclosure issue could possibly be combined with other flaws to achieve arbitrary code execution.

CVE-2012-1956, CVE-2012-3992, CVE-2012-3994

Multiple flaws were found in the location object implementation in Thunderbird. Malicious content could be used to perform cross-site scripting attacks, script injection, or spoofing attacks.

CVE-2012-3993, CVE-2012-4184

Two flaws were found in the way Chrome Object Wrappers were implemented. Malicious content could be used to perform cross-site scripting attacks or cause Thunderbird to execute arbitrary code.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Christian Holler, Jesse Ruderman, Soroush Dalili, miaubiz, Abhishek Arya, Atte Kettunen, Johnny Stenback, Alice White, moz_bug_r_a4, and Mariusz Mlynski as the original reporters of these issues.

Note: None of the issues in this advisory can 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 10.0.8 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.197.5. RHSA-2012:1362 — Critical: 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 critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fix

CVE-2012-4193

A flaw was found in the way Thunderbird handled security wrappers. Malicious content could cause Thunderbird to 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 moz_bug_r_a4 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.

4.197.6. RHSA-2012:1413 — Important: thunderbird security update

An updated thunderbird package that fixes multiple 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fix

CVE-2012-4194, CVE-2012-4195, CVE-2012-4196

Multiple flaws were found in the location object implementation in Thunderbird. Malicious content could be used to perform cross-site scripting attacks, bypass the same-origin policy, or cause Thunderbird to execute arbitrary code.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Mariusz Mlynski, moz_bug_r_a4, and Antoine Delignat-Lavaud as the original reporters of these issues.

Note: None of the issues in this advisory can 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 10.0.10 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.197.7. RHSA-2012:1483 — 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2012-4214, CVE-2012-4215, CVE-2012-4216, CVE-2012-5829, CVE-2012-5830, CVE-2012-5833, CVE-2012-5835, CVE-2012-5839, CVE-2012-5840, CVE-2012-5842

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-2012-4202

A buffer overflow flaw was found in the way Thunderbird handled GIF (Graphics Interchange Format) images. Content containing a malicious GIF image could cause Thunderbird to crash or, possibly, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-4207

A flaw was found in the way Thunderbird decoded the HZ-GB-2312 character encoding. Malicious content could cause Thunderbird to run JavaScript code with the permissions of different content.

CVE-2012-4209

A flaw was found in the location object implementation in Thunderbird. Malicious content could possibly use this flaw to allow restricted content to be loaded by plug-ins.

CVE-2012-5841

A flaw was found in the way cross-origin wrappers were implemented. Malicious content could use this flaw to perform cross-site scripting attacks.

CVE-2012-4201

A flaw was found in the evalInSandbox implementation in Thunderbird. Malicious content could use this flaw to perform cross-site scripting attacks.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Abhishek Arya, miaubiz, Jesse Ruderman, Andrew McCreight, Bob Clary, Kyle Huey, Atte Kettunen, Masato Kinugawa, Mariusz Mlynski, Bobby Holley, and moz_bug_r_a4 as the original reporters of these issues.

Note: All issues except CVE-2012-4202 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 10.0.11 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.197.8. RHSA-2012:1089 — Critical: thunderbird security update

An updated thunderbird package that fixes multiple 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2012-1948, **CVE-2012-1951**, **CVE-2012-1952**, **CVE-2012-1953**, **CVE-2012-1954**, **CVE-2012-1958**, **CVE-2012-1962**, **CVE-2012-1967**

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-2012-1959

Malicious content could bypass same-compartment security wrappers (SCSW) and execute arbitrary code with chrome privileges.

CVE-2012-1955

A flaw in the way Thunderbird called history.forward and history.back could allow an attacker to conceal a malicious URL, possibly tricking a user into believing they are viewing trusted content.

CVE-2012-1957

A flaw in a parser utility class used by Thunderbird to parse feeds (such as RSS) could allow an attacker to execute arbitrary JavaScript with the privileges of the user running Thunderbird. This issue could have affected other Thunderbird components or add-ons that assume the class returns sanitized input. (CVE-2012-1957)

CVE-2012-1961

A flaw in the way Thunderbird handled X-Frame-Options headers could allow malicious content to perform a clickjacking attack.

CVE-2012-1963

A flaw in the way Content Security Policy (CSP) reports were generated by Thunderbird could allow malicious content to steal a victim's OAuth 2.0 access tokens and OpenID credentials.

CVE-2012-1964

A flaw in the way Thunderbird handled certificate warnings could allow a man-in-the-middle attacker to create a crafted warning, possibly tricking a user into accepting an arbitrary certificate as trusted.

Bug Fix

BZ#838879

The nss update RHBA-2012:0337 for Red Hat Enterprise Linux 5 and 6 introduced a mitigation for the CVE-2011-3389 flaw. For compatibility reasons, it remains disabled by default in the nss packages. This update makes Thunderbird enable the mitigation by default. It can be disabled by setting the NSS_SSL_CBC_RANDOM_IV environment variable to 0 before launching Thunderbird.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Benoit Jacob, Jesse Ruderman, Christian Holler, Bill McCloskey, Abhishek Arya, Arthur Gerkis, Bill Keese, moz_bug_r_a4, Bobby Holley, Mariusz Mlynski, Mario Heiderich, Frédéric Buclin, Karthikeyan Bhargavan, and Matt McCutchen as the original reporters of these issues.

Note: None of the issues in this advisory can 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 10.0.6 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.197.9. RHSA-2012:1211 — Critical: thunderbird security update

An updated thunderbird package that fixes multiple 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 score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) associated with each description below.

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2012-1970, CVE-2012-1972, CVE-2012-1973, CVE-2012-1974, CVE-2012-1975, CVE-2012-1976, CVE-2012-3956, CVE-2012-3957, CVE-2012-3958, CVE-2012-3959, CVE-2012-3960, CVE-2012-3961, CVE-2012-3962, CVE-2012-3963, CVE-2012-3964

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-2012-3969, CVE-2012-3970

Content containing a malicious Scalable Vector Graphics (SVG) image file could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-3967, CVE-2012-3968

Two flaws were found in the way Thunderbird rendered certain images using WebGL. Malicious content could cause Thunderbird to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-3966

A flaw was found in the way Thunderbird decoded embedded bitmap images in Icon Format (ICO) files. Content containing a malicious ICO file could cause Thunderbird to crash or, under certain conditions, possibly execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-3980

A flaw was found in the way the "eval" command was handled by the Thunderbird Error Console. Running "eval" in the Error Console while viewing malicious content could possibly cause Thunderbird to execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2012-3972

An out-of-bounds memory read flaw was found in the way Thunderbird used the format-number feature of XSLT (Extensible Stylesheet Language Transformations). Malicious content could possibly cause an information leak, or cause Thunderbird to crash. (CVE-2012-3972)

CVE-2012-3978

A flaw was found in the location object implementation in Thunderbird. Malicious content could use this flaw to possibly allow restricted content to be loaded.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Gary Kwong, Christian Holler, Jesse Ruderman, John Schoenick, Vladimir Vukicevic, Daniel Holbert, Abhishek Arya, Frédéric Hoguin, miaubiz, Arthur Gerkis, Nicolas Grégoire, moz_bug_r_a4, and Colby Russell as the original reporters of these issues.

Note: All issues except CVE-2012-3969 and CVE-2012-3970 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 10.0.7 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

4.198. xen

4.198.1. RHBA-2013:0119 — xen bug fix and enhancement update

Updated *xen* packages that fix various bugs and add two enhancements are now available for Red Hat Enterprise Linux 5.

The *xen* packages provide administration tools and the xend service for managing the kernel-xen kernel for virtualization on Red Hat Enterprise Linux.

Bug Fixes

BZ#716924

Prior to this update, trying to unplug virtual CPUs (vCPU) could result in kernel call traces in the guest. As a consequence, guests could terminate unexpectedly when rebooting. This update modifies the underlying code for the userspace tools to stop vCPUs from using the "xm" and "virsh" commands when offline.

BZ#753796

Prior to this update, the xenconsole daemon (xconsoled) was not protected against clock skew (TSkew). This update modifies the underlying code and replaces a redundant executable with the "clock_gettime" command.

BZ#766483

Prior to this update, editing or appending entries in the grub2 menu could cause the pygrub boot loader to terminate or become unresponsive when using the "a" and "e" command line arguments. This update modifies the underlying code to handle the "a" and "e" arguments as expected.

BZ#771617

Prior to this update, the xentop tool could terminate with a segmentation fault when a bridge name contained only capital letters. This update modifies the underlying code to handle network device names that contain only capital letters as expected.

BZ#772639

Prior to this update, the "xen-network-common.sh" script contained a misprint. This update modifies the script and the misprint is now removed.

BZ#796598

Prior to this update, the xenconsole daemon could terminate with a segmentation fault when timestamps were enabled and guests were too verbose. This update modifies the timestamp log to allow for verbose guests.

BZ#803181

Prior to this update, the domU domain did not correctly use the iSCSI disk and the iSCSI disk was not assigned as expected to a guest. This update modifies the underlying code to handle format guessing for names that contain colons.

BZ#861349

Prior to this update, the unregister_iomem() function could cause the removal of iomem ranges, when qemu-dm unpluging emulated NICs. This update modifies the qemu-dm code and unregister_iomem() works now as expected.

Enhancements

BZ#769613

This update adds the "-p" and "--paused" options to the "xm restore" command so that guests can be paused when debugging issues with gdbsx without pausing vCPUs.

BZ#831122

This update adds customisable Xen live migration parameters and rollback capability to the xen package.

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

4.198.2. RHSA-2012:1130 — 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 for each vulnerability from the CVE link(s) associated with each 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-2012-2625

A flaw was found in the way the pyGrub boot loader handled compressed kernel images. A privileged guest user in a para-virtualized guest (a DomU) could use this flaw to create a crafted kernel image that, when attempting to boot it, could result in an out-of-memory condition in the privileged domain (the Dom0).

Red Hat would like to thank Xinli Niu for reporting this issue.

All users of xen are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, the xend service must be restarted for this update to take effect.

4.198.3. RHSA-2012:0370 — Important: xen security and bug fix update

Updated xen packages that fix one security issue and two 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. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link(s) associated with each 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-2012-0029

A heap overflow flaw was found in the way QEMU emulated the e1000 network interface card. A privileged guest user in a virtual machine whose network interface is configured to use the e1000 emulated driver could use this flaw to crash QEMU or, possibly, escalate their privileges on the host.

Red Hat would like to thank Nicolae Mogoreanu for reporting this issue.

Bug Fixes

BZ#797191

Adding support for jumbo frames introduced incorrect network device expansion when a bridge is created. The expansion worked correctly with the default configuration, but could have caused network setup failures when a user-defined network script was used. This update changes the expansion so network setup will not fail, even when a user-defined network script is used.

BZ#797836

A bug was found in xenconsoled, the Xen hypervisor console daemon. If timestamp logging for this daemon was enabled (using both the XENCONSOLED_TIMESTAMP_HYPERVISOR_LOG and XENCONSOLED_TIMESTAMP_GUEST_LOG options in "/etc/sysconfig/xend"), xenconsoled could crash if the guest emitted a lot of information to its serial console in a short period of time. Eventually, the guest would freeze after the console buffer was filled due to the crashed xenconsoled. Timestamp logging is disabled by default.

All xen 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.

4.198.4. RHSA-2012:1236 — 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(s) associated with each 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-2012-3515

A flaw was found in the way QEMU handled VT100 terminal escape sequences when emulating certain character devices. A guest user with privileges to write to a character device that is emulated on the host using a virtual console back-end could use this flaw to crash the qemu process on the host or, possibly, escalate their privileges on the host.

This flaw did not affect the default use of the Xen hypervisor implementation in Red Hat Enterprise Linux 5. This problem only affected fully-virtualized guests that have a serial or parallel device that uses a virtual console (vc) back-end. By default, the virtual console back-end is not used for such devices; only guests explicitly configured to use them in this way were affected.

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, all fully-virtualized guests must be restarted for this update to take effect.

4.199. xinetd

4.199.1. RHBA-2013:0117 — xinetd bug fix update

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

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 allows users to bind specific services to specific IP addresses on a host machine. Each service has its own specific configuration file for xinetd; the files are located in the /etc/xinetd.d directory.

Bug Fix

BZ#801507

Previously, when the xinetd daemon connected to the TCPMUX service, the service file descriptors were not closed properly. Consequently, xinetd terminated unexpectedly with a segmentation fault. With this update, the code has been fixed to close the file descriptors, and xinetd no longer crashes when a connection to TCPMUX service is established.

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

4.200. xorg-x11-server

4.200.1. RHBA-2012:1191 — xorg-x11-server bug fix update

Updated xorg-x11-server packages that fix a 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#835626

Previously, the RRSelectInput() function failed to perform endian conversion correctly. Consequently, some gtk2 applications run on a little-endian architecture but displayed on a big-endian architecture - or vice versa - terminated unexpectedly with the "BadValue (integer parameter out of range for operation)" error message returned. A patch has been applied to address this issue and the applications now run correctly in the described scenario.

All users of xorg-x11-server are advised to upgrade to these updated packages, which fix this bug.

4.200.2. RHBA-2012:1335 — xorg-x11-server bug fix update

Updated xorg-x11-server packages that fix a 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#859324

Previously, running multiple xterm processes generating large amounts of text caused a memory leak in the X server. Consequently, all available system RAM could be consumed over time. This update fixes the composite wrapper code that was leaking certain region structures and the X server no longer leaks memory in the described scenario.

All users of xorg-x11-server are advised to upgrade to these updated packages, which fix this bug.

4.200.3. RHBA-2013:0083 — xorg-x11-server bug fix update

Updated xorg-x11-server packages that fix multiple bugs 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 Fixes

BZ#794810

Previously, the RRSelectInput() function failed to perform endian conversion correctly. Consequently, certain GTK+ 2 applications run on a little-endian architecture but displayed on a big-endian architecture - or vice versa - terminated unexpectedly with the "BadValue (integer parameter out of range for operation)" error message. This problem has been fixed in this update so that the applications now run correctly in the described scenario.

BZ#508923

An unexpected termination in software image transfers on 64-bit systems that caused the X virtual framebuffer (Xvfb) to terminate unexpectedly with a segmentation fault has been fixed.

BZ#498357

Previously, when the number of server clients changed from >0 clients to 0 clients, if started with neither the "-noreset" or "-terminate" flags, Xvfb consumed more memory than expected. With this update, this bug has been fixed.

BZ#822438

When using a direct XDMCP query to connect to a Red Hat Enterprise Linux 6 server, the X server terminated unexpectedly with the SIGBART signal. The same problem affected Xephyr and Xnest. With this update, the bug has been fixed so that the X server, Xephyr, and Xnest run properly after connecting to the server with a direct XDMCP query.

BZ#854634

Previously, there was a memory leak occurring in the X server when running four xterm instances with scrolling data on each of them. This bug has been fixed in this update so that the memory leak in the X server no longer occurs.

BZ#871754

Previously, there was a bug in the X server preventing users from switching a graphical screen to a text screen. As a result, users were unable to use a graphical screen and a text screen in the same session. With this update, the problem has been fixed and does not occur anymore.

BZ#868353

When rebooting or shutting down the system, a screen with the reboot or shutdown messages was not displayed. With this update, the bug has been fixed so that the screen with the messages is displayed correctly when rebooting or shutting down the system.

BZ#865967

When logging out of the graphical session on a system with NVIDIA or AMD graphics cards using the DisplayPort interface, a fatal X server error occurred and a backtrace was logged into the X server log file. With this update, logging out on the mentioned systems works as expected and the error no longer occurs.

BZ#871964

On certain HP ProLiant DL380e Gen8 Server configurations, switching to a different virtual console, or switching to runlevel 3 from runlevel 5, or shutting down the system from runlevel 5 did not work correctly. With this update, the problem has been fixed and the system behaves as expected when performing the mentioned operations.

All users of xorg-x11-server are advised to upgrade to these updated packages, which fix these bugs.

4.201. xulrunner

4.201.1. RHBA-2012:0497 — xulrunner bug fix update

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

XULRunner provides the XUL Runtime environment for applications using the Gecko layout engine.

Bug Fix

BZ#811205

Previously, XULRunner incorrectly handled generation of cryptographic key pairs when using a third-party software token that implemented an additional cryptographic algorithm. As a consequence, this additional algorithm could have not been used for the key generation. With this update, use of third-party software tokens that implement additional cryptography algorithms for key generation is now supported correctly.

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

4.201.2. RHSA-2012:1361 — 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 for each vulnerability from the CVE link(s) associated with each description below.

XULRunner provides the XUL Runtime environment for applications using the Gecko layout engine.

Security Fix

CVE-2012-4193

A flaw was found in the way XULRunner handled security wrappers. A web page containing malicious content could possibly cause an application linked against XULRunner (such as Mozilla Firefox) to execute arbitrary code with the privileges of the user running the application.

For technical details regarding this flaw, refer to the Mozilla security advisories.

Red Hat would like to thank the Mozilla project for reporting this issue. Upstream acknowledges moz_bug_r_a4 as the original reporter.

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.

4.202. ypserv

4.202.1. RHBA-2012:0379 — ypserv bug fix update

An updated ypserv package that fixes one bug is now available for Red Hat Enterprise Linux 5.

The ypserv package contains the Network Information Service (NIS) server, which provides network information (login names, passwords, home directories, group information) to all of the machines on a network. It can enable users to log in on any machine on the network as long as the machine has the Network Information Service (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).

Bug Fix

BZ#788445

When requesting entries from a non-existing NIS map, the ypserv daemon incorrectly returned 0 (YP_FALSE) instead of -1 (YP_NOMAP). This caused the autofs utility to fail, and thus prevented file systems from being mounted automatically. With this update, ypserv returns the correct return code and autofs works as expected in this scenario.

All users of ypserv are advised to upgrade to this updated package, which fixes this bug.

4.203. yum

4.203.1. RHBA-2012:1117 — yum bug fix update

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

Yum is a command-line utility that allows the user to check for updates and automatically download and install updated RPM packages. Yum automatically obtains and downloads dependencies, prompting the user for permission as necessary.

Bug Fix

BZ#749337

After having installed a 64-bit package and running the "yum localupdate" command with the same package for both 64-bit and 32-bit architectures, yum installed the 32-bit package if the file list contained the current package versions. With this update, yum now checks for the matching package name and architecture in this scenario; if either the name or architecture does not match, yum does not perform any action.

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

4.204. yum-metadata-parser

4.204.1. RHBA-2012:1115 — yum-metadata-parser bug fix update

Updated yum-metadata-parser packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The yum-metadata-parser packages provide a fast metadata parser for Yum implemented in C.

Bug Fix

BZ#725798

If the primary.xml file contained malformed data, the yum-metadata-parser utility terminated unexpectedly due to a NULL pointer dereference. The underlying source code has been modified, so that yum-metadata-parser exits gracefully with an error message in this scenario.

All users of yum-metadata-parser are advised to upgrade to these updated packages, which fix this bug.

4.205. yum-rhn-plugin

4.205.1. RHBA-2013:0105 — yum-rhn-plugin bug fix and enhancement update

An updated yum-rhn-plugin package that fixes one bug and adds two enhancements 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.

Bug Fix

BZ#783958

The timeout option in the /etc/yum.conf file allows the system administrator to specify how many seconds the yum package manager waits for a connection before it times out. Previously, rhnplugin ignored this value, which could occasionally cause it to time out during communication with Red Hat Network, especially in a slow network environment. This update corrects this error, and rhnplugin now respects the timeout value set for all yum repositories as expected.

Enhancements

BZ#799732

Prior to this update, it was not possible to set global settings for rhnplugin that would apply to all channels the system is subscribed to. Now channels inherit the global settings by default, but the settings can be overridden if desired.

BZ#830194

This update improves the messaging of rhnplugin to incorporate receiving content from Red Hat Subscription Manager.

All users are advised to upgrade to this updated package, which fixes this bug and adds these enhancements.

4.206. yum-updatesd

4.206.1. RHBA-2013:0067 — yum-updatesd bug fix update

An updated yum-updatesd package that fixes two bugs is now available for Red Hat Enterprise Linux 5.

The yum-updatesd package provides notification of updates which are available to be applied to the system. This notification can be done either via syslog, email or over the D-BUS communication system.

Bug Fixes

BZ#563494

Previously, after calling the doSetup routine the yum-updatesd daemon was losing the contents of the "ident" variable. Consequently, the data sent to syslog could not be identified properly in the /var/log/messages file. This update modifies the "ident" variable to preserve as expected and information in syslog messages in the /var/log/messages file is correct.

BZ#597431

Due to a misprint, email notifications about available updates contained the word "packets" instead of "packages". This update corrects the spelling.

All users of the yum-updatesd are advised to upgrade to this updated package, which fixes these bugs.

4.207. zlib

4.207.1. RHEA-2012:1084 — zlib enhancement update

Updated zlib packages that add two enhancements are now available for Red Hat Enterprise Linux 5.

The zlib packages provide a general-purpose lossless data compression library which is used by various programs.

Enhancements

BZ#690835

Prior to this update, zlib did not provide minizip packages. As a consequence, there was no library available for extracting and creating zip archives. This update adds the minizip packages to zlib to create and extract zip archives.

BZ#803810

Prior to this update, zlib did not contain the pkgconfig files. As a consequence, some applications that use pkgconfig to check dependencies could not find the zlib library. This update adds the pkgconfig files to the zlib packages. Now, applications can find the zlib library using the pkgconfig tool.

All users of zlib are advised to upgrade to these updated packages, which add these enhancements.

4.208. zsh

4.208.1. RHBA-2012:1204 — zsh bug fix update

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

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, but includes many enhancements. The zsh shell supports command line editing, built-in spelling correction, programmable command completion, shell functions with autoloading, a history mechanism, and more.

Bug Fixes

BZ#758681

Prior to this update, zsh interpreted variable assignments as other commands and tried to execute them when running zsh in ksh compatibility mode due to a parser error. This update modifies the underling code to interpret variable assignments as expected.

BZ#788050

Prior to this update, the tab completion for Apache Subversion (SVN) did not work as expected when running the "svn diff" command in zsh. This update modifies the underlying code to ensure that SVN runs as expected.

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

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

ant17-1.7.1-1jpp.0

- Group: Development/Build Tools
- Summary: Build tool for Java supporting version 1.7
- Description: Ant is a platform-independent build tool for java. It's used by apache jakarta and xml projects.

hypervkvpd-0-0.7.el5

- 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.

java-1.7.0-openjdk-1.7.0.9-2.3.3.el5.1

- Group: Development/Languages
- Summary: OpenJDK Runtime Environment
- Description: The OpenJDK runtime environment.

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.

php53-odbc64-5.3.3-2.el5

- Group: Development/Languages
- Summary: A module for PHP applications that use ODBC databases via unixODBC64
- Description: The php53-odbc64 package contains a dynamic shared object that will add database support through ODBC to PHP. ODBC is an open specification which provides a consistent API for developers to use for accessing data sources (which are often, but not always, databases). PHP is an HTML-embeddable scripting language. If you need ODBC support for PHP applications, you will need to install this package and the php package. The php53-odbc64 package uses the 64-bit ABI from unixODBC 2.2.12.

rsyslog5-5.8.12-4.el5

- Group: System Environment/Daemons

- Summary: Enhanced system logging and kernel message trapping daemon
- Description: Rsyslog is an enhanced, multi-threaded syslog daemon. It supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grain output format control. It is compatible with stock sysklogd and can be used as a drop-in replacement. Rsyslog is simple to set up, with advanced features suitable for enterprise-class, encryption-protected syslog relay chains.

scl-utils-20120927-2.el5

- Group: Applications/File
- Summary: Utilities for alternative packaging
- Description: Run-time utility for alternative packaging.

A.1.2. Dropped Packages

None

A.1.3. Updated Packages

ImageMagick-6.2.8.0-12.el5 - ImageMagick-6.2.8.0-15.el5_8

- Group: Applications/Multimedia
- Summary: An X application for displaying and manipulating images.
- Description: ImageMagick(TM) is an image display and manipulation tool for the X Window System. ImageMagick can read and write JPEG, TIFF, PNM, GIF, and Photo CD image formats. It can resize, rotate, sharpen, color reduce, or add special effects to an image, and when finished you can either save the completed work in the original format or a different one. ImageMagick also includes command line programs for creating animated or transparent .gifs, creating composite images, creating thumbnail images, and more. ImageMagick is one of your choices if you need a program to manipulate and dis play images. If you want to develop your own applications which use ImageMagick code or APIs, you need to install ImageMagick-devel as well.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

OpenIPMI-2.0.16-12.el5 - OpenIPMI-2.0.16-16.el5

- Group: System Environment/Base
- Summary: OpenIPMI (Intelligent Platform Management Interface) library and tools

- Description: The Open IPMI project aims to develop an open code base to allow access to platform information using Intelligent Platform Management Interface (IPMI). This package contains the tools of the OpenIPMI 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

aide-0.13.1-6.el5 - aide-0.13.1-8.el5

- Group: Applications/System
- Summary: Intrusion detection environment
- Description: AIDE (Advanced Intrusion Detection Environment) is a file integrity checker and intrusion detection program.
- Added Dependencies:
  - libgcrypt-devel >= 1.4.4-5.el5_8.2
- Removed Dependencies:
  - libgcrypt-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

alsa-utils-1.0.17-6.el5 - alsa-utils-1.0.17-7.el5

- Group: Applications/Multimedia
- Summary: Advanced Linux Sound Architecture (ALSA) utilities
- Description: This package contains command line utilities for the Advanced Linux Sound Architecture (ALSA).
- 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-11.1.2.250-1 - anaconda-11.1.2.259-1

- 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.
- Added Dependencies:
  - kudzu-devel >= 1.2.57.1.26-7
- Removed Dependencies:
  - kudzu-devel >= 1.2.57.1.26-3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

aspell-en-6.0-2.1 - aspell-en-6.0-3

- Group: Applications/Text
- Summary: English dictionaries for Aspell.
- Description: Provides the word list/dictionaries for the following: English, Canadian English, British English
- 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.rc2.163.el5 - autofs-5.0.1-0.rc2.177.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

bind-9.3.6-20.P1.el5 - bind-9.3.6-20.P1.el5_8.5

- 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

bind97-9.7.0-6.P2.el5_7.4 - bind97-9.7.0-17.P2.el5

- 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.
- Added Dependencies:
  - docbook-style-xsl
  - libxslt
- 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 - binutils-2.17.50.0.6-20.el5_8.3

- 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

busybox-1.2.0-13.el5 - busybox-1.2.0-14.el5

- Group: System Environment/Shells
- Summary: Statically linked binary providing simplified versions of system commands

- Description: Busybox is a single binary which includes versions of a large number of system commands, including a shell. This package can be very useful for recovering from certain types of system failures, particularly those involving broken shared libraries.
- 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-2.0.115-96.el5 - cman-2.0.115-109.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

cmirror-1.1.39-13.el5 - cmirror-1.1.39-15.el5

- Group: System Environment/Base
- Summary: cmirror - The Cluster Mirror Package
- Description: cmirror - Cluster Mirroring
- 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-0.12.2-51.el5 - conga-0.12.2-64.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

coreutils-5.97-34.el5 - coreutils-5.97-34.el5_8.1

- Group: System Environment/Base
- Summary: The GNU core utilities: a set of tools commonly used in shell scripts
- Description: These are the GNU core utilities. This package is the combination of the old GNU fileutils, sh-utils, and textutils packages.
- 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-2.6-23.el5_4.1 - cpio-2.6-25.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

crontabs-1.10-8 - crontabs-1.10-11.el5

- Group: System Environment/Base
- Summary: Root crontab files used to schedule the execution of programs.
- Description: The crontabs package contains root crontab files. Crontab is the program used to install, uninstall or list the tables used to drive the cron daemon. The cron daemon checks the crontab files to see when particular commands are scheduled to be executed. If commands are scheduled, it executes them. Crontabs handles a basic system function, so it should be installed on your 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

cscope-15.5-15.1.el5_3.1 - cscope-15.5-20.el5

- Group: Development/Tools
- Summary: C source code tree search and browse tool

- Description: cscope is a mature, ncurses based, C source code tree browsing tool. It allows users to search large source code bases for variables, functions, macros, etc, as well as perform general regex and plain text searches. Results are returned in lists, from which the user can select individual matches for use in file editing.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ctdb-1.0.112-1.el5 - ctdb-1.0.112-2.el5

- Group: System Environment/Daemons
- Summary: A Clustered Database based on Samba's Trivial Database (TDB)
- Description: CTDB is a cluster implementation of the TDB database used by Samba and other projects to store temporary data. If an application is already using TDB for temporary data it is very easy to convert that application to be cluster aware and use CTDB instead.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cvs-1.11.22-11.el5 - cvs-1.11.22-11.el5_8.1

- Group: Development/Tools
- Summary: A version control system.
- Description: CVS (Concurrent Versions System) is a version control system that can record the history of your files (usually, but not always, source code). CVS only stores the differences between versions, instead of every version of every file you have ever created. CVS also keeps a log of who, when, and why changes occurred. CVS is very helpful for managing releases and controlling the concurrent editing of source files among multiple authors. Instead of providing version control for a collection of files in a single directory, CVS provides version control for a hierarchical collection of directories consisting of revision controlled files. These directories and files can then be combined together to form a software release.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cyrus-sasl-2.1.22-5.el5_4.3 - cyrus-sasl-2.1.22-7.el5_8.1

- Group: System Environment/Libraries
- Summary: The Cyrus SASL library.
- Description: The cyrus-sasl package contains the Cyrus implementation of SASL. SASL is the Simple Authentication and Security Layer, a method for adding authentication support to connection-based 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

dapl-2.0.25-2.3.el5 - dapl-2.0.34-1.el5

- Group: System Environment/Libraries
- Summary: Library providing access to the DAT 1.2 and 2.0 APIs
- Description: libdat and libdapl provide a userspace implementation of the DAT 1.2 and 2.0 API and is built to natively support InfiniBand/iWARP network technology.
- Added Dependencies:
  - libibverbs-devel > 1.1.4
  - librdmacm-devel > 1.0.14
- Removed Dependencies:
  - libibverbs-devel >= 1.1.3
  - librdmacm-devel >= 1.0.10

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

devhelp-0.12-21.el5 - devhelp-0.12-22.el5

- Group: Development/Tools
- Summary: API document browser
- Description: An API document browser for GNOME 2.
- Added Dependencies:
  - gecko-devel-unstable >= 2.0
- Removed Dependencies:
  - gecko-devel-unstable >= 1.9.2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

device-mapper-multipath-0.4.7-48.el5 - device-mapper-multipath-0.4.7-54.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 - dhcp-3.0.5-31.el5_8.1

- 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

diffutils-2.8.1-15.2.3.el5 - diffutils-2.8.1-16.el5

- Group: Applications/Text
- Summary: A GNU collection of diff utilities.
- Description: Diffutils includes four utilities: diff, cmp, diff3 and sdiff. Diff compares two files and shows the differences, line by line. The cmp command shows the offset and line numbers where two files differ, or cmp can show the characters that differ between the two files. The diff3 command shows the differences between three files. Diff3 can be used when two people have made independent changes to a common original; diff3 can produce a merged file that contains both sets of changes and warnings about conflicts. The sdiff command can be used to merge two files interactively. Install diffutils if you need to compare text 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

doxygen-1.4.7-1.1 - doxygen-1.4.7-2

- Group: Development/Tools
- Summary: A documentation system for C/C++.
- Description: Doxygen can generate an online class browser (in HTML) and/or a reference manual (in LaTeX) from a set of documented source files. The documentation is extracted directly from the sources. Doxygen can also be configured to extract the code structure from undocumented source 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

e2fsprogs-1.39-33.el5 - e2fsprogs-1.39-35.el5

- 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

e4fsprogs-1.41.12-2.el5 - e4fsprogs-1.41.12-3.el5

- Group: System Environment/Base

- Group: System Environment/Base
- Summary: Utilities for managing the fourth extended (ext4) filesystem
- Description: The e4fsprogs package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in the fourth extended (ext4) filesystem. E4fsprogs contains e4fsck (used to repair filesystem inconsistencies after an unclean shutdown), mke4fs (used to initialize a partition to contain an empty ext4 filesystem), debugfs (used to examine the internal structure of a filesystem, to manually repair a corrupted filesystem, or to create test cases for e4fsck), tune4fs (used to modify filesystem parameters), and most of the other core ext4fs filesystem utilities. Please note that "e4fsprogs" simply contains renamed static binaries from the equivalent upstream e2fsprogs release; it is packaged this way for Red Hat Enterprise Linux 5 to ensure that the many changes included for ext4 do not destabilize the core e2fsprogs in RHEL5. You should install the e4fsprogs package if you need to manage the performance of an ext4 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

esc-1.1.0-12.el5 - esc-1.1.0-13.el5_8.2

- Group: Applications/Internet
- Summary: Enterprise Security Client Smart Card Client
- Description: Enterprise Security Client allows the user to enroll and manage their cryptographic smartcards.
- Added Dependencies:
  - xulrunner >= 10.0.0
  - xulrunner-devel >= 10.0.0
- Removed Dependencies:
  - xulrunner >= 1.9.2
  - xulrunner-devel >= 1.9.2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

etherboot-5.4.4-15.el5 - etherboot-5.4.4-16.el5

- Group: Development/Tools
- Summary: Etherboot collection of boot roms
- Description: Etherboot is a software package for creating ROM images that can download code over an Ethernet network to be executed on an x86 computer. Many network adapters have a socket where a ROM chip can be installed. Etherboot is code that can be put in such a ROM
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

expat-1.95.8-8.3.el5_5.3 - expat-1.95.8-11.el5_8

- Group: System Environment/Libraries
- Summary: A library for parsing XML.
- Description: This is expat, the C library for parsing XML, written by James Clark. Expat is a stream oriented XML parser. This means that you register handlers with the parser prior to starting the parse. These handlers are called when the parser discovers the associated structures in the document being parsed. A start tag is an example of the kind of structures for which you may register handlers.
- Added Dependencies:
  - check-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

file-4.17-21 - file-4.17-28

- Group: Applications/File

- Summary: A utility for determining file types.
- Description: The file command is used to identify a particular file according to the type of data contained by the file. File can identify many different file types, including ELF binaries, system libraries, RPM packages, and different graphics formats. You should install the file package, since the file command is such a useful utility.
- 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-3.6.26-1.el5_7 - firefox-10.0.11-1.el5_8

- 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:
  - xulrunner-devel >= 10.0.11-1
- Removed Dependencies:
  - xulrunner-devel >= 1.9.2.26-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

freeradius2-2.1.12-3.el5 - freeradius2-2.1.12-5.el5

- Group: System Environment/Daemons
- Summary: High-performance and highly configurable free RADIUS server
- Description: The FreeRADIUS Server Project is a high performance and highly configurable GPL'd free RADIUS server. The server is similar in some respects to Livingston's 2.0 server. While FreeRADIUS started as a variant of the Cistron RADIUS server, they don't share a lot in common any more. It now has many more features than Cistron or Livingston, and is much

more configurable. FreeRADIUS is an Internet authentication daemon, which implements the RADIUS protocol, as defined in RFC 2865 (and others). It allows Network Access Servers (NAS boxes) to perform authentication for dial-up users. There are also RADIUS clients available for Web servers, firewalls, Unix logins, and more. Using RADIUS allows authentication and authorization for a network to be centralized, and minimizes the amount of re-configuration which has to be done when adding or deleting new users.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

freetype-2.2.1-28.el5_7.2 - freetype-2.2.1-31.el5_8.1

- 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

ftp-0.17-37.el5 - ftp-0.17-38.el5

- Group: Applications/Internet
- Summary: The standard UNIX FTP (File Transfer Protocol) client.
- Description: The ftp package provides the standard UNIX command-line FTP (File Transfer Protocol) client. FTP is a widely used protocol for transferring files over the Internet and for archiving files. If your system is on a network, you should install ftp in order to do file transfers.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gawk-3.1.5-15.el5 - gawk-3.1.5-16.el5

- Group: Applications/Text
- Summary: The GNU version of the awk text processing utility.
- Description: The gawk packages contains the GNU version of awk, a text processing utility. Awk interprets a special-purpose programming language to do quick and easy text pattern matching and reformatting jobs. Install the gawk package if you need a text processing utility. Gawk is considered to be a standard Linux tool for processing text.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gcc-4.1.2-52.el5 - gcc-4.1.2-54.el5

- Group: Development/Languages
- Summary: Various compilers (C, C++, Objective-C, Java, ...)
- Description: The gcc package contains the GNU Compiler Collection version 4.1. You'll need this package in order to compile C code.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

gcc44-4.4.6-3.el5.1 - gcc44-4.4.7-1.el5

- Group: Development/Languages
- Summary: GNU Compiler Collection version 4.4
- Description: The gcc44 package contains the GNU Compiler Collection version 4.4.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdb-7.0.1-42.el5 - gdb-7.0.1-45.el5

- Group: Development/Debuggers
- Summary: A GNU source-level debugger for C, C++, Java and other languages
- Description: GDB, the GNU debugger, allows you to debug programs written in C, C++, Java, and other languages, by executing them in a controlled fashion and printing their data.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdbm-1.8.0-26.2.1.el5_6.1 - gdbm-1.8.0-28.el5

- Group: System Environment/Libraries
- Summary: A GNU set of database routines which use extensible hashing.
- Description: Gdbm is a GNU database indexing library, including routines which use extensible hashing. Gdbm works in a similar way to standard UNIX dbm routines. Gdbm is useful for developers who write C applications and need access to a simple and efficient database or who are building C applications which will use such a database. If you're a C developer and your

programs need access to simple database routines, you should install gdbm. You'll also need to install gdbm-devel.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gfs-kmod-0.1.34-17.el5 - gfs-kmod-0.1.34-18.el5

- Group: System Environment/Kernel
- Summary: gfs kernel modules
- Description: gfs - The Global File System is a symmetric, shared-disk, cluster file system.
- Added Dependencies:
  - kernel-devel-ia64 = 2.6.18-318.el5
  - kernel-xen-devel-ia64 = 2.6.18-318.el5
- Removed Dependencies:
  - kernel-devel-ia64 = 2.6.18-302.el5
  - kernel-xen-devel-ia64 = 2.6.18-302.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gfs-utils-0.1.20-13.el5 - gfs-utils-0.1.20-14.el5

- Group: System Environment/Kernel
- Summary: Utilities for managing the global filesystem (GFS)
- Description: The gfs-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

gfs2-utils-0.1.62-34.el5 - gfs2-utils-0.1.62-35.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

ghostscript-8.70-14.el5 - ghostscript-8.70-14.el5_8.1

- Group: Applications/Publishing
- Summary: A PostScript(TM) interpreter and renderer.
- Description: Ghostscript is a set of software that provides a PostScript(TM) interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language) and an interpreter for Portable Document Format (PDF) files. Ghostscript translates PostScript code into many common, bitmapped formats, like those understood by your printer or screen. Ghostscript is normally used to display PostScript files and to print PostScript files to non-PostScript printers. If you need to display PostScript files or print them to non-PostScript printers, you should install ghostscript. If you install ghostscript, you also need to install the ghostscript-fonts package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

gimp-2.2.13-2.0.7.el5_6.2 - gimp-2.2.13-2.0.10.el5

- Group: Applications/Multimedia
- Summary: GNU Image Manipulation Program
- Description: GIMP (GNU Image Manipulation Program) is a powerful image composition and editing program, which can be extremely useful for creating logos and other graphics for webpages. GIMP has many of the tools and filters you would expect to find in similar commercial offerings, and some interesting extras as well. GIMP provides a large image manipulation toolbox, including channel operations and layers, effects, sub-pixel imaging and anti-aliasing, and conversions, all with multi-level undo.
- 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-2.5-81 - glibc-2.5-107

- 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

gnbd-1.1.7-1.el5 - gnbd-1.1.7-3.el5

- Group: System Environment/Kernel
- Summary: GFS's Network Block Device
- Description: gnbd - GFS's Network Block Device
- 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-session-2.16.0-8.el5 - gnome-session-2.16.0-10.el5

- Group: User Interface/Desktops
- Summary: GNOME session manager
- Description: gnome-session manages a GNOME desktop session. It starts up the other core GNOME components and handles logout and saving the session.
- 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-vfs2-2.16.2-8.el5 - gnome-vfs2-2.16.2-10.el5

- 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-1.4.1-3.el5_4.8 - gnutls-1.4.1-10.el5

- 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

gpxe-0.9.7-8.el5 - gpxe-0.9.7-9.el5

- Group: System Environment/Base
- Summary: A network boot loader
- Description: gPXE is an open source network bootloader. It provides a direct replacement for proprietary PXE ROMs, with many extra features such as DNS, HTTP, iSCSI, 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

grub-0.97-13.5 - grub-0.97-13.10.el5

- Group: System Environment/Base
- Summary: GRUB - the Grand Unified Boot Loader.
- Description: GRUB (Grand Unified Boot Loader) is an experimental boot loader capable of booting into most free operating systems - Linux, FreeBSD, NetBSD, GNU Mach, and others as well as most commercial operating systems.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gtk+-1.2.10-56.el5 - gtk+-1.2.10-57.el5

- Group: System Environment/Libraries
- Summary: The GIMP ToolKit (GTK+), a library for creating GUIs for X.
- Description: The gtk+ package contains the GIMP ToolKit (GTK+), a library for creating graphical user interfaces for the X Window System. GTK+ was originally written for the GIMP (GNU Image Manipulation Program) image processing program, but is now used by several other programs as well.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gtk2-2.10.4-21.el5_7.7 - gtk2-2.10.4-29.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

hal-0.5.8.1-62.el5 - hal-0.5.8.1-64.el5

- Group: System Environment/Libraries
- Summary: Hardware Abstraction Layer
- Description: HAL is daemon for collection and maintaining information from several sources about the hardware on the system. It provides a live device list through D-BUS.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hplip3-3.9.8-11.el5_6.1 - hplip3-3.9.8-15.el5

- Group: System Environment/Daemons
- Summary: HP Linux Imaging and Printing Project
- Description: The Hewlett-Packard Linux Imaging and Printing Project provides drivers for HP printers and multi-function peripherals.
- 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-2.2.3-63.el5 - httpd-2.2.3-74.el5

- 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-0.213.26-1.el5 - hwdata-0.213.28-1.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

ibsim-0.5-2.el5 - ibsim-0.5-3.el5

- Group: System Environment/Libraries
- Summary: InfiniBand fabric simulator for management

- Description: ibsim provides simulation of infiniband fabric for using with OFA OpenSM, diagnostic and management tools.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ibutils-1.2-11.2.el5 - ibutils-1.5.7-1.el5

- Group: System Environment/Libraries
- Summary: OpenIB Mellanox InfiniBand Diagnostic Tools
- Description: ibutils provides IB network and path diagnostics.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

infiniband-diags-1.5.3-1.el5 - infiniband-diags-1.5.12-2.el5

- Group: System Environment/Libraries
- Summary: OpenFabrics Alliance InfiniBand Diagnostic Tools
- Description: This package provides IB diagnostic programs and scripts needed to diagnose an IB subnet.
- Added Dependencies:
  - opensm-devel >= 3.3.13
  - perl
- Removed Dependencies:
  - opensm-devel >= 3.3.0
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

initscripts-8.45.42-1.el5 - initscripts-8.45.42-1.el5_8.1

- 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-2.1.3-1.el5 - ipa-client-2.1.3-4.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

iproute-2.6.18-13.el5 - iproute-2.6.18-15.el5

- Group: Applications/System
- Summary: Advanced IP routing and network device configuration tools.
- Description: The iproute package contains networking utilities (ip and rtmon, for example) which are designed to use the advanced networking capabilities of the Linux 2.4.x and 2.6.x kernel.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iprutils-2.3.7-2.el5 - iprutils-2.3.11-2.el5

- Group: System Environment/Base
- Summary: Utilities for the IBM Power Linux RAID adapters
- Description: Provides a suite of utilities to manage and configure SCSI devices supported by the ipr SCSI storage device 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

ipsec-tools-0.6.5-14.el5_5.5 - ipsec-tools-0.6.5-14.el5_8.5

- Group: System Environment/Base
- Summary: Tools for configuring and using IPSEC
- Description: This is the IPsec-Tools package. You need this package in order to really use the IPsec functionality in the linux-2.5+ kernels. This package builds: - setkey, a program to directly manipulate policies and SAs - racoon, an IKEv1 keying daemon
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iptables-1.3.5-9.1.el5 - iptables-1.3.5-9.2.el5_8

- Group: System Environment/Base
- Summary: Tools for managing Linux kernel packet filtering capabilities.
- Description: The iptables utility controls the network packet filtering code in the Linux kernel. If you need to set up firewalls and/or IP masquerading, you should install this package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iscsi-initiator-utils-6.2.0.872-13.el5 - iscsi-initiator-utils-6.2.0.872-16.el5

- Group: System Environment/Daemons
- Summary: iSCSI daemon and utility programs
- Description: 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.
- Added Dependencies:
  - libtool
- 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-1.6.0.0-1.24.1.10.4.el5 - java-1.6.0-openjdk-1.6.0.0-1.30.1.11.5.el5

- 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

jpackage-utils-1.7.3-1jpp.2.el5 - jpackage-utils-1.7.3-1jpp.3.el5

- Group: Utilities
- Summary: JPackage utilities
- Description: Utilities for the JPackage Project <http://www.jpackage.org/>: * /usr/bin/build-classpath build the Java classpath in a portable manner * /usr/bin/build-jar-repository build a jar repository in a portable manner * /usr/bin/rebuild-jar-repository rebuild a jar repository in a portable manner (after a jvm change...) * /usr/bin/build-classpath-directory build the Java classpath from a directory * /usr/bin/diff-jars show jar content differences * /usr/bin/jvmjar install jvm extensions * /usr/bin/create-jar-links create custom jar links * /usr/bin/clean-binary-files remove binary files from sources * /usr/bin/check-binary-files check for presence of unexpected binary files * /usr/share/java-utils/java-functions shell script functions library for Java applications * /etc/java/jpackage-release string identifying the currently installed JPackage release * /etc/java/java.conf system-wide Java configuration file * /etc/rpm/macros.jpackage RPM macros for Java packagers and developers * /usr/share/doc/jpackage-utils-1.7.3/jpackage-policy Java packaging policy for packagers and developers It contains also the License, man pages, documentation, XSL files of general use with maven2, a header file for spec files 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

kbd-1.12-21.el5 - kbd-1.12-22.el5

- Group: System Environment/Base
- Summary: Tools for configuring the console (keyboard, virtual terminals, etc.)
- Description: The kbd package contains tools for managing a Linux system's console's behavior, including the keyboard, the screen fonts, the virtual terminals and font 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

kdebase-3.5.4-25.el5 - kdebase-3.5.4-26.el5

- Group: User Interface/Desktops
- Summary: K Desktop Environment - core files
- Description: Core applications for the K Desktop Environment. Included are: kdm (replacement for xdm), kwin (window manager), konqueror (filemanager, web browser, ftp client, ...), konsole (xterm replacement), kpanel (application starter and desktop pager), kaudio (audio server), kdehelp (viewer for kde help files, info and man pages), kthememgr (system for managing alternate theme packages) plus other KDE components (kcheckpass, kikbd, kscreensaver, kcontrol, kfind, kfontmanager, kmenuedit).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kernel-2.6.18-308.el5 - kernel-2.6.18-348.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-154.el5 - kexec-tools-1.102pre-161.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

ksh-20100621-5.el5 - ksh-20100621-12.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

kudzu-1.2.57.1.26-3 - kudzu-1.2.57.1.26-7

- Group: Applications/System
- Summary: The Red Hat Linux hardware probing tool.
- Description: Kudzu is a hardware probing tool run at system boot time to determine what hardware has been added or removed from the 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

kvm-83-249.el5 - kvm-83-262.el5

- 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 = 2.6.18-339.el5
  - kernel-devel = 2.6.18-339.el5
- Removed Dependencies:
  - kernel-debug-devel = 2.6.18-304.el5
  - kernel-devel = 2.6.18-304.el5
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

lftp-3.7.11-7.el5 - lftp-3.7.11-8.el5

- Group: Applications/Internet
- Summary: A sophisticated file transfer program
- Description: LFTP is a sophisticated ftp/http file transfer program. 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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libcxgb3-1.3.0-1.el5 - libcxgb3-1.3.1-2.el5

- Group: System Environment/Libraries
- Summary: Chelsio T3 iWARP HCA Userspace Driver
- Description: Userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables Chelsio iWARP capable ethernet devices.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libcxgb4-1.1.1-2.el5 - libcxgb4-1.2.0-2.el5

- Group: System Environment/Libraries
- Summary: Chelsio T3 iWARP HCA Userspace Driver

- Description: Userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables Chelsio iWARP capable ethernet devices.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libehca-1.2.1-6.el5 - libehca-1.2.2-1.el5

- Group: System Environment/Libraries
- Summary: IBM InfiniBand HCA Userspace Driver
- Description: IBM hardware driver for use with libibverbs user space verbs access library.
- Added Dependencies:
  - libibverbs-devel > 1.1.4
- Removed Dependencies:
  - libibverbs-devel >= 1.1.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libexif-0.6.20-1.el5_7.1 - libexif-0.6.21-1.el5_8

- Group: System Environment/Libraries
- Summary: Library for extracting extra information from image files
- Description: Most digital cameras produce EXIF files, which are JPEG files with extra tags that contain information about the image. The EXIF library allows you to parse an EXIF file and read the data from those tags.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libgcrypt-1.4.4-5.el5 - libgcrypt-1.4.4-5.el5_8.2

- Group: System Environment/Libraries
- Summary: A general-purpose cryptography library
- Description: Libgcrypt is a general purpose crypto library based on the code used in GNU Privacy Guard. This is a development version.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibcm-1.0.5-1.el5 - libibcm-1.0.5-2.el5

- Group: System Environment/Libraries
- Summary: Userspace InfiniBand Connection Manager
- Description: libibcm provides a userspace library that handles the majority of the low level work required to open an RDMA connection between two machines.
- Added Dependencies:
  - libibverbs-devel >= 1.1
- Removed Dependencies:
  - libibverbs-devel >= 1.1.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibmad-1.3.3-1.el5 - libibmad-1.3.8-1.el5

- Group: System Environment/Libraries
- Summary: OpenFabrics Alliance InfiniBand MAD library
- Description: libibmad provides low layer IB functions for use by the IB diagnostic and management programs. These include MAD, SA, SMP, and other basic IB functions.
- Added Dependencies:
  - libibumad-devel = 1.3.7
- Removed Dependencies:
  - libibumad-devel = 1.3.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibumad-1.3.3-1.el5 - libibumad-1.3.7-1.el5

- Group: System Environment/Libraries
- Summary: OpenFabrics Alliance InfiniBand umad (user MAD) library
- Description: libibumad provides the user MAD library functions which sit on top of the user MAD modules in the kernel. These are used by the IB diagnostic and management tools, including OpenSM.
- Added Dependencies:
  - autoconf
  - automake
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibverbs-1.1.3-2.el5 - libibverbs-1.1.6-3.el5

- Group: System Environment/Libraries

- Summary: A library for direct userspace use of RDMA (InfiniBand/iWARP) hardware
- Description: libibverbs is a library that allows userspace processes to use RDMA "verbs" as described in the InfiniBand Architecture Specification and the RDMA Protocol Verbs Specification. This includes direct hardware access from userspace to InfiniBand/iWARP adapters (kernel bypass) for fast path operations. For this library to be useful, a device-specific plug-in module should also be 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

libipathverbs-1.2-2.el5 - libipathverbs-1.2-3.el5

- Group: System Environment/Libraries
- Summary: QLogic InfiniPath HCA Userspace Driver
- Description: QLogic hardware driver for use with libibverbs user space verbs access library. This driver supports QLogic InfiniPath based cards.
- Added Dependencies:
  - valgrind-devel
- Removed Dependencies:
  - valgrind
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libmlx4-1.0.1-7.el5 - libmlx4-1.0.2-1.el5

- Group: System Environment/Libraries
- Summary: Mellanox ConnectX InfiniBand HCA Userspace Driver
- Description: libmlx4 provides a device-specific userspace driver for Mellanox ConnectX HCAs for use with the libibverbs library.

- Added Dependencies:
  - libibverbs-devel > 1.1.4
- Removed Dependencies:
  - libibverbs-devel >= 1.1.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libmthca-1.0.5-6.el5 - libmthca-1.0.6-1.el5

- Group: System Environment/Libraries
- Summary: Mellanox InfiniBand HCA Userspace Driver
- Description: libmthca provides a device-specific userspace driver for Mellanox HCAs (MT23108 InfiniHost and MT25208 InfiniHost III Ex) for use with the libibverbs library.
- Added Dependencies:
  - libibverbs-devel > 1.1.4
- Removed Dependencies:
  - libibverbs-devel >= 1.1.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libnes-0.9.0-2.el5 - libnes-1.1.3-1.el5

- Group: System Environment/Libraries
- Summary: NetEffect RNIC Userspace Driver
- Description: Userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables NetEffect iWARP capable ethernet devices.
- Added Dependencies:
  - libibverbs-devel > 1.1.4
- Removed Dependencies:

- libibverbs-devel >= 1.1.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libpng-1.2.10-7.1.el5_7.5 - libpng-1.2.10-17.el5_8

- Group: System Environment/Libraries
- Summary: A library of functions for manipulating PNG image format files
- Description: The libpng package contains a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files. PNG is a bit-mapped graphics format similar to the GIF format. PNG was created to replace the GIF format, since GIF uses a patented data compression algorithm. Libpng should be installed if you need to manipulate PNG 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

librdmacm-1.0.10-1.el5 - librdmacm-1.0.15-2.el5

- Group: System Environment/Libraries
- Summary: Userspace RDMA Connection Manager
- Description: librdmacm provides a userspace RDMA Communication Managment API.
- Added Dependencies:
  - libibverbs-devel >= 1.1
- Removed Dependencies:
  - libibverbs-devel >= 1.1.3
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

libsdp-1.1.99-11.el5 - libsdp-1.1.108-1.el5

- Group: System Environment/Libraries
- Summary: A library for direct userspace use of Sockets Direct Protocol
- Description: libsdp is an LD_PRELOAD-able library that can be used to have existing applications use InfiniBand Sockets Direct Protocol (SDP) instead of TCP sockets, transparently and without recompilation. For information on how to configure libsdp, see libsdp.conf, which is installed in $(sysconfdir) (usually /usr/local/etc or /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

libtalloc-2.0.1-11.el5 - libtalloc-2.0.7-2.el5

- Group: System Environment/Daemons
- Summary: A hierarchical memory allocator
- Description: A library that implements a hierarchical allocator with destructors.
- Added Dependencies:
  - doxygen
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libtdb-1.2.1-6.el5 - libtdb-1.2.10-1.el5

- Group: System Environment/Daemons

- Summary: The tdb library
- Description: A library that implements a trivial database.
- Added Dependencies:
  - python-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libtiff-3.8.2-7.el5_6.7 - libtiff-3.8.2-15.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

libuser-0.54.7-2.1.el5_5.2 - libuser-0.54.7-3.el5

- Group: System Environment/Base
- Summary: A user and group account administration library.
- Description: The libuser library implements a standardized interface for manipulating and administering user and group accounts. The library uses pluggable back-ends to interface to its data sources. Sample applications modeled after those included with the shadow password suite are included.
- 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-0.8.2-25.el5 - libvirt-0.8.2-29.el5

- 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

libvorbis-1.1.2-3.el5_4.4 - libvorbis-1.1.2-3.el5_7.6

- Group: System Environment/Libraries
- Summary: The Vorbis General Audio Compression Codec.
- Description: Ogg Vorbis is a fully open, non-proprietary, patent-and royalty-free, general-purpose compressed audio format for audio and music at fixed and variable bitrates from 16 to 128 kbps/channel. The libvorbis package contains runtime libraries for use in programs that support Ogg Voribs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

libxml2-2.6.26-2.1.12.el5_7.2 - libxml2-2.6.26-2.1.15.el5_8.5

- 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

libxslt-1.1.17-2.el5_2.2 - libxslt-1.1.17-4.el5_8.3

- Group: Development/Libraries
- Summary: Library providing the Gnome XSLT engine
- Description: This C library allows to transform XML files into other XML files (or HTML, text, ...) using the standard XSLT stylesheet transformation mechanism. To use it you need to have a version of libxml2 >= 2.6.25 installed. The xsltproc command is a command line interface to the XSLT engine
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

linuxwacom-0.7.8.3-11.el5 - linuxwacom-0.7.8.3-11.2.el5_8

- Group: User Interface/X Hardware Support

- Group: User Interface/X Hardware Support
- Summary: Wacom Drivers from Linux Wacom Project
- Description: The Linux Wacom Project manages the drivers, libraries, and documentation for configuring and running Wacom tablets under the Linux operating system. It contains diagnostic applications as well as X.org XInput drivers.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

logrotate-3.7.4-12 - logrotate-3.7.4-14

- Group: System Environment/Base
- Summary: Rotates, compresses, removes and mails system log files.
- Description: The logrotate utility is designed to simplify the administration of log files on a system which generates a lot of log files. Logrotate allows for the automatic rotation compression, removal and mailing of log files. Logrotate can be set to handle a log file daily, weekly, monthly or when the log file gets to a certain size. Normally, logrotate runs as a daily cron job. Install the logrotate package if you need a utility to deal with the log files on your 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

logwatch-7.3-9.el5_6 - logwatch-7.3-10.el5

- Group: Applications/System
- Summary: A log file analysis program
- Description: Logwatch is a customizable, pluggable log-monitoring system. It will go through your logs for a given period of time and make a report in the areas that you wish with the detail that you wish. Easy to use - works right out of the package on many systems.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lvm2-2.02.88-7.el5 - lvm2-2.02.88-10.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

lvm2-cluster-2.02.88-7.el5 - lvm2-cluster-2.02.88-9.el5

- Group: System Environment/Base
- Summary: Cluster extensions for userland logical volume management tools
- Description: Extensions to LVM2 to support clusters.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

m2crypto-0.16-8.el5 - m2crypto-0.16-9.el5

- Group: System Environment/Libraries
- Summary: Support for using OpenSSL in python scripts
- Description: This package allows you to call OpenSSL functions from python 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

man-1.6d-2.el5 - man-1.6d-3.el5

- Group: System Environment/Base
- Summary: A set of documentation tools: man, apropos and whatis.
- Description: The man package includes three tools for finding information and/or documentation about your Linux system: man, apropos, and whatis. The man system formats and displays on-line manual pages about commands or functions on your system. Apropos searches the whatis database (containing short descriptions of system commands) for a string. Whatis searches its own database for a complete word. The man package should be installed on your system because it is the primary way to find documentation on a Linux 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

man-pages-overrides-5.8.3-2.el5 - man-pages-overrides-5.9.2-2.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

mdadm-2.6.9-3.el5 - mdadm-2.6.9-5.el5

- Group: System Environment/Base
- Summary: mdadm controls Linux md devices (software RAID arrays)
- Description: mdadm is used to create, manage, and monitor Linux MD (software RAID) devices. As such, it provides similar functionality to the raidtools package. However, mdadm is a single program, and it can perform almost all functions without a configuration file, though a configuration file can be used to help with some common tasks.
- 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-1.17-1.56.el5 - microcode_ctl-1.17-3.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-5.1.19.6-75.el5 - mkinitrd-5.1.19.6-79.el5

- 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

mod_auth_kerb-5.1-3.el5_7.1 - mod_auth_kerb-5.1-5.el5

- Group: System Environment/Daemons
- Summary: Kerberos authentication module for HTTP
- Description: mod_auth_kerb is module for the Apache HTTP Server designed to provide Kerberos authentication over HTTP. The module supports the Negotiate authentication method, which performs full Kerberos authentication based on ticket exchanges.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

mod_nss-1.0.8-4.el5_6.1 - mod_nss-1.0.8-7.el5

- Group: System Environment/Daemons
- Summary: SSL/TLS module for the Apache HTTP server
- Description: The mod_nss module provides strong cryptography for the Apache Web server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols using the Network Security Services (NSS) security 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

mod_python-3.2.8-3.1 - mod_python-3.2.8-4.el5

- Group: System Environment/Daemons
- Summary: An embedded Python interpreter for the Apache Web server.
- Description: Mod_python is a module that embeds the Python language interpreter within the server, allowing Apache handlers to be written in Python. Mod_python brings together the versatility of Python and the power of the Apache Web server for a considerable boost in flexibility and performance over the traditional CGI approach.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mozldap-6.0.5-1.el5 - mozldap-6.0.5-2.el5

- Group: System Environment/Libraries
- Summary: Mozilla LDAP C SDK

- Description: The Mozilla LDAP C SDK is a set of libraries that allow applications to communicate with LDAP directory servers. These libraries are derived from the University of Michigan and Netscape LDAP libraries. They use Mozilla NSPR and NSS for crypto.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mpitests-3.2-1.el5 - mpitests-3.2-2.el5

- Group: Applications
- Summary: MPI Benchmarks and tests
- Description: Set of popular MPI benchmarks: IMB-2.3 Presta-1.4.0 OSU benchmarks ver 2.2
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mstflint-1.4-1.el5 - mstflint-1.4-2.el5

- Group: Applications/System
- Summary: Mellanox firmware burning tool
- Description: This package contains a burning tool for Mellanox manufactured HCA cards. It also provides access to the relevant source code.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

mt-st-0.9b-2.2.2 - mt-st-0.9b-4.el5

- Group: Applications/System
- Summary: Install mt-st if you need a tool to control tape drives.
- Description: The mt-st package contains the mt and st tape drive management programs. Mt (for magnetic tape drives) and st (for SCSI tape devices) can control rewinding, ejecting, skipping files and blocks and more. Install mt-st if you need a tool to manage tape drives.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mutt-1.4.2.2-3.0.2.el5 - mutt-1.4.2.2-6.el5

- Group: Applications/Internet
- Summary: A text mode mail user agent.
- Description: Mutt is a text-mode mail user agent. Mutt supports color, threading, arbitrary key remapping, and a lot of customization. You should install mutt if you have used it in the past and you prefer it, or if you are new to mail programs and have not decided which one you are going to use.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mvapich-1.2.0-0.3562.1.el5 - mvapich-1.2.0-0.3562.2.el5

- Group: Development/Libraries

- Summary: MPI implementation over Infiniband RDMA-enabled interconnect
- Description: This is high performance and scalable MPI-1 implementation over Infiniband and RDMA-enabled interconnects. This implementation is based on MPICH and MVICH. MVAPICH is pronounced as `em-vah-pich''.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mvapich2-1.4-1.el5 - mvapich2-1.4-2.el5

- Group: Development/Libraries
- Summary: OSU MVAPICH2 MPI package
- Description: This is an MPI-2 implementation which includes all MPI-1 features. It is based on MPICH2 and MVICH.
- 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-5.0.77-4.el5_6.6 - mysql-5.0.95-3.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 MySQL client programs, the client shared libraries, and generic MySQL files.
- No added dependencies
- Removed Dependencies:

    - gperf
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

net-snmp-5.3.2.2-17.el5 - net-snmp-5.3.2.2-20.el5

- Group: System Environment/Daemons
- Summary: A collection of SNMP protocol tools and libraries.
- Description: SNMP (Simple Network Management Protocol) is a protocol used for network management. The NET-SNMP project includes various SNMP tools: an extensible agent, an SNMP library, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl mib browser. This package contains the snmpd and snmptrapd daemons, documentation, etc. You will probably also want to install the net-snmp-utils package, which contains NET-SNMP utilities. Building option: --without tcp_wrappers : disable tcp_wrappers support
- 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-1.0.9-60.el5 - nfs-utils-1.0.9-66.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-4.8.8-2.el5 - nspr-4.9.1-6.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-3.12.10-8.el5 - nss-3.13.5-8.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:
  - nspr-devel >= 4.9.1
- Removed Dependencies:
  - nspr-devel >= 4.8.8
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nss_ldap-253-49.el5 - nss_ldap-253-51.el5

- 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

openais-0.80.6-36.el5 - openais-0.80.6-37.el5

- Group: System Environment/Base
- Summary: The openais Standards-Based Cluster Framework executive and APIs
- Description: This package contains the openais executive, openais service handlers, default configuration files and init script.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openib-1.4.1-6.el5 - openib-1.5.4.1-4.el5

- Group: System Environment/Base
- Summary: OpenIB Infiniband Driver Stack
- Description: User space initialization scripts for the kernel InfiniBand drivers
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openldap-2.3.43-25.el5 - openldap-2.3.43-25.el5_8.1

- Group: System Environment/Daemons
- Summary: The configuration files, libraries, and documentation for OpenLDAP.
- Description: OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. LDAP is a set of protocols for accessing directory services (usually phone book style information, but other information is possible) over the Internet, similar to the way DNS (Domain Name System) information is propagated over the Internet. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.
- 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.el5 - openmotif-2.3.1-6.1.el5_8

- 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

openmpi-1.4-4.el5 - openmpi-1.4-7.el5

- Group: Development/Libraries
- Summary: Open Message Passing Interface
- Description: Open MPI is an open source, freely available implementation of both the MPI-1 and MPI-2 standards, combining technologies and resources from several other projects (FT-MPI, LA-MPI, LAM/MPI, and PACX-MPI) in order to build the best MPI library available. A completely new MPI-2 compliant implementation, Open MPI offers advantages for system and software vendors, application developers, and computer science researchers. For more information, see http://www.open-mpi.org/ .
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

opensm-3.3.3-2.el5 - opensm-3.3.13-1.el5

- Group: System Environment/Daemons
- Summary: OpenIB InfiniBand Subnet Manager and management utilities
- Description: OpenSM is the OpenIB project's Subnet Manager for Infiniband networks. The subnet manager is run as a system daemon on one of the machines in the infiniband fabric to manage the fabric's routing state. This package also contains various tools for diagnosing and testing Infiniband networks that can be used from any machine and do not need to be run on a machine running the opensm daemon.
- Added Dependencies:
  - libibmad-devel = 1.3.8
- Removed Dependencies:

    - libibmad-devel = 1.3.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openssl-0.9.8e-22.el5 - openssl-0.9.8e-22.el5_8.4

- 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

openssl097a-0.9.7a-9.el5_4.2 - openssl097a-0.9.7a-11.el5_8.2

- 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-2.6.32-3.el5 - openswan-2.6.32-4.el5

- 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

pam-0.99.6.2-6.el5_5.2 - pam-0.99.6.2-12.el5

- Group: System Environment/Base
- Summary: A security tool which provides authentication for applications
- Description: PAM (Pluggable Authentication Modules) is a system security tool that allows system administrators to set authentication policy without having to recompile programs that handle authentication.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

parted-1.8.1-29.el5 - parted-1.8.1-30.el5

- Group: Applications/System

- Group: Applications/System
- Summary: The GNU disk partition manipulation program
- Description: The GNU Parted program allows you to create, destroy, resize, move, and copy hard disk partitions. Parted can be used for creating space for new operating systems, reorganizing disk usage, and copying data to new hard disks.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pdksh-5.2.14-37.el5 - pdksh-5.2.14-37.el5_8.1

- Group: System Environment/Shells
- Summary: A public domain shell implementing ksh-88
- Description: The pdksh package contains public domain implementation of ksh-88. The ksh shell is a command interpreter intended for both interactive and shell script use. Ksh's command language is a superset of the sh shell language. Pdksh is unmaintained since 1998 and is obsoleted by ksh package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perftest-1.2.3-1.el5 - perftest-1.3.0-1.el5

- Group: Productivity/Networking/Diagnostic
- Summary: IB Performance Tests
- Description: Perftest is a collection of simple test programs designed to utilize RDMA communications and provide performance numbers over those RDMA connections. It does not work on normal TCP/IP networks, only on RDMA networks.
- Added Dependencies:

    - libibumad-devel > 1.3.6
    - libibverbs-devel > 1.1.4
    - librdmacm-devel > 1.0.14
  - Removed Dependencies:
    - libibverbs-devel >= 1.1.3
    - librdmacm-devel >= 1.0.10
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

perl-5.8.8-38.el5 - perl-5.8.8-38.el5_8

  - 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-DBD-Pg-1.49-2.el5_3.1 - perl-DBD-Pg-1.49-4.el5_8

  - Group: Development/Libraries
  - Summary: A PostgreSQL interface for perl
  - Description: An implementation of DBI for PostgreSQL for 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

perl-LDAP-0.33-3.fc6 - perl-LDAP-0.33-4.el5_8

- Group: Development/Libraries
- Summary: LDAP Perl module
- Description: Net::LDAP is a collection of modules that implements a LDAP services API for Perl programs. The module may be used to search directories or perform maintenance functions such as adding, deleting or modifying entries.
- 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-XML-SAX-0.14-11 - perl-XML-SAX-0.14-13.el5

- Group: Development/Libraries
- Summary: XML-SAX Perl module
- Description: XML-SAX Perl module.
- 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-5.1.6-32.el5 - php-5.1.6-39.el5_8

- 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

php53-5.3.3-5.el5 - php53-5.3.3-13.el5_8

- 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-0.8.4-24.el5 - piranha-0.8.4-25.el5

- 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

pirut-1.3.28-19.el5 - pirut-1.3.28-20.el5

- Group: Applications/System
- Summary: Package Installation, Removal and Update Tools
- Description: pirut (pronounced "pirate") provides a set of graphical tools for managing 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

pm-utils-0.99.3-10.el5 - pm-utils-0.99.3-14.el5

- Group: System Environment/Base
- Summary: Power management utilities and scripts
- Description: The pm-utils package contains utilities and scripts useful for tasks related to power management.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

postfix-2.3.3-2.3.el5_6 - postfix-2.3.3-6.el5

- Group: System Environment/Daemons
- Summary: Postfix Mail Transport Agent
- Description: Postfix is a Mail Transport Agent (MTA), supporting LDAP, SMTP AUTH (SASL), TLS
- Added Dependencies:
  - mysql
  - mysql-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

postgresql-8.1.23-1.el5_7.3 - postgresql-8.1.23-6.el5_8

- Group: Applications/Databases
- Summary: PostgreSQL client programs and libraries.
- Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for the whole package, as well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

postgresql84-8.4.9-1.el5_7.1 - postgresql84-8.4.13-1.el5_8

- Group: Applications/Databases
- Summary: PostgreSQL client programs
- Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for the whole package, as well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a local or remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ppc64-utils-0.13-13.el5 - ppc64-utils-0.13-13.el5_8.2

- Group: System Environment/Base
- Summary: Linux/PPC64 specific utilities
- Description: A collection of utilities for Linux on PPC64 platforms.
- 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-3.2.7-18.el5 - procps-3.2.7-22.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

psmisc-22.2-7.el5_6.2 - psmisc-22.2-11

- Group: Applications/System
- Summary: Utilities for managing processes on your system.
- Description: The psmisc package contains utilities for managing processes on your system: pstree, killall and fuser. The pstree command displays a tree structure of all of the running processes on your system. The killall command sends a specified signal (SIGTERM if nothing is specified) to processes identified by name. The fuser command identifies the PIDs of processes that are using specified files or 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

python-2.4.3-46.el5 - python-2.4.3-56.el5

- Group: Development/Languages
- Summary: An interpreted, interactive, object-oriented programming language.
- Description: Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC). Programmers can write new built-in modules for Python in C or C++. Python can be used as an extension language for applications that need a programmable interface. This package contains most of the standard Python modules, as well as modules for interfacing to the Tix widget set for Tk and RPM. Note that documentation for Python is provided in the python-docs package.
- Added Dependencies:
  - expat-devel >= 1.95.8-11
- Removed Dependencies:
  - expat-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

python-iniparse-0.2.3-4.el5 - python-iniparse-0.2.3-6.el5

- Group: Development/Libraries
- Summary: Python Module for Accessing and Modifying Configuration Data in INI files
- Description: iniparse is an INI parser for Python which is API compatible with the standard library's ConfigParser, preserves structure of INI files (order of sections & options, indentation, comments, and blank lines are preserved when data is updated), and is more convenient to use.
- 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-0.98.9-1.el5 - python-rhsm-1.0.10-1.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.
- Added Dependencies:
  - openssl-devel
- Removed Dependencies:
  - rpm-python
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

qlvnictools-0.0.1-12.el5 - qlvnictools-0.0.1-13.el5

- Group: System Environment/Base
- Summary: VNIC ULP service
- Description: VNIC ULP service
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

qperf-0.4.6-1.el5 - qperf-0.4.6-3.el5

- Group: Networking/Diagnostic
- Summary: Measure socket and RDMA performance
- Description: Measure socket and RDMA performance.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

qt-3.3.6-25.el5 - qt-3.3.6-26.el5

- Group: System Environment/Libraries
- Summary: The shared library for the Qt GUI toolkit.
- Description: Qt is a GUI software toolkit which simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System. Qt is written in C++ and is fully object-oriented. This package contains the shared library needed to run qt applications, as well as the README files for qt.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

quagga-0.98.6-5.el5_5.2 - quagga-0.98.6-11.el5

- Group: System Environment/Daemons
- Summary: Routing daemon
- Description: Quagga is a free software that manages TCP/IP based routing protocol. It takes multi-server and multi-thread approach to resolve the current complexity of the Internet. Quagga supports BGP4, BGP4+, OSPFv2, OSPFv3, RIPv1, RIPv2, and RIPng. Quagga is intended to be used as a Route Server and a Route Reflector. It is not a toolkit, it provides full routing

power under a new architecture. Quagga by design has a process for each protocol. Quagga is a fork of GNU Zebra.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

quota-3.13-5.el5 - quota-3.13-8.el5

- Group: System Environment/Base
- Summary: System administration tools for monitoring users' disk usage.
- Description: The quota package contains system administration tools for monitoring and limiting user and or group disk usage per filesystem.
- Added Dependencies:
  - autoconf
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rds-tools-1.5-1.el5 - rds-tools-2.0.6-1.el5

- Group: Applications/System
- Summary: RDS support tools
- Description: Various tools for support of the RDS (Reliable Datagram Socket) API. RDS is specific to InfiniBand and iWARP networks and does not work on non-RDMA hardware.
- 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-5.8.0.3 - redhat-release-5Server-5.9.0.2

- 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-43 - redhat-release-notes-5Server-46

- 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-2.0.52-28.el5 - rgmanager-2.0.52-37.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-0.4.20-77.el5 - rhn-client-tools-0.4.20-86.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

rhnsd-4.7.0-10.el5 - rhnsd-4.7.0-14.el5

- Group: System Environment/Base
- Summary: Red Hat Network query daemon
- Description: The Red Hat Update Agent that automatically queries the Red Hat Network servers and determines which packages need to be updated on your machine, and runs any actions.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

rp-pppoe-3.5-32.1 - rp-pppoe-3.5-33.el5

- Group: System Environment/Daemons
- Summary: A PPP over Ethernet client (for xDSL support).
- Description: PPPoE (Point-to-Point Protocol over Ethernet) is a protocol used by many ADSL Internet Service Providers. This package contains the Roaring Penguin PPPoE client, a user-mode program that does not require any kernel modifications. It is fully compliant with RFC 2516, the official PPPoE specification.
- 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-4.4.2.3-27.el5 - rpm-4.4.2.3-31.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-1.8.5-24.el5 - ruby-1.8.5-27.el5

- Group: Development/Languages

- 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

samba-3.0.33-3.37.el5 - samba-3.0.33-3.39.el5_8

- Group: System Environment/Daemons
- Summary: The Samba SMB server.
- 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 server that can be used to provide network services to SMB (sometimes called "Lan Manager") clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.
- 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-3.5.10-0.107.el5 - samba3x-3.6.6-0.129.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:
  - automake
  - libtdb-devel >= 1.2.6
- Removed Dependencies:
  - libtdb-devel >= 1.2.1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

scim-bridge-0.4.5-10.el5 - scim-bridge-0.4.5-11.el5

- Group: System Environment/Libraries
- Summary: SCIM Bridge Gtk IM module
- Description: SCIM Bridge is a C implementation of a Gtk IM module for SCIM.
- 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-2.4.6-327.el5 - selinux-policy-2.4.6-338.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

setroubleshoot-2.0.5-5.el5 - setroubleshoot-2.0.5-5.el5_8.1

- Group: Applications/System
- Summary: Helps troubleshoot SELinux problems
- Description: setroubleshoot gui. Application that allows you to view setroubleshoot-server messages. Provides tools to help diagnose SELinux problems. When AVC messages are generated an alert can be generated that will give information about the problem and help track its resolution. Alerts can be configured to user preference. The same tools can be run on existing log 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

shadow-utils-4.0.17-20.el5 - shadow-utils-4.0.17-21.el5

- Group: System Environment/Base
- Summary: Utilities for managing accounts and shadow password files.
- Description: The shadow-utils package includes the necessary programs for converting UNIX password files to the shadow password format, plus programs for managing user and group accounts. The pwconv command converts passwords to the shadow password format. The pwunconv command unconverts shadow passwords and generates an npasswd file (a standard UNIX password file). The pwck command checks the integrity of password and shadow files. The lastlog command prints out the last login times for all users. The useradd, userdel, and usermod commands are used for managing user accounts. The groupadd, groupdel, and groupmod commands are used for managing group accounts.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides

- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

smartmontools-5.38-3.el5 - smartmontools-5.42-2.el5

- Group: System Environment/Base
- Summary: Tools for monitoring SMART capable hard disks
- Description: The smartmontools package contains two utility programs (smartctl and smartd) to control and monitor storage systems using the Self- Monitoring, Analysis and Reporting Technology System (SMART) built into most modern ATA and SCSI hard disks. In many cases, these utilities will provide advanced warning of disk degradation and failure.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

specspo-13-1.el5 - specspo-13-4.el5

- Group: Documentation
- Summary: Package descriptions, summaries, and groups.
- Description: The specspo package contains the portable object catalogues used to internationalize packages.
- 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-3.3.6-5 - sqlite-3.3.6-6

- 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

squirrelmail-1.4.8-5.el5_4.10 - squirrelmail-1.4.8-21.el5

- Group: Applications/Internet
- Summary: SquirrelMail webmail client
- Description: SquirrelMail is a standards-based webmail package written in PHP4. It includes built-in pure PHP support for the IMAP and SMTP protocols, and all pages render in pure HTML 4.0 (with no Javascript) for maximum compatibility across browsers. It has very few requirements and is very easy to configure and install. SquirrelMail has all the functionality you would want from an email client, including strong MIME support, address books, and folder manipulation.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

srptools-0.0.4-8.el5 - srptools-0.0.4-10.el5

- Group: System Environment/Base
- Summary: Tools for using the InfiniBand SRP protocol devices

- Description: In conjunction with the kernel ib_srp driver, srptools allows you to discover and use SCSI devices via the SCSI RDMA Protocol over InfiniBand.
- Added Dependencies:
  - libibverbs-devel > 1.1.3
- Removed Dependencies:
  - libibverbs-devel >= 1.1.2-4
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sssd-1.5.1-49.el5 - sssd-1.5.1-58.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.
- Added Dependencies:
  - dbus-devel >= 1.1.2
  - libtdb-devel >= 1.2.10
- Removed Dependencies:
  - dbus-devel
  - libtdb-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

strace-4.5.18-5.el5_5.5 - strace-4.5.18-18.el5

- Group: Development/Debuggers
- Summary: Tracks and displays system calls associated with a running process

- Description: The strace program intercepts and records the system calls called and received by a running process. Strace can print a record of each system call, its arguments and its return value. Strace is useful for diagnosing problems and debugging, as well as for instructional purposes. Install strace if you need a tool to track the system calls made and received by a process.
- 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-0.98.14-1.el5 - subscription-manager-1.0.24-1.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.
- Added Dependencies:
  - GConf2-devel
- 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-1.11-1.el5 - subscription-manager-migration-data-1.11.2.7-1.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-1.6.11-7.el5_6.4 - subversion-1.6.11-10.el5_8

- 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-1.7.2p1-13.el5 - sudo-1.7.2p1-22.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

symlinks-1.2-24.2.2 - symlinks-1.2-26.el5

- Group: Applications/System
- Summary: A utility which maintains a system's symbolic links.
- Description: The symlinks utility performs maintenance on symbolic links. Symlinks checks for symlink problems, including dangling symlinks which point to nonexistent files. Symlinks can also automatically convert absolute symlinks to relative symlinks. Install the symlinks package if you need a program for maintaining symlinks on your 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

syslinux-3.11-7 - syslinux-4.02-7.2.el5

- Group: Applications/System
- Summary: Simple kernel loader which boots from a FAT filesystem
- Description: SYSLINUX is a suite of bootloaders, currently supporting DOS FAT filesystems, Linux ext2/ext3 filesystems (EXTLINUX), PXE network boots (PXELINUX), or ISO 9660 CD-ROMs (ISOLINUX). It also includes a tool, MEMDISK, which loads legacy operating systems from these media.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sysstat-7.0.2-11.el5 - sysstat-7.0.2-12.el5

- Group: Applications/System
- Summary: The sar and iostat system monitoring commands.
- Description: This package provides the sar and iostat commands for Linux. Sar and iostat enable system monitoring of disk, network, and other IO activity.
- 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-bind-4.0.3-5.el5 - system-config-bind-4.0.3-6.el5

- Group: Applications/System
- Summary: The Red Hat BIND DNS Configuration Tool.
- Description: The system-config-bind package provides a graphical user interface (GUI) to configure the Berkeley Internet Name Domain (BIND) Domain Name System (DNS) server, "named", with a set of python modules. Users new to BIND configuration can use this tool to quickly set up a working DNS 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

system-config-cluster-1.0.57-12 - system-config-cluster-1.0.57-16

- 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-lvm-1.1.5-9.el5 - system-config-lvm-1.1.5-13.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

system-config-netboot-0.1.45.1-3.el5 - system-config-netboot-0.1.45.1-5.el5

- Group: Applications/System
- Summary: network booting/install configuration utility (GUI)
- Description: system-config-netboot is a utility which allows you to configure diskless environments and network installations.
- 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-printer-0.7.32.10-1.el5_7.1 - system-config-printer-0.7.32.10-3.el5

- Group: System Environment/Base
- Summary: A printer administration tool
- Description: system-config-printer is a graphical user interface that allows the user to configure a CUPS print 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

systemtap-1.6-6.el5 - systemtap-1.8-6.el5

- Group: Development/System
- Summary: Programmable system-wide instrumentation system
- Description: SystemTap is an instrumentation system for systems running Linux. Developers can write instrumentation scripts to collect data on the operation of the system. The base systemtap package contains/requires the components needed to locally develop and execute systemtap scripts.
- Added Dependencies:
  - gcc-c++
- Removed Dependencies:
  - gettext
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tar-1.15.1-31.el5 - tar-1.15.1-32.el5_8

- Group: Applications/Archiving
- Summary: A GNU file archiving program

- Description: The GNU tar program saves many files together in one archive and can restore individual files (or all of the files) from that archive. Tar can also be used to add supplemental files to an archive and to update or list files in the archive. Tar includes multivolume support, automatic archive compression/decompression, the ability to perform remote archives, and the ability to perform incremental and full backups. If you want to use tar for remote backups, you also need to install the rmt package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tcl-8.4.13-4.el5 - tcl-8.4.13-6.el5

- Group: Development/Languages
- Summary: Tcl scripting language development environment
- Description: The Tcl (Tool Command Language) provides a powerful platform for creating integration applications that tie together diverse applications, protocols, devices, and frameworks. When paired with the Tk toolkit, Tcl provides a fastest and powerful way to create cross-platform GUI applications. Tcl can also be used for a variety of web-related tasks and for creating powerful command languages for applications.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tcsh617-6.17-5.el5 - tcsh617-6.17-7.el5

- Group: System Environment/Shells
- Summary: An enhanced version of csh, the C shell
- Description: Tcsh is an enhanced but completely compatible version of csh, the C shell. Tcsh is a command language interpreter which can be used both as an interactive login shell and as a shell script command processor. Tcsh includes a command line editor, programmable word completion, spelling correction, a history mechanism, job control and a C language like syntax.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

telnet-0.17-39.el5 - telnet-0.17-41.el5

- Group: Applications/Internet
- Summary: The client program for the telnet remote login protocol.
- Description: Telnet is a popular protocol for logging into remote systems over the Internet. The telnet package provides a command line telnet client.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tetex-3.0-33.13.el5 - tetex-3.0-33.15.el5_8.1

- Group: Applications/Publishing
- Summary: The TeX text formatting system.
- Description: TeTeX is an implementation of TeX for Linux or UNIX systems. TeX takes a text file and a set of formatting commands as input and creates a typesetter-independent .dvi (DeVice Independent) file as output. Usually, TeX is used in conjunction with a higher level formatting package like LaTeX or PlainTeX, since TeX by itself is not very user-friendly. The output format needn't to be DVI, but also PDF, when using pdflatex or similar tools. Install tetex if you want to use the TeX text formatting system. Consider to install tetex-latex (a higher level formatting package which provides an easier-to-use interface for TeX). Unless you are an expert at using TeX, you should also install the tetex-doc package, which includes the documentation for TeX.
- 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.22.el5_7 - tomcat5-5.5.23-0jpp.37.el5

- 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-2011l-4.el5 - tzdata-2012i-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

udev-095-14.27.el5_7.1 - udev-095-14.29.el5

- Group: System Environment/Base
- Summary: A userspace implementation of devfs
- Description: The udev package contains an implementation of devfs in userspace using sysfs and netlink.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

util-linux-2.13-0.59.el5 - util-linux-2.13-0.59.el5_8

- Group: System Environment/Base
- Summary: A collection of basic system utilities.
- Description: The util-linux package contains a large variety of low-level system utilities that are necessary for a Linux system to function. Among others, Util-linux contains the fdisk configuration tool and the login 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

vim-7.0.109-7.el5 - vim-7.0.109-7.2.el5

- Group: Applications/Editors
- Summary: The VIM editor.
- Description: VIM (VIsual editor iMproved) is an updated and improved version of the vi editor. Vi was the first real screen-based editor for UNIX, and is still very popular. VIM improves on vi by adding new features: multiple windows, multi-level undo, block highlighting 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

virt-who-0.5-5.el5 - virt-who-0.7-9.el5

- Group: System Environment/Base
- Summary: Agent for reporting virtual guest IDs to subscription-manager
- Description: Agent that collects information about virtual guests present in the system and report them to the subscription 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

vsftpd-2.0.5-24.el5 - vsftpd-2.0.5-28.el5

- Group: System Environment/Daemons
- Summary: vsftpd - Very Secure Ftp Daemon
- Description: vsftpd is a Very Secure FTP daemon. It was written completely from scratch.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes

- No removed obsoletes

wget-1.11.4-2.el5_4.1 - wget-1.11.4-3.el5_8.2

- Group: Applications/Internet
- Summary: A utility for retrieving files using the HTTP or FTP protocols.
- Description: GNU Wget is a file retrieval utility which can use either the HTTP or FTP protocols. Wget features include the ability to work in the background while you are logged out, recursive retrieval of directories, file name wildcard matching, remote file timestamp storage and comparison, use of Rest with FTP servers and Range with HTTP servers to retrieve files over slow or unstable connections, support for Proxy servers, and configurability.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

wireshark-1.0.15-1.el5_6.4 - wireshark-1.0.15-5.el5

- Group: Applications/Internet
- Summary: Network traffic analyzer
- Description: Wireshark is a network traffic analyzer for Unix-ish operating systems. This package lays base for libpcap, a packet capture and filtering library, contains command-line utilities, contains plugins and documentation for wireshark. A graphical user interface is packaged separately to GTK+ package.
- 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-3.0.3-135.el5 - xen-3.0.3-142.el5

- 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-2.3.14-16.el5 - xinetd-2.3.14-17.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-server-1.1.1-48.90.el5 - xorg-x11-server-1.1.1-48.100.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-1.9.2.26-1.el5_7 - xulrunner-10.0.11-1.el5_8

- 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:
  - libpng-devel
  - mesa-libGL-devel
  - nspr-devel >= 4.8.9
  - nss-devel >= 3.13.1
- Removed Dependencies:
  - nspr-devel >= 4.8
  - nss-devel >= 3.12.8
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yelp-2.16.0-26.el5 - yelp-2.16.0-29.el5

- 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 >= 10.0
- Removed Dependencies:
    - gecko-devel-unstable >= 1.9.2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ypserv-2.19-9.el5 - ypserv-2.19-9.el5_8.1

- 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-3.2.22-39.el5 - yum-3.2.22-40.el5

- Group: System Environment/Base
- Summary: RPM installer/updater
- Description: Yum is a utility that can check for and automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically prompting the user as 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

yum-metadata-parser-1.1.2-3.el5 - yum-metadata-parser-1.1.2-4.el5

- Group: Development/Libraries
- Summary: A fast metadata parser for yum
- Description: Fast metadata parser for yum implemented in C.
- 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-0.5.4-26.el5 - yum-rhn-plugin-0.5.4-29.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

yum-updatesd-0.9-2.el5 - yum-updatesd-0.9-5.el5

- Group: System Environment/Base
- Summary: Update notification daemon
- Description: yum-updatesd provides a daemon which checks for available updates and can notify you when they are available via email, syslog or dbus.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

zlib-1.2.3-4.el5 - zlib-1.2.3-7.el5

- Group: System Environment/Libraries
- Summary: The zlib compression and decompression library.
- Description: Zlib is a general-purpose, patent-free, lossless data compression library which is used by many different programs.
- Added Dependencies:
  - autoconf
  - automake
  - libtool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

zsh-4.2.6-6.el5 - zsh-4.2.6-8.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

ant17-1.7.1-1jpp.0

- Group: Development/Build Tools
- Summary: Build tool for Java supporting version 1.7
- Description: Ant is a platform-independent build tool for java. It's used by apache jakarta and xml projects.

hypervkvpd-0-0.7.el5

- 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.

java-1.7.0-openjdk-1.7.0.9-2.3.3.el5.1

- Group: Development/Languages
- Summary: OpenJDK Runtime Environment
- Description: The OpenJDK runtime environment.

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.

php53-odbc64-5.3.3-2.el5

- Group: Development/Languages
- Summary: A module for PHP applications that use ODBC databases via unixODBC64
- Description: The php53-odbc64 package contains a dynamic shared object that will add database support through ODBC to PHP. ODBC is an open specification which provides a consistent API for developers to use for accessing data sources (which are often, but not always, databases). PHP is an HTML-embeddable scripting language. If you need ODBC support for PHP applications, you will need to install this package and the php package. The php53-odbc64 package uses the 64-bit ABI from unixODBC 2.2.12.

rsyslog5-5.8.12-4.el5

- Group: System Environment/Daemons
- Summary: Enhanced system logging and kernel message trapping daemon
- Description: Rsyslog is an enhanced, multi-threaded syslog daemon. It supports MySQL, syslog/TCP, RFC 3195, permitted sender lists, filtering on any message part, and fine grain output format control. It is compatible with stock sysklogd and can be used as a drop-in replacement. Rsyslog is simple to set up, with advanced features suitable for enterprise-class, encryption-protected syslog relay chains.

scl-utils-20120927-2.el5

- Group: Applications/File
- Summary: Utilities for alternative packaging
- Description: Run-time utility for alternative packaging.

A.2.2. Dropped Packages

None

A.2.3. Updated Packages

ImageMagick-6.2.8.0-12.el5 - ImageMagick-6.2.8.0-15.el5_8

- Group: Applications/Multimedia
- Summary: An X application for displaying and manipulating images.
- Description: ImageMagick(TM) is an image display and manipulation tool for the X Window System. ImageMagick can read and write JPEG, TIFF, PNM, GIF, and Photo CD image formats. It can resize, rotate, sharpen, color reduce, or add special effects to an image, and when finished you can either save the completed work in the original format or a different one. ImageMagick also includes command line programs for creating animated or transparent .gifs, creating composite images, creating thumbnail images, and more. ImageMagick is one of your choices if you need a program to manipulate and dis play images. If you want to develop your own applications which use ImageMagick code or APIs, you need to install ImageMagick-devel as well.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

OpenIPMI-2.0.16-12.el5 - OpenIPMI-2.0.16-16.el5

- Group: System Environment/Base
- Summary: OpenIPMI (Intelligent Platform Management Interface) library and tools
- Description: The Open IPMI project aims to develop an open code base to allow access to platform information using Intelligent Platform Management Interface (IPMI). This package contains the tools of the OpenIPMI 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

aide-0.13.1-6.el5 - aide-0.13.1-8.el5

- Group: Applications/System
- Summary: Intrusion detection environment
- Description: AIDE (Advanced Intrusion Detection Environment) is a file integrity checker and intrusion detection program.
- Added Dependencies:
  - libgcrypt-devel >= 1.4.4-5.el5_8.2
- Removed Dependencies:
  - libgcrypt-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

alsa-utils-1.0.17-6.el5 - alsa-utils-1.0.17-7.el5

- Group: Applications/Multimedia
- Summary: Advanced Linux Sound Architecture (ALSA) utilities
- Description: This package contains command line utilities for the Advanced Linux Sound Architecture (ALSA).
- 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-11.1.2.250-1 - anaconda-11.1.2.259-1

- 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.
- Added Dependencies:
  - kudzu-devel >= 1.2.57.1.26-7
- Removed Dependencies:
  - kudzu-devel >= 1.2.57.1.26-3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

aspell-en-6.0-2.1 - aspell-en-6.0-3

- Group: Applications/Text
- Summary: English dictionaries for Aspell.

- Description: Provides the word list/dictionaries for the following: English, Canadian English, British English
- 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.rc2.163.el5 - autofs-5.0.1-0.rc2.177.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

bind-9.3.6-20.P1.el5 - bind-9.3.6-20.P1.el5_8.5

- 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

bind97-9.7.0-6.P2.el5_7.4 - bind97-9.7.0-17.P2.el5

- 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.
- Added Dependencies:
  - docbook-style-xsl
  - libxslt
- 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 - binutils-2.17.50.0.6-20.el5_8.3

- 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

busybox-1.2.0-13.el5 - busybox-1.2.0-14.el5

- Group: System Environment/Shells
- Summary: Statically linked binary providing simplified versions of system commands
- Description: Busybox is a single binary which includes versions of a large number of system commands, including a shell. This package can be very useful for recovering from certain types of system failures, particularly those involving broken shared libraries.
- 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-2.0.115-96.el5 - cman-2.0.115-109.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

coreutils-5.97-34.el5 - coreutils-5.97-34.el5_8.1

- Group: System Environment/Base
- Summary: The GNU core utilities: a set of tools commonly used in shell scripts

- Description: These are the GNU core utilities. This package is the combination of the old GNU fileutils, sh-utils, and textutils packages.
- 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-2.6-23.el5_4.1 - cpio-2.6-25.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

crontabs-1.10-8 - crontabs-1.10-11.el5

- Group: System Environment/Base
- Summary: Root crontab files used to schedule the execution of programs.
- Description: The crontabs package contains root crontab files. Crontab is the program used to install, uninstall or list the tables used to drive the cron daemon. The cron daemon checks the crontab files to see when particular commands are scheduled to be executed. If commands are scheduled, it executes them. Crontabs handles a basic system function, so it should be

installed on your 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

cscope-15.5-15.1.el5_3.1 - cscope-15.5-20.el5

- Group: Development/Tools
- Summary: C source code tree search and browse tool
- Description: cscope is a mature, ncurses based, C source code tree browsing tool. It allows users to search large source code bases for variables, functions, macros, etc, as well as perform general regex and plain text searches. Results are returned in lists, from which the user can select individual matches for use in file editing.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cvs-1.11.22-11.el5 - cvs-1.11.22-11.el5_8.1

- Group: Development/Tools
- Summary: A version control system.
- Description: CVS (Concurrent Versions System) is a version control system that can record the history of your files (usually, but not always, source code). CVS only stores the differences between versions, instead of every version of every file you have ever created. CVS also keeps a log of who, when, and why changes occurred. CVS is very helpful for managing releases and controlling the concurrent editing of source files among multiple authors. Instead of providing version control for a collection of files in a single directory, CVS provides version control for a hierarchical collection of directories consisting of revision controlled files. These directories and files can then be combined together to form a software release.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

cyrus-sasl-2.1.22-5.el5_4.3 - cyrus-sasl-2.1.22-7.el5_8.1

- Group: System Environment/Libraries
- Summary: The Cyrus SASL library.
- Description: The cyrus-sasl package contains the Cyrus implementation of SASL. SASL is the Simple Authentication and Security Layer, a method for adding authentication support to connection-based 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

dapl-2.0.25-2.3.el5 - dapl-2.0.34-1.el5

- Group: System Environment/Libraries
- Summary: Library providing access to the DAT 1.2 and 2.0 APIs
- Description: libdat and libdapl provide a userspace implementation of the DAT 1.2 and 2.0 API and is built to natively support InfiniBand/iWARP network technology.
- Added Dependencies:
  - libibverbs-devel > 1.1.4
  - librdmacm-devel > 1.0.14
- Removed Dependencies:
  - libibverbs-devel >= 1.1.3
  - librdmacm-devel >= 1.0.10
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

devhelp-0.12-21.el5 - devhelp-0.12-22.el5

- Group: Development/Tools
- Summary: API document browser
- Description: An API document browser for GNOME 2.
- Added Dependencies:
  - gecko-devel-unstable >= 2.0
- Removed Dependencies:
  - gecko-devel-unstable >= 1.9.2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

device-mapper-multipath-0.4.7-48.el5 - device-mapper-multipath-0.4.7-54.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 - dhcp-3.0.5-31.el5_8.1

- 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

diffutils-2.8.1-15.2.3.el5 - diffutils-2.8.1-16.el5

- Group: Applications/Text
- Summary: A GNU collection of diff utilities.
- Description: Diffutils includes four utilities: diff, cmp, diff3 and sdiff. Diff compares two files and shows the differences, line by line. The cmp command shows the offset and line numbers where two files differ, or cmp can show the characters that differ between the two files. The diff3 command shows the differences between three files. Diff3 can be used when two people have made independent changes to a common original; diff3 can produce a merged file that contains both sets of changes and warnings about conflicts. The sdiff command can be used to merge two files interactively. Install diffutils if you need to compare text 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

doxygen-1.4.7-1.1 - doxygen-1.4.7-2

- Group: Development/Tools
- Summary: A documentation system for C/C++.
- Description: Doxygen can generate an online class browser (in HTML) and/or a reference manual (in LaTeX) from a set of documented source files. The documentation is extracted directly from the sources. Doxygen can also be configured to extract the code structure from undocumented source 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

e2fsprogs-1.39-33.el5 - e2fsprogs-1.39-35.el5

- 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

e4fsprogs-1.41.12-2.el5 - e4fsprogs-1.41.12-3.el5

- Group: System Environment/Base

- Summary: Utilities for managing the fourth extended (ext4) filesystem
- Description: The e4fsprogs package contains a number of utilities for creating, checking, modifying, and correcting any inconsistencies in the fourth extended (ext4) filesystem. E4fsprogs contains e4fsck (used to repair filesystem inconsistencies after an unclean shutdown), mke4fs (used to initialize a partition to contain an empty ext4 filesystem), debugfs (used to examine the internal structure of a filesystem, to manually repair a corrupted filesystem, or to create test cases for e4fsck), tune4fs (used to modify filesystem parameters), and most of the other core ext4fs filesystem utilities. Please note that "e4fsprogs" simply contains renamed static binaries from the equivalent upstream e2fsprogs release; it is packaged this way for Red Hat Enterprise Linux 5 to ensure that the many changes included for ext4 do not destabilize the core e2fsprogs in RHEL5. You should install the e4fsprogs package if you need to manage the performance of an ext4 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

esc-1.1.0-12.el5 - esc-1.1.0-13.el5_8.2

- Group: Applications/Internet
- Summary: Enterprise Security Client Smart Card Client
- Description: Enterprise Security Client allows the user to enroll and manage their cryptographic smartcards.
- Added Dependencies:
  - xulrunner >= 10.0.0
  - xulrunner-devel >= 10.0.0
- Removed Dependencies:
  - xulrunner >= 1.9.2
  - xulrunner-devel >= 1.9.2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

etherboot-5.4.4-15.el5 - etherboot-5.4.4-16.el5

- Group: Development/Tools
- Summary: Etherboot collection of boot roms
- Description: Etherboot is a software package for creating ROM images that can download code over an Ethernet network to be executed on an x86 computer. Many network adapters have a socket where a ROM chip can be installed. Etherboot is code that can be put in such a ROM
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

expat-1.95.8-8.3.el5_5.3 - expat-1.95.8-11.el5_8

- Group: System Environment/Libraries
- Summary: A library for parsing XML.
- Description: This is expat, the C library for parsing XML, written by James Clark. Expat is a stream oriented XML parser. This means that you register handlers with the parser prior to starting the parse. These handlers are called when the parser discovers the associated structures in the document being parsed. A start tag is an example of the kind of structures for which you may register handlers.
- Added Dependencies:
  - check-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

file-4.17-21 - file-4.17-28

- Group: Applications/File
- Summary: A utility for determining file types.

- Description: The file command is used to identify a particular file according to the type of data contained by the file. File can identify many different file types, including ELF binaries, system libraries, RPM packages, and different graphics formats. You should install the file package, since the file command is such a useful utility.
- 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-3.6.26-1.el5_7 - firefox-10.0.11-1.el5_8

- 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:
  - xulrunner-devel >= 10.0.11-1
- Removed Dependencies:
  - xulrunner-devel >= 1.9.2.26-1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

freeradius2-2.1.12-3.el5 - freeradius2-2.1.12-5.el5

- Group: System Environment/Daemons
- Summary: High-performance and highly configurable free RADIUS server
- Description: The FreeRADIUS Server Project is a high performance and highly configurable GPL'd free RADIUS server. The server is similar in some respects to Livingston's 2.0 server. While FreeRADIUS started as a variant of the Cistron RADIUS server, they don't share a lot in common any more. It now has many more features than Cistron or Livingston, and is much more configurable. FreeRADIUS is an Internet authentication daemon, which implements the RADIUS protocol, as defined in RFC 2865 (and others). It allows Network Access Servers

(NAS boxes) to perform authentication for dial-up users. There are also RADIUS clients available for Web servers, firewalls, Unix logins, and more. Using RADIUS allows authentication and authorization for a network to be centralized, and minimizes the amount of re-configuration which has to be done when adding or deleting new users.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

freetype-2.2.1-28.el5_7.2 - freetype-2.2.1-31.el5_8.1

- 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

ftp-0.17-37.el5 - ftp-0.17-38.el5

- Group: Applications/Internet
- Summary: The standard UNIX FTP (File Transfer Protocol) client.
- Description: The ftp package provides the standard UNIX command-line FTP (File Transfer Protocol) client. FTP is a widely used protocol for transferring files over the Internet and for archiving files. If your system is on a network, you should install ftp in order to do file transfers.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gawk-3.1.5-15.el5 - gawk-3.1.5-16.el5

- Group: Applications/Text
- Summary: The GNU version of the awk text processing utility.
- Description: The gawk packages contains the GNU version of awk, a text processing utility. Awk interprets a special-purpose programming language to do quick and easy text pattern matching and reformatting jobs. Install the gawk package if you need a text processing utility. Gawk is considered to be a standard Linux tool for processing text.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gcc-4.1.2-52.el5 - gcc-4.1.2-54.el5

- Group: Development/Languages
- Summary: Various compilers (C, C++, Objective-C, Java, ...)
- Description: The gcc package contains the GNU Compiler Collection version 4.1. You'll need this package in order to compile C code.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gcc44-4.4.6-3.el5.1 - gcc44-4.4.7-1.el5

- Group: Development/Languages
- Summary: GNU Compiler Collection version 4.4
- Description: The gcc44 package contains the GNU Compiler Collection version 4.4.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdb-7.0.1-42.el5 - gdb-7.0.1-45.el5

- Group: Development/Debuggers
- Summary: A GNU source-level debugger for C, C++, Java and other languages
- Description: GDB, the GNU debugger, allows you to debug programs written in C, C++, Java, and other languages, by executing them in a controlled fashion and printing their data.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gdbm-1.8.0-26.2.1.el5_6.1 - gdbm-1.8.0-28.el5

- Group: System Environment/Libraries
- Summary: A GNU set of database routines which use extensible hashing.
- Description: Gdbm is a GNU database indexing library, including routines which use extensible hashing. Gdbm works in a similar way to standard UNIX dbm routines. Gdbm is useful for developers who write C applications and need access to a simple and efficient database or who are building C applications which will use such a database. If you're a C developer and your programs need access to simple database routines, you should install gdbm. You'll also need to install gdbm-devel.

- 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-0.1.62-34.el5 - gfs2-utils-0.1.62-35.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

ghostscript-8.70-14.el5 - ghostscript-8.70-14.el5_8.1

- Group: Applications/Publishing
- Summary: A PostScript(TM) interpreter and renderer.
- Description: Ghostscript is a set of software that provides a PostScript(TM) interpreter, a set of C procedures (the Ghostscript library, which implements the graphics capabilities in the PostScript language) and an interpreter for Portable Document Format (PDF) files. Ghostscript translates PostScript code into many common, bitmapped formats, like those understood by your printer or screen. Ghostscript is normally used to display PostScript files and to print PostScript files to non-PostScript printers. If you need to display PostScript files or print them to non-PostScript printers, you should install ghostscript. If you install ghostscript, you also need to install the ghostscript-fonts package.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gimp-2.2.13-2.0.7.el5_6.2 - gimp-2.2.13-2.0.10.el5

- Group: Applications/Multimedia
- Summary: GNU Image Manipulation Program
- Description: GIMP (GNU Image Manipulation Program) is a powerful image composition and editing program, which can be extremely useful for creating logos and other graphics for webpages. GIMP has many of the tools and filters you would expect to find in similar commercial offerings, and some interesting extras as well. GIMP provides a large image manipulation toolbox, including channel operations and layers, effects, sub-pixel imaging and anti-aliasing, and conversions, all with multi-level undo.
- 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-2.5-81 - glibc-2.5-107

- 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-session-2.16.0-8.el5 - gnome-session-2.16.0-10.el5

- Group: User Interface/Desktops
- Summary: GNOME session manager
- Description: gnome-session manages a GNOME desktop session. It starts up the other core GNOME components and handles logout and saving the session.
- 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-vfs2-2.16.2-8.el5 - gnome-vfs2-2.16.2-10.el5

- 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-1.4.1-3.el5_4.8 - gnutls-1.4.1-10.el5

- 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

gpxe-0.9.7-8.el5 - gpxe-0.9.7-9.el5

- Group: System Environment/Base
- Summary: A network boot loader
- Description: gPXE is an open source network bootloader. It provides a direct replacement for proprietary PXE ROMs, with many extra features such as DNS, HTTP, iSCSI, 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

grub-0.97-13.5 - grub-0.97-13.10.el5

- Group: System Environment/Base
- Summary: GRUB - the Grand Unified Boot Loader.
- Description: GRUB (Grand Unified Boot Loader) is an experimental boot loader capable of booting into most free operating systems - Linux, FreeBSD, NetBSD, GNU Mach, and others as well as most commercial operating systems.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gtk+-1.2.10-56.el5 - gtk+-1.2.10-57.el5

- Group: System Environment/Libraries
- Summary: The GIMP ToolKit (GTK+), a library for creating GUIs for X.
- Description: The gtk+ package contains the GIMP ToolKit (GTK+), a library for creating graphical user interfaces for the X Window System. GTK+ was originally written for the GIMP (GNU Image Manipulation Program) image processing program, but is now used by several other programs as well.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

gtk2-2.10.4-21.el5_7.7 - gtk2-2.10.4-29.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

hal-0.5.8.1-62.el5 - hal-0.5.8.1-64.el5

- Group: System Environment/Libraries
- Summary: Hardware Abstraction Layer
- Description: HAL is daemon for collection and maintaining information from several sources about the hardware on the system. It provides a live device list through D-BUS.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hplip3-3.9.8-11.el5_6.1 - hplip3-3.9.8-15.el5

- Group: System Environment/Daemons
- Summary: HP Linux Imaging and Printing Project
- Description: The Hewlett-Packard Linux Imaging and Printing Project provides drivers for HP printers and multi-function peripherals.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

hsqldb-1.8.0.9-1jpp.2 - hsqldb-1.8.0.9-1jpp.3

- Group: Development/Java
- Summary: Hsqldb Database Engine
- Description: HSQLdb is a relational database engine written in JavaTM , with a JDBC driver, supporting a subset of ANSI-92 SQL. It offers a small (about 100k), fast database engine which offers both in memory and disk based tables. Embedded and server modes are available. Additionally, it includes tools such as a minimal web server, in-memory query and management tools (can be run as applets or servlets, too) and a number of demonstration examples. Downloaded code should be regarded as being of production quality. The product is currently

being used as a database and persistence engine in many Open Source Software projects and even in commercial projects and products! In it's current version it is extremely stable and reliable. It is best known for its small size, ability to execute completely in memory and its speed. Yet it is a completely functional relational database management system that is completely free under the Modified BSD License. Yes, that's right, completely free of cost or restrictions!

- 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-2.2.3-63.el5 - httpd-2.2.3-74.el5

- 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-0.213.26-1.el5 - hwdata-0.213.28-1.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

ibsim-0.5-2.el5 - ibsim-0.5-3.el5

- Group: System Environment/Libraries
- Summary: InfiniBand fabric simulator for management
- Description: ibsim provides simulation of infiniband fabric for using with OFA OpenSM, diagnostic and management tools.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ibutils-1.2-11.2.el5 - ibutils-1.5.7-1.el5

- Group: System Environment/Libraries
- Summary: OpenIB Mellanox InfiniBand Diagnostic Tools
- Description: ibutils provides IB network and path diagnostics.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

infiniband-diags-1.5.3-1.el5 - infiniband-diags-1.5.12-2.el5

- Group: System Environment/Libraries

- Summary: OpenFabrics Alliance InfiniBand Diagnostic Tools
- Description: This package provides IB diagnostic programs and scripts needed to diagnose an IB subnet.
- Added Dependencies:
  - opensm-devel >= 3.3.13
  - perl
- Removed Dependencies:
  - opensm-devel >= 3.3.0
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

initscripts-8.45.42-1.el5 - initscripts-8.45.42-1.el5_8.1

- 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-2.1.3-1.el5 - ipa-client-2.1.3-4.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

iproute-2.6.18-13.el5 - iproute-2.6.18-15.el5

- Group: Applications/System
- Summary: Advanced IP routing and network device configuration tools.
- Description: The iproute package contains networking utilities (ip and rtmon, for example) which are designed to use the advanced networking capabilities of the Linux 2.4.x and 2.6.x kernel.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

ipsec-tools-0.6.5-14.el5_5.5 - ipsec-tools-0.6.5-14.el5_8.5

- Group: System Environment/Base
- Summary: Tools for configuring and using IPSEC
- Description: This is the IPsec-Tools package. You need this package in order to really use the IPsec functionality in the linux-2.5+ kernels. This package builds: - setkey, a program to directly manipulate policies and SAs - racoon, an IKEv1 keying daemon
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

iptables-1.3.5-9.1.el5 - iptables-1.3.5-9.2.el5_8

- Group: System Environment/Base
- Summary: Tools for managing Linux kernel packet filtering capabilities.
- Description: The iptables utility controls the network packet filtering code in the Linux kernel. If you need to set up firewalls and/or IP masquerading, you should install this package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

iscsi-initiator-utils-6.2.0.872-13.el5 - iscsi-initiator-utils-6.2.0.872-16.el5

- Group: System Environment/Daemons
- Summary: iSCSI daemon and utility programs
- Description: 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.
- Added Dependencies:
  - libtool
- 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-1.6.0.0-1.24.1.10.4.el5 - java-1.6.0-openjdk-1.6.0.0-1.30.1.11.5.el5

- 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

jpackage-utils-1.7.3-1jpp.2.el5 - jpackage-utils-1.7.3-1jpp.3.el5

- Group: Utilities
- Summary: JPackage utilities
- Description: Utilities for the JPackage Project <http://www.jpackage.org/>: * /usr/bin/build-classpath build the Java classpath in a portable manner * /usr/bin/build-jar-repository build a jar repository in a portable manner * /usr/bin/rebuild-jar-repository rebuild a jar repository in a portable manner (after a jvm change...) * /usr/bin/build-classpath-directory build the Java classpath from a directory * /usr/bin/diff-jars show jar content differences * /usr/bin/jvmjar install jvm extensions * /usr/bin/create-jar-links create custom jar links * /usr/bin/clean-binary-files remove binary files from sources * /usr/bin/check-binary-files check for presence of unexpected binary files * /usr/share/java-utils/java-functions shell script functions library for Java applications * /etc/java/jpackage-release string identifying the currently installed JPackage release * /etc/java/java.conf system-wide Java configuration file * /etc/rpm/macros.jpackage RPM macros for Java packagers and developers * /usr/share/doc/jpackage-utils-1.7.3/jpackage-policy Java packaging policy for packagers and developers It contains also the License, man pages, documentation, XSL files of general use with maven2, a header file for spec files 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

kbd-1.12-21.el5 - kbd-1.12-22.el5

- Group: System Environment/Base
- Summary: Tools for configuring the console (keyboard, virtual terminals, etc.)

- Description: The kbd package contains tools for managing a Linux system's console's behavior, including the keyboard, the screen fonts, the virtual terminals and font 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

kdebase-3.5.4-25.el5 - kdebase-3.5.4-26.el5

- Group: User Interface/Desktops
- Summary: K Desktop Environment - core files
- Description: Core applications for the K Desktop Environment. Included are: kdm (replacement for xdm), kwin (window manager), konqueror (filemanager, web browser, ftp client, ...), konsole (xterm replacement), kpanel (application starter and desktop pager), kaudio (audio server), kdehelp (viewer for kde help files, info and man pages), kthememgr (system for managing alternate theme packages) plus other KDE components (kcheckpass, kikbd, kscreensaver, kcontrol, kfind, kfontmanager, kmenuedit).
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

kernel-2.6.18-308.el5 - kernel-2.6.18-348.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-154.el5 - kexec-tools-1.102pre-161.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

ksh-20100621-5.el5 - ksh-20100621-12.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

kudzu-1.2.57.1.26-3 - kudzu-1.2.57.1.26-7

- Group: Applications/System
- Summary: The Red Hat Linux hardware probing tool.
- Description: Kudzu is a hardware probing tool run at system boot time to determine what hardware has been added or removed from the 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

kvm-83-249.el5 - kvm-83-262.el5

- 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 = 2.6.18-339.el5
  - kernel-devel = 2.6.18-339.el5
- Removed Dependencies:
  - kernel-debug-devel = 2.6.18-304.el5
  - kernel-devel = 2.6.18-304.el5
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

lftp-3.7.11-7.el5 - lftp-3.7.11-8.el5

- Group: Applications/Internet
- Summary: A sophisticated file transfer program
- Description: LFTP is a sophisticated ftp/http file transfer program. 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.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libcxgb3-1.3.0-1.el5 - libcxgb3-1.3.1-2.el5

- Group: System Environment/Libraries
- Summary: Chelsio T3 iWARP HCA Userspace Driver
- Description: Userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables Chelsio iWARP capable ethernet devices.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libcxgb4-1.1.1-2.el5 - libcxgb4-1.2.0-2.el5

- Group: System Environment/Libraries
- Summary: Chelsio T3 iWARP HCA Userspace Driver
- Description: Userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables Chelsio iWARP capable ethernet devices.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libexif-0.6.20-1.el5_7.1 - libexif-0.6.21-1.el5_8

- Group: System Environment/Libraries
- Summary: Library for extracting extra information from image files
- Description: Most digital cameras produce EXIF files, which are JPEG files with extra tags that contain information about the image. The EXIF library allows you to parse an EXIF file and read the data from those tags.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libgcrypt-1.4.4-5.el5 - libgcrypt-1.4.4-5.el5_8.2

- Group: System Environment/Libraries
- Summary: A general-purpose cryptography library
- Description: Libgcrypt is a general purpose crypto library based on the code used in GNU Privacy Guard. This is a development version.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibcm-1.0.5-1.el5 - libibcm-1.0.5-2.el5

- Group: System Environment/Libraries
- Summary: Userspace InfiniBand Connection Manager
- Description: libibcm provides a userspace library that handles the majority of the low level work required to open an RDMA connection between two machines.
- Added Dependencies:
  - libibverbs-devel >= 1.1
- Removed Dependencies:
  - libibverbs-devel >= 1.1.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibmad-1.3.3-1.el5 - libibmad-1.3.8-1.el5

- Group: System Environment/Libraries
- Summary: OpenFabrics Alliance InfiniBand MAD library
- Description: libibmad provides low layer IB functions for use by the IB diagnostic and management programs. These include MAD, SA, SMP, and other basic IB functions.
- Added Dependencies:
  - libibumad-devel = 1.3.7
- Removed Dependencies:
  - libibumad-devel = 1.3.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibumad-1.3.3-1.el5 - libibumad-1.3.7-1.el5

- Group: System Environment/Libraries
- Summary: OpenFabrics Alliance InfiniBand umad (user MAD) library

- Description: libibumad provides the user MAD library functions which sit on top of the user MAD modules in the kernel. These are used by the IB diagnostic and management tools, including OpenSM.
- Added Dependencies:
  - autoconf
  - automake
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libibverbs-1.1.3-2.el5 - libibverbs-1.1.6-3.el5

- Group: System Environment/Libraries
- Summary: A library for direct userspace use of RDMA (InfiniBand/iWARP) hardware
- Description: libibverbs is a library that allows userspace processes to use RDMA "verbs" as described in the InfiniBand Architecture Specification and the RDMA Protocol Verbs Specification. This includes direct hardware access from userspace to InfiniBand/iWARP adapters (kernel bypass) for fast path operations. For this library to be useful, a device-specific plug-in module should also be 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

libipathverbs-1.2-2.el5 - libipathverbs-1.2-3.el5

- Group: System Environment/Libraries
- Summary: QLogic InfiniPath HCA Userspace Driver
- Description: QLogic hardware driver for use with libibverbs user space verbs access library. This driver supports QLogic InfiniPath based cards.
- Added Dependencies:

    - valgrind-devel
  - Removed Dependencies:
    - valgrind
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

libmlx4-1.0.1-7.el5 - libmlx4-1.0.2-1.el5

  - Group: System Environment/Libraries
  - Summary: Mellanox ConnectX InfiniBand HCA Userspace Driver
  - Description: libmlx4 provides a device-specific userspace driver for Mellanox ConnectX HCAs for use with the libibverbs library.
  - Added Dependencies:
    - libibverbs-devel > 1.1.4
  - Removed Dependencies:
    - libibverbs-devel >= 1.1.3
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

libmthca-1.0.5-6.el5 - libmthca-1.0.6-1.el5

  - Group: System Environment/Libraries
  - Summary: Mellanox InfiniBand HCA Userspace Driver
  - Description: libmthca provides a device-specific userspace driver for Mellanox HCAs (MT23108 InfiniHost and MT25208 InfiniHost III Ex) for use with the libibverbs library.
  - Added Dependencies:
    - libibverbs-devel > 1.1.4
  - Removed Dependencies:
    - libibverbs-devel >= 1.1.3

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libnes-0.9.0-2.el5 - libnes-1.1.3-1.el5

- Group: System Environment/Libraries
- Summary: NetEffect RNIC Userspace Driver
- Description: Userspace hardware driver for use with the libibverbs InfiniBand/iWARP verbs library. This driver enables NetEffect iWARP capable ethernet devices.
- Added Dependencies:
  - libibverbs-devel > 1.1.4
- Removed Dependencies:
  - libibverbs-devel >= 1.1.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libpng-1.2.10-7.1.el5_7.5 - libpng-1.2.10-17.el5_8

- Group: System Environment/Libraries
- Summary: A library of functions for manipulating PNG image format files
- Description: The libpng package contains a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files. PNG is a bit-mapped graphics format similar to the GIF format. PNG was created to replace the GIF format, since GIF uses a patented data compression algorithm. Libpng should be installed if you need to manipulate PNG 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

librdmacm-1.0.10-1.el5 - librdmacm-1.0.15-2.el5

- Group: System Environment/Libraries
- Summary: Userspace RDMA Connection Manager
- Description: librdmacm provides a userspace RDMA Communication Managment API.
- Added Dependencies:
  - libibverbs-devel >= 1.1
- Removed Dependencies:
  - libibverbs-devel >= 1.1.3
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libsdp-1.1.99-11.el5 - libsdp-1.1.108-1.el5

- Group: System Environment/Libraries
- Summary: A library for direct userspace use of Sockets Direct Protocol
- Description: libsdp is an LD_PRELOAD-able library that can be used to have existing applications use InfiniBand Sockets Direct Protocol (SDP) instead of TCP sockets, transparently and without recompilation. For information on how to configure libsdp, see libsdp.conf, which is installed in $(sysconfdir) (usually /usr/local/etc or /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

libtalloc-2.0.1-11.el5 - libtalloc-2.0.7-2.el5

- Group: System Environment/Daemons
- Summary: A hierarchical memory allocator
- Description: A library that implements a hierarchical allocator with destructors.
- Added Dependencies:
  - doxygen
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libtdb-1.2.1-6.el5 - libtdb-1.2.10-1.el5

- Group: System Environment/Daemons
- Summary: The tdb library
- Description: A library that implements a trivial database.
- Added Dependencies:
  - python-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libtiff-3.8.2-7.el5_6.7 - libtiff-3.8.2-15.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

libuser-0.54.7-2.1.el5_5.2 - libuser-0.54.7-3.el5

- Group: System Environment/Base
- Summary: A user and group account administration library.
- Description: The libuser library implements a standardized interface for manipulating and administering user and group accounts. The library uses pluggable back-ends to interface to its data sources. Sample applications modeled after those included with the shadow password suite are included.
- 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-0.8.2-25.el5 - libvirt-0.8.2-29.el5

- 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

libvorbis-1.1.2-3.el5_4.4 - libvorbis-1.1.2-3.el5_7.6

- Group: System Environment/Libraries
- Summary: The Vorbis General Audio Compression Codec.
- Description: Ogg Vorbis is a fully open, non-proprietary, patent-and royalty-free, general-purpose compressed audio format for audio and music at fixed and variable bitrates from 16 to 128 kbps/channel. The libvorbis package contains runtime libraries for use in programs that support Ogg Voribs.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libwpd-0.8.7-3.el5 - libwpd-0.8.7-3.1.el5_8

- Group: System Environment/Libraries
- Summary: Library for reading and converting WordPerfect(tm) documents.
- Description: Library that handles Word Perfect documents.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

libxml2-2.6.26-2.1.12.el5_7.2 - libxml2-2.6.26-2.1.15.el5_8.6

- 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

libxslt-1.1.17-2.el5_2.2 - libxslt-1.1.17-4.el5_8.3

- Group: Development/Libraries
- Summary: Library providing the Gnome XSLT engine
- Description: This C library allows to transform XML files into other XML files (or HTML, text, ...) using the standard XSLT stylesheet transformation mechanism. To use it you need to have a version of libxml2 >= 2.6.25 installed. The xsltproc command is a command line interface to the XSLT engine
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

linuxwacom-0.7.8.3-11.el5 - linuxwacom-0.7.8.3-11.2.el5_8

- Group: User Interface/X Hardware Support
- Summary: Wacom Drivers from Linux Wacom Project
- Description: The Linux Wacom Project manages the drivers, libraries, and documentation for configuring and running Wacom tablets under the Linux operating system. It contains diagnostic applications as well as X.org XInput drivers.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

logrotate-3.7.4-12 - logrotate-3.7.4-14

- Group: System Environment/Base
- Summary: Rotates, compresses, removes and mails system log files.
- Description: The logrotate utility is designed to simplify the administration of log files on a system which generates a lot of log files. Logrotate allows for the automatic rotation compression, removal and mailing of log files. Logrotate can be set to handle a log file daily, weekly, monthly or when the log file gets to a certain size. Normally, logrotate runs as a daily cron job. Install the logrotate package if you need a utility to deal with the log files on your 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

logwatch-7.3-9.el5_6 - logwatch-7.3-10.el5

- Group: Applications/System
- Summary: A log file analysis program
- Description: Logwatch is a customizable, pluggable log-monitoring system. It will go through your logs for a given period of time and make a report in the areas that you wish with the detail that you wish. Easy to use - works right out of the package on many systems.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

lvm2-2.02.88-7.el5 - lvm2-2.02.88-10.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

m2crypto-0.16-8.el5 - m2crypto-0.16-9.el5

- Group: System Environment/Libraries
- Summary: Support for using OpenSSL in python scripts
- Description: This package allows you to call OpenSSL functions from python 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

man-1.6d-2.el5 - man-1.6d-3.el5

- Group: System Environment/Base
- Summary: A set of documentation tools: man, apropos and whatis.
- Description: The man package includes three tools for finding information and/or documentation

about your Linux system: man, apropos, and whatis. The man system formats and displays on-line manual pages about commands or functions on your system. Apropos searches the whatis database (containing short descriptions of system commands) for a string. Whatis searches its own database for a complete word. The man package should be installed on your system because it is the primary way to find documentation on a Linux 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

man-pages-overrides-5.8.3-2.el5 - man-pages-overrides-5.9.2-2.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

mdadm-2.6.9-3.el5 - mdadm-2.6.9-5.el5

- Group: System Environment/Base
- Summary: mdadm controls Linux md devices (software RAID arrays)
- Description: mdadm is used to create, manage, and monitor Linux MD (software RAID) devices. As such, it provides similar functionality to the raidtools package. However, mdadm is a single program, and it can perform almost all functions without a configuration file, though a configuration file can be used to help with some common tasks.
- 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-1.17-1.56.el5 - microcode_ctl-1.17-3.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-5.1.19.6-75.el5 - mkinitrd-5.1.19.6-79.el5

- 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

mod_auth_kerb-5.1-3.el5_7.1 - mod_auth_kerb-5.1-5.el5

- Group: System Environment/Daemons
- Summary: Kerberos authentication module for HTTP
- Description: mod_auth_kerb is module for the Apache HTTP Server designed to provide Kerberos authentication over HTTP. The module supports the Negotiate authentication method, which performs full Kerberos authentication based on ticket exchanges.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mod_nss-1.0.8-4.el5_6.1 - mod_nss-1.0.8-7.el5

- Group: System Environment/Daemons
- Summary: SSL/TLS module for the Apache HTTP server
- Description: The mod_nss module provides strong cryptography for the Apache Web server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols using the Network Security Services (NSS) security 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

mod_python-3.2.8-3.1 - mod_python-3.2.8-4.el5

- Group: System Environment/Daemons
- Summary: An embedded Python interpreter for the Apache Web server.

- Description: Mod_python is a module that embeds the Python language interpreter within the server, allowing Apache handlers to be written in Python. Mod_python brings together the versatility of Python and the power of the Apache Web server for a considerable boost in flexibility and performance over the traditional CGI approach.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mozldap-6.0.5-1.el5 - mozldap-6.0.5-2.el5

- Group: System Environment/Libraries
- Summary: Mozilla LDAP C SDK
- Description: The Mozilla LDAP C SDK is a set of libraries that allow applications to communicate with LDAP directory servers. These libraries are derived from the University of Michigan and Netscape LDAP libraries. They use Mozilla NSPR and NSS for crypto.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mpitests-3.2-1.el5 - mpitests-3.2-2.el5

- Group: Applications
- Summary: MPI Benchmarks and tests
- Description: Set of popular MPI benchmarks: IMB-2.3 Presta-1.4.0 OSU benchmarks ver 2.2
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mstflint-1.4-1.el5 - mstflint-1.4-2.el5

- Group: Applications/System
- Summary: Mellanox firmware burning tool
- Description: This package contains a burning tool for Mellanox manufactured HCA cards. It also provides access to the relevant source code.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mt-st-0.9b-2.2.2 - mt-st-0.9b-4.el5

- Group: Applications/System
- Summary: Install mt-st if you need a tool to control tape drives.
- Description: The mt-st package contains the mt and st tape drive management programs. Mt (for magnetic tape drives) and st (for SCSI tape devices) can control rewinding, ejecting, skipping files and blocks and more. Install mt-st if you need a tool to manage tape drives.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mutt-1.4.2.2-3.0.2.el5 - mutt-1.4.2.2-6.el5

- Group: Applications/Internet
- Summary: A text mode mail user agent.
- Description: Mutt is a text-mode mail user agent. Mutt supports color, threading, arbitrary key remapping, and a lot of customization. You should install mutt if you have used it in the past and you prefer it, or if you are new to mail programs and have not decided which one you are going to use.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mvapich-1.2.0-0.3562.1.el5 - mvapich-1.2.0-0.3562.2.el5

- Group: Development/Libraries
- Summary: MPI implementation over Infiniband RDMA-enabled interconnect
- Description: This is high performance and scalable MPI-1 implementation over Infiniband and RDMA-enabled interconnects. This implementation is based on MPICH and MVICH. MVAPICH is pronounced as `em-vah-pich''.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

mvapich2-1.4-1.el5 - mvapich2-1.4-2.el5

- Group: Development/Libraries
- Summary: OSU MVAPICH2 MPI package
- Description: This is an MPI-2 implementation which includes all MPI-1 features. It is based on MPICH2 and MVICH.
- 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-5.0.77-4.el5_6.6 - mysql-5.0.95-3.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 MySQL client programs, the client shared libraries, and generic MySQL files.
- No added dependencies
- Removed Dependencies:
  - gperf
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

net-snmp-5.3.2.2-17.el5 - net-snmp-5.3.2.2-20.el5

- Group: System Environment/Daemons
- Summary: A collection of SNMP protocol tools and libraries.
- Description: SNMP (Simple Network Management Protocol) is a protocol used for network management. The NET-SNMP project includes various SNMP tools: an extensible agent, an SNMP library, tools for requesting or setting information from SNMP agents, tools for generating and handling SNMP traps, a version of the netstat command which uses SNMP, and a Tk/Perl mib browser. This package contains the snmpd and snmptrapd daemons, documentation, etc. You will probably also want to install the net-snmp-utils package, which contains NET-SNMP utilities. Building option: --without tcp_wrappers : disable tcp_wrappers support
- 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-1.0.9-60.el5 - nfs-utils-1.0.9-66.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-4.8.8-2.el5 - nspr-4.9.1-6.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-3.12.10-8.el5 - nss-3.13.5-8.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:
  - nspr-devel >= 4.9.1
- Removed Dependencies:
  - nspr-devel >= 4.8.8
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

nss_ldap-253-49.el5 - nss_ldap-253-51.el5

- 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

openais-0.80.6-36.el5 - openais-0.80.6-37.el5

- Group: System Environment/Base
- Summary: The openais Standards-Based Cluster Framework executive and APIs
- Description: This package contains the openais executive, openais service handlers, default configuration files and init script.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openib-1.4.1-6.el5 - openib-1.5.4.1-4.el5

- Group: System Environment/Base
- Summary: OpenIB Infiniband Driver Stack
- Description: User space initialization scripts for the kernel InfiniBand drivers
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openldap-2.3.43-25.el5 - openldap-2.3.43-25.el5_8.1

- Group: System Environment/Daemons
- Summary: The configuration files, libraries, and documentation for OpenLDAP.
- Description: OpenLDAP is an open source suite of LDAP (Lightweight Directory Access Protocol) applications and development tools. LDAP is a set of protocols for accessing directory services (usually phone book style information, but other information is possible) over the Internet, similar to the way DNS (Domain Name System) information is propagated over the

Internet. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.

- 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.el5 - openmotif-2.3.1-6.1.el5_8

- 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

openmpi-1.4-4.el5 - openmpi-1.4-7.el5

- Group: Development/Libraries
- Summary: Open Message Passing Interface
- Description: Open MPI is an open source, freely available implementation of both the MPI-1 and MPI-2 standards, combining technologies and resources from several other projects (FT-MPI, LA-MPI, LAM/MPI, and PACX-MPI) in order to build the best MPI library available. A completely new MPI-2 compliant implementation, Open MPI offers advantages for system and software vendors, application developers, and computer science researchers. For more information, see http://www.open-mpi.org/ .
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openoffice.org-3.1.1-19.5.el5_5.6 - openoffice.org-3.1.1-19.10.el5_8.4

- Group: Applications/Productivity
- Summary: OpenOffice.org comprehensive office suite.
- Description: OpenOffice.org is an Open Source, community-developed, multi-platform office productivity suite. It includes the key desktop applications, such as a word processor, spreadsheet, presentation manager, formula editor and drawing program, with a user interface and feature set similar to other office suites. Sophisticated and flexible, OpenOffice.org also works transparently with a variety of file formats, including Microsoft Office. Usage: Simply type "ooffice" to run OpenOffice.org or select the requested component (Writer, Calc, Impress, etc.) from your desktop menu. On first start a few files will be installed in the user's home, 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

opensm-3.3.3-2.el5 - opensm-3.3.13-1.el5

- Group: System Environment/Daemons
- Summary: OpenIB InfiniBand Subnet Manager and management utilities
- Description: OpenSM is the OpenIB project's Subnet Manager for Infiniband networks. The subnet manager is run as a system daemon on one of the machines in the infiniband fabric to manage the fabric's routing state. This package also contains various tools for diagnosing and testing Infiniband networks that can be used from any machine and do not need to be run on a machine running the opensm daemon.
- Added Dependencies:
  - libibmad-devel = 1.3.8
- Removed Dependencies:
  - libibmad-devel = 1.3.3

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

openssl-0.9.8e-22.el5 - openssl-0.9.8e-22.el5_8.4

- 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

openssl097a-0.9.7a-9.el5_4.2 - openssl097a-0.9.7a-11.el5_8.2

- 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-2.6.32-3.el5 - openswan-2.6.32-4.el5

- 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

pam-0.99.6.2-6.el5_5.2 - pam-0.99.6.2-12.el5

- Group: System Environment/Base
- Summary: A security tool which provides authentication for applications
- Description: PAM (Pluggable Authentication Modules) is a system security tool that allows system administrators to set authentication policy without having to recompile programs that handle authentication.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

parted-1.8.1-29.el5 - parted-1.8.1-30.el5

- Group: Applications/System

- Summary: The GNU disk partition manipulation program
- Description: The GNU Parted program allows you to create, destroy, resize, move, and copy hard disk partitions. Parted can be used for creating space for new operating systems, reorganizing disk usage, and copying data to new hard disks.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pdksh-5.2.14-37.el5 - pdksh-5.2.14-37.el5_8.1

- Group: System Environment/Shells
- Summary: A public domain shell implementing ksh-88
- Description: The pdksh package contains public domain implementation of ksh-88. The ksh shell is a command interpreter intended for both interactive and shell script use. Ksh's command language is a superset of the sh shell language. Pdksh is unmaintained since 1998 and is obsoleted by ksh package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

perftest-1.2.3-1.el5 - perftest-1.3.0-1.el5

- Group: Productivity/Networking/Diagnostic
- Summary: IB Performance Tests
- Description: Perftest is a collection of simple test programs designed to utilize RDMA communications and provide performance numbers over those RDMA connections. It does not work on normal TCP/IP networks, only on RDMA networks.
- Added Dependencies:
  - libibumad-devel > 1.3.6

    - libibverbs-devel > 1.1.4
    - librdmacm-devel > 1.0.14
  - Removed Dependencies:
    - libibverbs-devel >= 1.1.3
    - librdmacm-devel >= 1.0.10
  - No added provides
  - No removed provides
  - No added conflicts
  - No removed conflicts
  - No added obsoletes
  - No removed obsoletes

perl-5.8.8-38.el5 - perl-5.8.8-38.el5_8

  - 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-DBD-Pg-1.49-2.el5_3.1 - perl-DBD-Pg-1.49-4.el5_8

  - Group: Development/Libraries
  - Summary: A PostgreSQL interface for perl
  - Description: An implementation of DBI for PostgreSQL for 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

perl-LDAP-0.33-3.fc6 - perl-LDAP-0.33-4.el5_8

- Group: Development/Libraries
- Summary: LDAP Perl module
- Description: Net::LDAP is a collection of modules that implements a LDAP services API for Perl programs. The module may be used to search directories or perform maintenance functions such as adding, deleting or modifying entries.
- 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-XML-SAX-0.14-11 - perl-XML-SAX-0.14-13.el5

- Group: Development/Libraries
- Summary: XML-SAX Perl module
- Description: XML-SAX Perl module.
- 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-5.1.6-32.el5 - php-5.1.6-39.el5_8

- 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

php53-5.3.3-5.el5 - php53-5.3.3-13.el5_8

- 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-2.6.6-5.el5_7.4 - pidgin-2.6.6-11.el5.4

- 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
- Removed Dependencies:
  - krb5-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

pirut-1.3.28-19.el5 - pirut-1.3.28-20.el5

- Group: Applications/System
- Summary: Package Installation, Removal and Update Tools
- Description: pirut (pronounced "pirate") provides a set of graphical tools for managing 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

pm-utils-0.99.3-10.el5 - pm-utils-0.99.3-14.el5

- Group: System Environment/Base
- Summary: Power management utilities and scripts
- Description: The pm-utils package contains utilities and scripts useful for tasks related to power management.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

postfix-2.3.3-2.3.el5_6 - postfix-2.3.3-6.el5

- Group: System Environment/Daemons
- Summary: Postfix Mail Transport Agent
- Description: Postfix is a Mail Transport Agent (MTA), supporting LDAP, SMTP AUTH (SASL), TLS
- Added Dependencies:
  - mysql
  - mysql-devel
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

postgresql-8.1.23-1.el5_7.3 - postgresql-8.1.23-6.el5_8

- Group: Applications/Databases
- Summary: PostgreSQL client programs and libraries.
- Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for the whole package, as well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

postgresql84-8.4.9-1.el5_7.1 - postgresql84-8.4.13-1.el5_8

- Group: Applications/Databases
- Summary: PostgreSQL client programs
- Description: PostgreSQL is an advanced Object-Relational database management system (DBMS) that supports almost all SQL constructs (including transactions, subselects and user-defined types and functions). The postgresql package includes the client programs and libraries that you'll need to access a PostgreSQL DBMS server. These PostgreSQL client programs are programs that directly manipulate the internal structure of PostgreSQL databases on a PostgreSQL server. These client programs can be located on the same machine with the PostgreSQL server, or may be on a remote machine which accesses a PostgreSQL server over a network connection. This package contains the docs in HTML for the whole package, as well as command-line utilities for managing PostgreSQL databases on a PostgreSQL server. If you want to manipulate a PostgreSQL database on a local or remote PostgreSQL server, you need this package. You also need to install this package if you're installing the postgresql-server package.
- 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-3.2.7-18.el5 - procps-3.2.7-22.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

psmisc-22.2-7.el5_6.2 - psmisc-22.2-11

- Group: Applications/System
- Summary: Utilities for managing processes on your system.
- Description: The psmisc package contains utilities for managing processes on your system: pstree, killall and fuser. The pstree command displays a tree structure of all of the running processes on your system. The killall command sends a specified signal (SIGTERM if nothing is specified) to processes identified by name. The fuser command identifies the PIDs of processes that are using specified files or 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

python-2.4.3-46.el5 - python-2.4.3-56.el5

- Group: Development/Languages
- Summary: An interpreted, interactive, object-oriented programming language.
- Description: Python is an interpreted, interactive, object-oriented programming language often compared to Tcl, Perl, Scheme or Java. Python includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system

calls and libraries, as well as to various windowing systems (X11, Motif, Tk, Mac and MFC). Programmers can write new built-in modules for Python in C or C++. Python can be used as an extension language for applications that need a programmable interface. This package contains most of the standard Python modules, as well as modules for interfacing to the Tix widget set for Tk and RPM. Note that documentation for Python is provided in the python-docs package.

- Added Dependencies:
  - expat-devel >= 1.95.8-11
- Removed Dependencies:
  - expat-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

python-iniparse-0.2.3-4.el5 - python-iniparse-0.2.3-6.el5

- Group: Development/Libraries
- Summary: Python Module for Accessing and Modifying Configuration Data in INI files
- Description: iniparse is an INI parser for Python which is API compatible with the standard library's ConfigParser, preserves structure of INI files (order of sections & options, indentation, comments, and blank lines are preserved when data is updated), and is more convenient to use.
- 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-0.98.9-1.el5 - python-rhsm-1.0.10-1.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.

- Added Dependencies:
  - openssl-devel
- Removed Dependencies:
  - rpm-python
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

qlvnictools-0.0.1-12.el5 - qlvnictools-0.0.1-13.el5

- Group: System Environment/Base
- Summary: VNIC ULP service
- Description: VNIC ULP service
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

qperf-0.4.6-1.el5 - qperf-0.4.6-3.el5

- Group: Networking/Diagnostic
- Summary: Measure socket and RDMA performance
- Description: Measure socket and RDMA performance.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

qt-3.3.6-25.el5 - qt-3.3.6-26.el5

- Group: System Environment/Libraries
- Summary: The shared library for the Qt GUI toolkit.
- Description: Qt is a GUI software toolkit which simplifies the task of writing and maintaining GUI (Graphical User Interface) applications for the X Window System. Qt is written in C++ and is fully object-oriented. This package contains the shared library needed to run qt applications, as well as the README files for qt.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

quagga-0.98.6-5.el5_5.2 - quagga-0.98.6-11.el5

- Group: System Environment/Daemons
- Summary: Routing daemon
- Description: Quagga is a free software that manages TCP/IP based routing protocol. It takes multi-server and multi-thread approach to resolve the current complexity of the Internet. Quagga supports BGP4, BGP4+, OSPFv2, OSPFv3, RIPv1, RIPv2, and RIPng. Quagga is intended to be used as a Route Server and a Route Reflector. It is not a toolkit, it provides full routing power under a new architecture. Quagga by design has a process for each protocol. Quagga is a fork of GNU Zebra.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

quota-3.13-5.el5 - quota-3.13-8.el5

- Group: System Environment/Base

- Group: System Environment/Base
- Summary: System administration tools for monitoring users' disk usage.
- Description: The quota package contains system administration tools for monitoring and limiting user and or group disk usage per filesystem.
- Added Dependencies:
  - autoconf
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rds-tools-1.5-1.el5 - rds-tools-2.0.6-1.el5

- Group: Applications/System
- Summary: RDS support tools
- Description: Various tools for support of the RDS (Reliable Datagram Socket) API. RDS is specific to InfiniBand and iWARP networks and does not work on non-RDMA hardware.
- 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-5.8.0.3 - redhat-release-5Client-5.9.0.2

- 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-43 - redhat-release-notes-5Client-46

- 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-0.4.20-77.el5 - rhn-client-tools-0.4.20-86.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

rhnsd-4.7.0-10.el5 - rhnsd-4.7.0-14.el5

- Group: System Environment/Base

- Summary: Red Hat Network query daemon
- Description: The Red Hat Update Agent that automatically queries the Red Hat Network servers and determines which packages need to be updated on your machine, and runs any actions.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

rp-pppoe-3.5-32.1 - rp-pppoe-3.5-33.el5

- Group: System Environment/Daemons
- Summary: A PPP over Ethernet client (for xDSL support).
- Description: PPPoE (Point-to-Point Protocol over Ethernet) is a protocol used by many ADSL Internet Service Providers. This package contains the Roaring Penguin PPPoE client, a user-mode program that does not require any kernel modifications. It is fully compliant with RFC 2516, the official PPPoE specification.
- 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-4.4.2.3-27.el5 - rpm-4.4.2.3-31.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-1.8.5-24.el5 - ruby-1.8.5-27.el5

- 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

samba-3.0.33-3.37.el5 - samba-3.0.33-3.39.el5_8

- Group: System Environment/Daemons
- Summary: The Samba SMB server.
- 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 server that can be used to provide network services to SMB (sometimes called "Lan Manager") clients. Samba uses NetBIOS over TCP/IP (NetBT) protocols and does NOT need the NetBEUI (Microsoft Raw NetBIOS frame) protocol.
- 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-3.5.10-0.107.el5 - samba3x-3.6.6-0.129.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:
  - automake
  - libtdb-devel >= 1.2.6
- Removed Dependencies:
  - libtdb-devel >= 1.2.1
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

scim-bridge-0.4.5-10.el5 - scim-bridge-0.4.5-11.el5

- Group: System Environment/Libraries
- Summary: SCIM Bridge Gtk IM module
- Description: SCIM Bridge is a C implementation of a Gtk IM module for SCIM.
- 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-2.4.6-327.el5 - selinux-policy-2.4.6-338.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

setroubleshoot-2.0.5-5.el5 - setroubleshoot-2.0.5-5.el5_8.1

- Group: Applications/System
- Summary: Helps troubleshoot SELinux problems
- Description: setroubleshoot gui. Application that allows you to view setroubleshoot-server messages. Provides tools to help diagnose SELinux problems. When AVC messages are generated an alert can be generated that will give information about the problem and help track its resolution. Alerts can be configured to user preference. The same tools can be run on existing log 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

shadow-utils-4.0.17-20.el5 - shadow-utils-4.0.17-21.el5

- Group: System Environment/Base
- Summary: Utilities for managing accounts and shadow password files.
- Description: The shadow-utils package includes the necessary programs for converting UNIX

password files to the shadow password format, plus programs for managing user and group accounts. The pwconv command converts passwords to the shadow password format. The pwunconv command unconverts shadow passwords and generates an npasswd file (a standard UNIX password file). The pwck command checks the integrity of password and shadow files. The lastlog command prints out the last login times for all users. The useradd, userdel, and usermod commands are used for managing user accounts. The groupadd, groupdel, and groupmod commands are used for managing group accounts.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

smartmontools-5.38-3.el5 - smartmontools-5.42-2.el5

- Group: System Environment/Base
- Summary: Tools for monitoring SMART capable hard disks
- Description: The smartmontools package contains two utility programs (smartctl and smartd) to control and monitor storage systems using the Self- Monitoring, Analysis and Reporting Technology System (SMART) built into most modern ATA and SCSI hard disks. In many cases, these utilities will provide advanced warning of disk degradation and failure.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

specspo-13-1.el5 - specspo-13-4.el5

- Group: Documentation
- Summary: Package descriptions, summaries, and groups.
- Description: The specspo package contains the portable object catalogues used to internationalize packages.
- No added dependencies

- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

spice-client-0.8.1-6.el5 - spice-client-0.8.1-8.el5

- Group: User Interface/Desktops
- Summary: Implements the client side of the SPICE protocol
- Description: The Simple Protocol for Independent Computing Environments (SPICE) is a remote display system built for virtual environments which allows you to view a computing 'desktop' environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. This package contains the SPICE client application.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

spice-xpi-2.4-4.el5 - spice-xpi-2.4-6.el5

- Group: Applications/Internet
- Summary: SPICE extension for Mozilla
- Description: SPICE extension for mozilla allows the client to be used from a web browser.
- 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-3.3.6-5 - sqlite-3.3.6-6

- 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

squirrelmail-1.4.8-5.el5_4.10 - squirrelmail-1.4.8-21.el5

- Group: Applications/Internet
- Summary: SquirrelMail webmail client
- Description: SquirrelMail is a standards-based webmail package written in PHP4. It includes built-in pure PHP support for the IMAP and SMTP protocols, and all pages render in pure HTML 4.0 (with no Javascript) for maximum compatibility across browsers. It has very few requirements and is very easy to configure and install. SquirrelMail has all the functionality you would want from an email client, including strong MIME support, address books, and folder manipulation.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

srptools-0.0.4-8.el5 - srptools-0.0.4-10.el5

- Group: System Environment/Base
- Summary: Tools for using the InfiniBand SRP protocol devices
- Description: In conjunction with the kernel ib_srp driver, srptools allows you to discover and use SCSI devices via the SCSI RDMA Protocol over InfiniBand.
- Added Dependencies:
  - libibverbs-devel > 1.1.3
- Removed Dependencies:
  - libibverbs-devel >= 1.1.2-4
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

sssd-1.5.1-49.el5 - sssd-1.5.1-58.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.
- Added Dependencies:
  - dbus-devel >= 1.1.2
  - libtdb-devel >= 1.2.10
- Removed Dependencies:
  - dbus-devel
  - libtdb-devel
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

strace-4.5.18-5.el5_5.5 - strace-4.5.18-18.el5

- Group: Development/Debuggers
- Summary: Tracks and displays system calls associated with a running process
- Description: The strace program intercepts and records the system calls called and received by a running process. Strace can print a record of each system call, its arguments and its return value. Strace is useful for diagnosing problems and debugging, as well as for instructional purposes. Install strace if you need a tool to track the system calls made and received by a process.
- 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-0.98.14-1.el5 - subscription-manager-1.0.24-1.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.
- Added Dependencies:
  - GConf2-devel
- 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-1.11-1.el5 - subscription-manager-migration-data-1.11.2.7-1.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-1.6.11-7.el5_6.4 - subversion-1.6.11-10.el5_8

- 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-1.7.2p1-13.el5 - sudo-1.7.2p1-22.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

symlinks-1.2-24.2.2 - symlinks-1.2-26.el5

- Group: Applications/System
- Summary: A utility which maintains a system's symbolic links.
- Description: The symlinks utility performs maintenance on symbolic links. Symlinks checks for symlink problems, including dangling symlinks which point to nonexistent files. Symlinks can also automatically convert absolute symlinks to relative symlinks. Install the symlinks package if you need a program for maintaining symlinks on your 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

syslinux-3.11-7 - syslinux-4.02-7.2.el5

- Group: Applications/System
- Summary: Simple kernel loader which boots from a FAT filesystem
- Description: SYSLINUX is a suite of bootloaders, currently supporting DOS FAT filesystems, Linux ext2/ext3 filesystems (EXTLINUX), PXE network boots (PXELINUX), or ISO 9660 CD-ROMs (ISOLINUX). It also includes a tool, MEMDISK, which loads legacy operating systems from these media.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts

- No removed conflicts
- No added obsoletes
- No removed obsoletes

sysstat-7.0.2-11.el5 - sysstat-7.0.2-12.el5

- Group: Applications/System
- Summary: The sar and iostat system monitoring commands.
- Description: This package provides the sar and iostat commands for Linux. Sar and iostat enable system monitoring of disk, network, and other IO activity.
- 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-bind-4.0.3-5.el5 - system-config-bind-4.0.3-6.el5

- Group: Applications/System
- Summary: The Red Hat BIND DNS Configuration Tool.
- Description: The system-config-bind package provides a graphical user interface (GUI) to configure the Berkeley Internet Name Domain (BIND) Domain Name System (DNS) server, "named", with a set of python modules. Users new to BIND configuration can use this tool to quickly set up a working DNS 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

system-config-lvm-1.1.5-9.el5 - system-config-lvm-1.1.5-13.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

system-config-netboot-0.1.45.1-3.el5 - system-config-netboot-0.1.45.1-5.el5

- Group: Applications/System
- Summary: network booting/install configuration utility (GUI)
- Description: system-config-netboot is a utility which allows you to configure diskless environments and network installations.
- 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-printer-0.7.32.10-1.el5_7.1 - system-config-printer-0.7.32.10-3.el5

- Group: System Environment/Base
- Summary: A printer administration tool
- Description: system-config-printer is a graphical user interface that allows the user to configure a CUPS print 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

systemtap-1.6-6.el5 - systemtap-1.8-6.el5

- Group: Development/System
- Summary: Programmable system-wide instrumentation system
- Description: SystemTap is an instrumentation system for systems running Linux. Developers can write instrumentation scripts to collect data on the operation of the system. The base systemtap package contains/requires the components needed to locally develop and execute systemtap scripts.
- Added Dependencies:
  - gcc-c++
- Removed Dependencies:
  - gettext
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tar-1.15.1-31.el5 - tar-1.15.1-32.el5_8

- Group: Applications/Archiving
- Summary: A GNU file archiving program
- Description: The GNU tar program saves many files together in one archive and can restore individual files (or all of the files) from that archive. Tar can also be used to add supplemental files to an archive and to update or list files in the archive. Tar includes multivolume support, automatic archive compression/decompression, the ability to perform remote archives, and the ability to perform incremental and full backups. If you want to use tar for remote backups, you also need to install the rmt package.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

tcl-8.4.13-4.el5 - tcl-8.4.13-6.el5

- Group: Development/Languages
- Summary: Tcl scripting language development environment
- Description: The Tcl (Tool Command Language) provides a powerful platform for creating integration applications that tie together diverse applications, protocols, devices, and frameworks. When paired with the Tk toolkit, Tcl provides a fastest and powerful way to create cross-platform GUI applications. Tcl can also be used for a variety of web-related tasks and for creating powerful command languages for applications.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tcsh617-6.17-5.el5 - tcsh617-6.17-7.el5

- Group: System Environment/Shells
- Summary: An enhanced version of csh, the C shell
- Description: Tcsh is an enhanced but completely compatible version of csh, the C shell. Tcsh is a command language interpreter which can be used both as an interactive login shell and as a shell script command processor. Tcsh includes a command line editor, programmable word completion, spelling correction, a history mechanism, job control and a C language like syntax.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

telnet-0.17-39.el5 - telnet-0.17-41.el5

- Group: Applications/Internet

- Summary: The client program for the telnet remote login protocol.
- Description: Telnet is a popular protocol for logging into remote systems over the Internet. The telnet package provides a command line telnet client.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tetex-3.0-33.13.el5 - tetex-3.0-33.15.el5_8.1

- Group: Applications/Publishing
- Summary: The TeX text formatting system.
- Description: TeTeX is an implementation of TeX for Linux or UNIX systems. TeX takes a text file and a set of formatting commands as input and creates a typesetter-independent .dvi (DeVice Independent) file as output. Usually, TeX is used in conjunction with a higher level formatting package like LaTeX or PlainTeX, since TeX by itself is not very user-friendly. The output format needn't to be DVI, but also PDF, when using pdflatex or similar tools. Install tetex if you want to use the TeX text formatting system. Consider to install tetex-latex (a higher level formatting package which provides an easier-to-use interface for TeX). Unless you are an expert at using TeX, you should also install the tetex-doc package, which includes the documentation for TeX.
- 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-2.0.0.24-28.el5_7 - thunderbird-10.0.11-1.el5_8

- Group: Applications/Internet
- Summary: Mozilla Thunderbird mail/newsgroup client
- Description: Mozilla Thunderbird is a standalone mail and newsgroup client.
- Added Dependencies:

- alsa-lib-devel
- autoconf213
- bzip2-devel
- freetype-devel >= 2.1.9
- gnome-vfs2-devel
- krb5-devel
- libgnome-devel
- libgnomeui-devel
- libnotify-devel
- mesa-libGL-devel
- nspr-devel >= 4.8.9
- nss-devel >= 3.13.1
- pango-devel
- startup-notification-devel

- Removed Dependencies:
  - cairo-devel >= 1.0
  - expat-devel
  - freetype-devel
  - gzip
  - nspr-devel >= 4.6
  - nss-devel >= 3.10
  - tcsh
  - unzip
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

tomcat5-5.5.23-0jpp.22.el5_7 - tomcat5-5.5.23-0jpp.37.el5

- 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-2011l-4.el5 - tzdata-2012i-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

udev-095-14.27.el5_7.1 - udev-095-14.29.el5

- Group: System Environment/Base
- Summary: A userspace implementation of devfs
- Description: The udev package contains an implementation of devfs in userspace using sysfs and netlink.
- No added dependencies
- No removed dependencies

- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

util-linux-2.13-0.59.el5 - util-linux-2.13-0.59.el5_8

- Group: System Environment/Base
- Summary: A collection of basic system utilities.
- Description: The util-linux package contains a large variety of low-level system utilities that are necessary for a Linux system to function. Among others, Util-linux contains the fdisk configuration tool and the login 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

vim-7.0.109-7.el5 - vim-7.0.109-7.2.el5

- Group: Applications/Editors
- Summary: The VIM editor.
- Description: VIM (VIsual editor iMproved) is an updated and improved version of the vi editor. Vi was the first real screen-based editor for UNIX, and is still very popular. VIM improves on vi by adding new features: multiple windows, multi-level undo, block highlighting 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

virt-who-0.5-5.el5 - virt-who-0.7-9.el5

- Group: System Environment/Base
- Summary: Agent for reporting virtual guest IDs to subscription-manager
- Description: Agent that collects information about virtual guests present in the system and report them to the subscription 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

vsftpd-2.0.5-24.el5 - vsftpd-2.0.5-28.el5

- Group: System Environment/Daemons
- Summary: vsftpd - Very Secure Ftp Daemon
- Description: vsftpd is a Very Secure FTP daemon. It was written completely from scratch.
- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

wget-1.11.4-2.el5_4.1 - wget-1.11.4-3.el5_8.2

- Group: Applications/Internet
- Summary: A utility for retrieving files using the HTTP or FTP protocols.
- Description: GNU Wget is a file retrieval utility which can use either the HTTP or FTP protocols. Wget features include the ability to work in the background while you are logged out, recursive retrieval of directories, file name wildcard matching, remote file timestamp storage and comparison, use of Rest with FTP servers and Range with HTTP servers to retrieve files over slow or unstable connections, support for Proxy servers, and configurability.

- No added dependencies
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

wireshark-1.0.15-1.el5_6.4 - wireshark-1.0.15-5.el5

- Group: Applications/Internet
- Summary: Network traffic analyzer
- Description: Wireshark is a network traffic analyzer for Unix-ish operating systems. This package lays base for libpcap, a packet capture and filtering library, contains command-line utilities, contains plugins and documentation for wireshark. A graphical user interface is packaged separately to GTK+ package.
- 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-3.0.3-135.el5 - xen-3.0.3-142.el5

- 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-2.3.14-16.el5 - xinetd-2.3.14-17.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-server-1.1.1-48.90.el5 - xorg-x11-server-1.1.1-48.100.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-1.9.2.26-1.el5_7 - xulrunner-10.0.11-1.el5_8

- 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:
  - libpng-devel
  - mesa-libGL-devel
  - nspr-devel >= 4.8.9
  - nss-devel >= 3.13.1
- Removed Dependencies:
  - nspr-devel >= 4.8
  - nss-devel >= 3.12.8
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

yelp-2.16.0-26.el5 - yelp-2.16.0-29.el5

- 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 >= 10.0
- Removed Dependencies:
  - gecko-devel-unstable >= 1.9.2
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts

- No added obsoletes
- No removed obsoletes

ypserv-2.19-9.el5 - ypserv-2.19-9.el5_8.1

- 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-3.2.22-39.el5 - yum-3.2.22-40.el5

- Group: System Environment/Base
- Summary: RPM installer/updater
- Description: Yum is a utility that can check for and automatically download and install updated RPM packages. Dependencies are obtained and downloaded automatically prompting the user as 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

yum-metadata-parser-1.1.2-3.el5 - yum-metadata-parser-1.1.2-4.el5

- Group: Development/Libraries
- Summary: A fast metadata parser for yum
- Description: Fast metadata parser for yum implemented in C.
- 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-0.5.4-26.el5 - yum-rhn-plugin-0.5.4-29.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

yum-updatesd-0.9-2.el5 - yum-updatesd-0.9-5.el5

- Group: System Environment/Base
- Summary: Update notification daemon
- Description: yum-updatesd provides a daemon which checks for available updates and can notify you when they are available via email, syslog or dbus.
- No added dependencies
- No removed dependencies
- No added provides

- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

zlib-1.2.3-4.el5 - zlib-1.2.3-7.el5

- Group: System Environment/Libraries
- Summary: The zlib compression and decompression library.
- Description: Zlib is a general-purpose, patent-free, lossless data compression library which is used by many different programs.
- Added Dependencies:
  - autoconf
  - automake
  - libtool
- No removed dependencies
- No added provides
- No removed provides
- No added conflicts
- No removed conflicts
- No added obsoletes
- No removed obsoletes

zsh-4.2.6-6.el5 - zsh-4.2.6-8.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 1-2.7.400	**2013-10-31**	**Rüdiger Landmann**

Rebuild with publican 4.0.0

Revision 1-2.7	**Tue Aug 27 2013**	**Eliška Slobodová**

Republished the book to include a firefox known issue.

Revision 1-2.6	**Wed Aug 21 2013**	**Miroslav Svoboda**

Added a new kernel advisory, RHSA-2013-1166.

Revision 1-2.5	**Mon Apr 22 2013**	**Eliška Slobodová**

Republished the book with a new kernel known issue.

Revision 1-2.1	**Tue Jan 08 2013**	**Eliška Slobodová**

Release of the Red Hat Enterprise Linux 5.9 Technical Notes.