Red Hat Enterprise Linux 5
5.11 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 5.11
Edition 11

Red Hat Customer Content Services

Red Hat Enterprise Linux 5 5.11 Technical Notes

Detailed notes on the changes implemented in Red Hat Enterprise Linux 5.11
Edition 11

Red Hat Customer Content Services

Legal Notice

Abstract

The Red Hat Enterprise Linux 5.11 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 5.10 and minor release Red Hat Enterprise Linux 5.11.

Table of Contents

Preface

The *Red Hat Enterprise Linux 5.11 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 5.10 minor release Red Hat Enterprise Linux 5.11.

For system administrators and others planning Red Hat Enterprise Linux 5.11 upgrades and deployments, the *Red Hat Enterprise Linux 5.11 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 5.11 Technical Notes* provide a single, organized source for change tracking and compliance testing.

For every user, the *Red Hat Enterprise Linux 5.11 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. Errata will be for high-severity security issues.

During the development of a Technology Preview feature, additional components can 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-2.6.18-391*

CDTB

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

Package: *ctdb-1.0.112-2*

Kerberos support for CIFS mounts

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

Package: *samba-client-3.0.33-3.40*

FreeIPMI

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

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

Package: *freeipmi-0.5.1-7*

TrouSerS and tpm-tools

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

- Creation, storage, and use of RSA keys securely (without being exposed in memory)
- Verification of a platform's software state using cryptographic hashes

TrouSerS is an implementation of the Trusted Computing Group's Software Stack (TSS) specification. You can use TrouSerS to write applications that make use of TPM hardware. **`tpm-tools`** is a suite of tools used to manage and utilize TPM hardware.

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

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

eCryptfs

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

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

Package: *ecryptfs-utils-75-8*

Stateless Linux

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

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

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

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

AIGLX

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

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

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

Packages: X Window System group of packages.

FireWire

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

At present, FireWire does not support the following:

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

In addition, the following issues still exist in FireWire:

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

Package: *kernel-2.6.18-391*

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-2.6.18-391*

Software based Fibre Channel over Ethernet (FCoE)

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

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

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

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

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

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

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

Package: *kernel-2.6.18-391*

iSER Support

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

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

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

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

cman fence_virsh fence agent

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

Package: *cman-2.0.115-124*

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-2.5-122*

Chapter 2. Known Issues

2.1. anaconda

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

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

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

  (BZ#846231)

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

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

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

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

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

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

  ```
  linksleep=10
  ```

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

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

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

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

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

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

    ```

    %post
    # Determine the boot device
    device=;

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

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

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

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

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

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

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

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

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

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

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

  (BZ#530465)

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

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

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

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

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

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

  - Define an initiator name:

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

  - Start iscsid:

    ```
    $ iscsid
    ```

  - Discover and login to target:

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

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

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

  - Mount your **/** partition:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The following known issue applies to the PowerPC architecture:

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

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

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

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

The following known issue applies to the Itanium architecture:

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

2.2. autofs

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

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

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

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

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

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

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

  or

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

2.3. cmirror

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

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

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

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

2.4. cpio

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

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

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

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

2.5. 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)

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.

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

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

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

- The **`sar`** and **`sadf`** commands can terminate unexpectedly with a segmentation fault when run on 64-bit PowerPC architecture. (BZ#BZ#984866)

- Hardware support for Intel/QLogix QLE7300 series InfiniBand adapters, which was included in Red Hat Enterprise Linux 5.9, has been removed at Red Hat Enterprise Linux 5.10. Please refer to Red Hat Knowledge Solution 426383 for more information.

- Earlier versions of the Broadcom MFW firmware on bnx2x devices have known bugs. A specific link problem is known to affect BCM57810 based devices with 10GBASE-KR connections. Consequently, depending on the exact timing, the network interface can fail to establish the link. To establish a more reliable link, update the MFW firmware on the bnx2x device's EEPROM (Electrically Erasable Programmable Read-Only Memory) to version 7.4.19 or later. The current version can be checked running **`ethtool -i $NET_DEVICE | grep firmware-version`**. Please consult your hardware vendor or manufacturer for instructions on how to update the MFW firmware on bnx2x devices.

- The Emulex **`lpfc`** driver is missing functionality required to support 16 Gb point-to-point configurations for all adapters in Red Hat Enterprise Linux 5. All other currently available 16 Gb **`lpfc`** configurations are supported on most adapters available. Specifically, the LPe16000B adapter is not supported for any configuration, and the LPe16000A adapter is supported for all configurations besides a point-to-point configuration.

- Red Hat Enterprise Linux 5 can become unresponsive or even terminate due to the lack of ticketed spinlocks in the **`shrink_active_list()`** function.

- When USB hardware uses the ACM interface, there is a race condition that can lead to a system deadlock due to the spinlocks not disabling interrupts. This has been noticed through various types of softlockups. To workaround this problem, reboot the machine.

- If **`kdump`** is configured on an i686 system using a non-PAE kernel and memory larger than 4 GB, it creates an elf core header which includes extra unavailable memory range. This causes **`kdump`** to become unresponsive.

- A large number of kernel log messages may flood **`netconsole`** while under heavy RX traffic, causing the **`netconsole`** kernel module to stop working. To work around this issue, avoid the use of **`netconsole`**, or remove the netconsole module using the **`rmmod netconsole`** command and re-configure it again using the **`insmod netconsole`** command.

- To update firmware on Mellanox cards, use **`mstflint`** which replaces the outdated **`tvflash`** utility.

- The kernel in Red Hat Enterprise Linux 5 does not support Data Center Bridging (DCB). Software-based Fibre Channel over Etherner (FCoE) is a Technology Preview and it is therefore recommended to use Red Hat Enterprise Linux 6 for fully supported software-based FCoE. The following hardware-accelerated FCoE cards are fully supported in Red Hat Enterprise Linux 5: Emulex LPFC, QLogic qla2xxx, Brocade BFA. (BZ#860112)

- The following problems can occur when using Brocade 1010 and 1020 Converged Network Adapters (CNAs):

  - BIOS firmware may not be able to log in the Fibre Channel over Ethernet (FCoE) session when loading a Brocade optional BIOS, which causes the server to be unable to boot and the following error message to appear:

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

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

  Contact Brocade for additional information on these problems.

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

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

  To work around this problem, unload the Brocade BFA driver.

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

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

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

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

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

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

  (BZ#765751)

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

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

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

  ```
  NMI Watchdog detected LOCKUP
  ```

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

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

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

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

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

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

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

  ```
  pci=nosort
  ```

  (BZ#703538)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

  - Downgrade the firmware revision of the 8Gb/s LPe1200x HBA to revision 1.11a5, or
  - Modify the LPFC driver's **`lpfc_enable_npiv`** module parameter to zero.

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

    ```
    options lpfc_enable_npiv=0
    ```

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

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

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

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

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

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

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

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

- A kernel panic may be triggered by the lpfc driver when multiple Emulex OneConnect Universal Converged Network Adapter initiators are included in the same Storage Area Network (SAN) zone. Typically, this kernel panic will present after a cable is pulled or one of the systems is rebooted. To work around this issue, configure the SAN to use single initiator zoning. (BZ#574858)
- If a Huawei USB modem is unplugged from a system, the device may not be detected when it is attached again. To work around this issue, the usbserial and usb-storage driver modules need to be reloaded, allowing the system to detect the device. Alternatively, the if the system is rebooted, the modem will be detected also. (BZ#517454)
- Memory on-line is not currently supported with the Boxboro-EX platform. (BZ#515299)
- Unloading a PF (SR-IOV Physical function) driver from a host when a guest is using a VF (virtual function) from that device can cause a host crash. A PF driver for an SR-IOV device should not be unloaded until after all guest virtual machines with assigned VFs from that SR-IOV device have terminated. (BZ#514360)
- Data corruption on NFS file systems might be encountered on network adapters without support for error-correcting code (ECC) memory that also have TCP segmentation offloading (TSO) enabled in the driver. Note: data that might be corrupted by the sender still passes the checksum performed by the IP stack of the receiving machine A possible work around to this issue is to disable TSO on network adapters that do not support ECC memory. (BZ#504811)
- After installation, a System z machine with a large number of memory and CPUs (e.g. 16 CPU's and 200GB of memory) might may fail to IPL. To work around this issue, change the line

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

  to

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

  The command **zipl -V** should now show **0x02000000** as the starting address for the initial RAM disk (initrd). Stop the logical partition (LPAR), and then manually increase the storage size of the LPAR.
- On certain hardware configurations the kernel may panic when the Broadcom iSCSI offload driver (**bnx2i.ko** and **cnic.ko**) is loaded. To work around this do not manually load the bnx2i or cnic modules, and temporarily disable the **iscsi** service from starting. To disable the iscsi service, run:

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

  On the first boot of your system, the **iscsi** service may start automatically. To bypass this, during bootup, enter interactive start up and stop the iscsi service from starting.
- In Red Hat Enterprise Linux 5, invoking the kernel system call "setpriority()" with a "which" parameter of type "PRIO_PROCESS" does not set the priority of child threads. (BZ#472251)
- A change to the cciss driver in Red Hat Enterprise Linux 5.4 made it incompatible with the **echo disk < /sys/power/state** suspend-to-disk operation. Consequently, the system will not suspend properly, returning messages such as:

  ```
  Stopping tasks:
  ==================================================================
  ```

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

(BZ#513472)

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

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

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

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

  ```
  options bnx2 disable_msi=1
  ```

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

- The **smartctl** tool cannot properly read SMART parameters from SATA devices. (BZ#429606)

- *IBM T60* laptops will power off completely when suspended and plugged into a docking station. To avoid this, boot the system with the argument **acpi_sleep=s3_bios**. (BZ#439006)

- The *QLogic iSCSI Expansion Card* for the *IBM Bladecenter* provides both ethernet and iSCSI functions. Some parts on the card are shared by both functions. However, the current **qla3xxx** and **qla4xxx** drivers support ethernet and iSCSI functions individually. Both drivers do not support the use of ethernet and iSCSI functions simultaneously.

  Because of this limitation, successive resets (via consecutive **ifdown**/**ifup** commands) may hang the device. To avoid this, allow a 10-second interval after an **ifup** before issuing an **ifdown**. Also, allow the same 10-second interval after an **ifdown** before issuing an **ifup**. This interval allows ample time to stabilize and re-initialize all functions when an **ifup** is issued. (BZ#276891)

- Laptops equipped with the *Cisco Aironet MPI-350* wireless may hang trying to get a DHCP address during any network-based installation using the wired ethernet port.

  To work around this, use local media for your installation. Alternatively, you can disable the wireless card in the laptop BIOS prior to installation (you can re-enable the wireless card after completing the installation). (BZ#213262)

- Hardware testing for the *Mellanox MT25204* has revealed that an internal error occurs under certain high-load conditions. When the **ib_mthca** driver reports a catastrophic error on this hardware, it is usually related to an insufficient completion queue depth relative to the number of outstanding work requests generated by the user application.

Although the driver will reset the hardware and recover from such an event, all existing connections at the time of the error will be lost. This generally results in a segmentation fault in the user application. Further, if **opensm** is running at the time the error occurs, then you need to manually restart it in order to resume proper operation. (BZ#251934)

- The *IBM T41* laptop model does not enter **Suspend Mode** properly; as such, **Suspend Mode** will still consume battery life as normal. This is because Red Hat Enterprise Linux 5 does not yet include the **radeonfb** module.

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

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

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

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

  (BZ#227496)

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

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

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

  (BZ#441329)

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

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

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

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

  (BZ#468967)

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

The following note applies to the PowerPC architecture:

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

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

  To work around this:

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

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

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

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

  (BZ#462663)

2.20. 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. krb5

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

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

2.22. kvm

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

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

- A Microsoft Windows 2008 guest can become unresponsive during boot if huge page memory is enabled on the Red Hat Enterprise Linux 5.9 host. To work around this problem, disable huge page memory on the Red Hat Enterprise Linux 5.9 host. (BZ#845489)
- A CD-ROM device can be assigned to a guest by configuring the guest to back a virtual CD-ROM device with a physical device's special file, for example, /dev/sr0. When a physical CD-ROM device is assigned to a guest, the guest assumes it has full control of the device. However, it is still possible to access the device from the host. In such a case, the guest can become confused about the CD-ROM state; for instance, running eject commands in the host to change media can cause the guest to attempt to read beyond the size of the new medium, resulting in I/O errors. To work around this problem, do not access a CD-ROM device from the host while it is assigned to a guest. (BZ#847259)
- VNC password authentication is disabled when the host system is operating in FIPS mode. QEMU exits if it is configured to run as a password-authenticated VNC server; if QEMU is configured to run as an unauthenticated VNC server, it will continue to run as expected.

- Erroneous boot-index of a guest with mixed virtio/IDE disks causes the guest to boot from the wrong disk after the OS installation and hang with the error message **`boot from HD`**.

- When using PCI device assignment with a 32-bit Microsoft Windows 2008 guest on an AMD-based host system, the assigned device may fail to work properly if it relies on MSI or MSI-X based interrupts. The reason for this is that the 32-bit version of Microsoft Windows 2008 does not enable MSI based interrupts for the family of processor exposed to the guest. To work around this problem, the user may wish to move to a RHEL6 host, use a 64-bit version of the guest operating system, or employ a wrapper script to modify the processor family exposed to the guest as follows (Note that this is only for 32-bit Windows guests):

  - Create the following wrapper script:

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

    ARGS=$@

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

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

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

  - Make the script executable:

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

  - Set proper SELinux permissions:

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

  - Update the guest XML to use the new wrapper:

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

    and replace:

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

    with:

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

(BZ#654208)

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

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

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

  To switch to e1000:

  - Shutdown the guest OS

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

    ```
    virsh edit GUEST
    ```

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

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

  - Save the changes and exit the text editor

  - Restart the guest OS

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

  - Create an XML template from an existing virtual machine:

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

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

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

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

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

  - Create the new virtual machine:

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

- The mute button in the audio control panel on a Windows virtual machine does not mute the sound.

- When migrating KVM guests between hosts, the NX CPU feature setting on both source and destination must match. Migrating a guest between a host with the NX feature disabled (i.e. disabled in the BIOS settings) and a host with the NX feature enabled may cause the guest to crash. (BZ#516029)

- The use of the qcow2 disk image format with KVM is considered a Technology Preview. (BZ#517880)

- 64-bit versions of Windows 7 do not have support for the AC'97 Audio Codec. Consequently, the virtualized sound device Windows 7 kvm guests will not function. (BZ#563122)

- Hot plugging emulated devices after migration may result in the virtual machine crashing after a reboot or the devices no longer being visible. (BZ#507191)

- The KVM modules from the **kmod-kvm** package do not support kernels prior to version 2.6.18-203.el5. If kmod-kvm is updated and an older kernel is kept installed, error messages similar to the following will be returned if attempting to install these modules on older kernels:

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

  (BZ#509361)

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

- The Preboot eXecution Environment (PXE) boot ROMs included with KVM are from the Etherboot project. Consequently, some bug fixes or features that are present on the newer gPXE project are not available on Etherboot. For example, Virtual Machines (VMs) cannot boot using Microsoft based PXE (that is, Remote Installation Services (RIS) or Windows Deployment Services (WDS)).

- The following QEMU / KVM features are currently disabled and not supported: (BZ#512837)

  - smb user directories
  - scsi emulation
  - "isapc" machine type
  - nested KVM guests
  - usb mass storage device emulation
  - usb wacom tablet emulation
  - usb serial emulation
  - usb network emulation

- usb bluetooth emulation
- device emulation for vmware drivers
- sb16 and es1370 sound card emulations
- bluetooth emulation
- qemu CPU models other than qemu32/64 and pentium3
- qemu block device drivers other than raw, qcow2, and host_device

2.23. 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/site/solutions/27421

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

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

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

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

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

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

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

  This message can be safely ignored.

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

2.27. 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 "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 does not support setting of the sha2_truncbug parameter starting with Red Hat Enterprise Linux 5.9, because the kernel does not support it.

2.32. 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 5.10.

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

2.36. 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.
- The *qspice-libs-devel* package delivered through the Virtualization channel of Red Hat Enterprise Linux 5 Client can be installed by the anaconda installer with broken dependencies. As a consequence, upgrading *qspice-libs-devel* fails due to unresolved dependencies. To work around this problem, remove qspice-libs-devel before upgrading on a system with only the Virtualization channel enabled.

2.38. samba3x

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

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

  ```
  Error looking up domain users
  ```

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

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

  Note that several tdb files have been updated and the printing support has been rewritten to use the actual 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.

- The *install-num-migrate-to-rhsm* tool has been removed from the *subscription-manager* package in Red Hat Enterprise Linux 5.11 due to low usage and incompatibilities with the new *subscription-manager-migration-data* packages. (BZ#1092754)

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. 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.

2.44. 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)

2.45. virtio-win

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

- The virtio-win network driver of Red Hat Enterprise Linux 5 can stop working when a Microsoft Windows XP guest is transferred to a Red Hat Enterprise Linux 6 host. To work around this problem, replace the Red Hat Enterprise Linux 5 drivers with the latest Red Hat Enterprise Linux 6 drivers before or after migrating the guest to the new host. (BZ#913094)
- Low performance with UDP messages larger than 1024 is a known Microsoft issue: http://support.microsoft.com/default.aspx/kb/235257. For the message larger than 1024 bytes follow the workaround procedure detailed in the above Microsoft knowledgebase article.
- Installation of Windows XP with the floppy containing guest drivers (in order to get the virtio-net drivers installed as part of the installation), will return messages stating that the viostor.sys file could not be found. viostor.sys is not part of the network drivers, but is on the same floppy as portions of the virtio-blk drivers. These messages can be safely ignored, simply accept the installation's offer to reboot, and the installation will continue normally.

2.46. 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)

2.47. 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)

2.52. yum

Yum is a command-line utility that allows the user to check for updates and automatically download and install updated RPM packages. Yum automatically obtains and downloads dependencies, prompting the user for permission as necessary.

- In Red Hat Enterprise Linux 5.10, users are allowed to install 32-bit and 64-bit packages in parallel. For example, when a 32-bit package is installed on the system and the user runs the **`yum install`** ***`package`*** command, the 64-bit version will be installed in parallel with the 32-bit version.

Chapter 3. Updated Packages

3.1. acroread

3.1.1. RHSA-2013:1402 — Important: Adobe Reader - notification of end of updates

Updated acroread packages that disable the Adobe Reader web browser plug-in are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

Adobe Reader allows users to view and print documents in Portable Document Format (PDF). Adobe Reader 9 reached the end of its support cycle on June 26, 2013, and will not receive any more security updates. Future versions of Adobe Acrobat Reader will not be available with Red Hat Enterprise Linux.

The Adobe Reader packages in the Red Hat Network (RHN) channels will continue to be available. Red Hat will continue to provide these packages only as a courtesy to customers. Red Hat will not provide updates to the Adobe Reader packages.

This update disables the Adobe Reader web browser plug-in, which is available via the acroread-plugin package, to prevent the exploitation of security issues without user interaction when a user visits a malicious web page.

Red Hat advises users to reconsider further use of Adobe Reader for Linux, as it may contain known, unpatched security issues. Alternative PDF rendering software, such as Evince and KPDF (part of the kdegraphics package) in Red Hat Enterprise Linux 5, or Evince and Okular (part of the kdegraphics package) in Red Hat Enterprise Linux 6, should be considered. These packages will continue to receive security fixes.

Red Hat will no longer provide security updates to these packages and recommends that customers not use this application on Red Hat Enterprise Linux effective immediately.

3.2. am-utils

3.2.1. RHBA-2014:0198 — am-utils bug fix update

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

[Updated 25 February 2014] This advisory has been updated with the correct description of the ENOENT error. No changes have been made to the packages.

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

Bug Fix

BZ#1065876

Previously, the am-utils automount utility (amd) did not properly handle possible "no such entity" error (ENOENT) returns when executing the umount system calls on file systems mounted within the autofs file system. As a consequence, amd terminated unexpectedly with a segmentation fault under some circumstances. With this update, amd handles ENOENT returns as expected, and the problem no longer occurs.

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

3.3. autofs

3.3.1. RHBA-2014:1240 — 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 in use and unmounts them when they are not busy.

Bug Fix

BZ#1049017

> In a previous version, a check for mounted file systems was removed from autofs mount control script if a miscellaneous device was not used. However, a subsequent update introduced a mount export function that requires this check. As a consequence, autofs mounts sometimes became unresponsive when re-reading the mount map. This update fixes the bug and autofs mounts no longer hang in the scenario described.

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

3.4. automake

3.4.1. RHSA-2014:1243 — Low: automake security update

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

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

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

Security Fix

CVE-2012-3386

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

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

All automake users are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

3.5. bind97

3.5.1. RHSA-2014:1244 — Moderate: bind97 security and bug fix update

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

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

The 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.

Security Fix

CVE-2014-0591

> A denial of service flaw was found in the way BIND handled queries for NSEC3-signed zones. A remote attacker could use this flaw against an authoritative name server that served NCES3-signed zones by sending a specially crafted query, which, when processed, would cause named to crash.

Note: The CVE-2014-0591 issue does not directly affect the version of bind97 shipped in Red Hat Enterprise Linux 5. This issue is being addressed however to assure it is not introduced in future builds of bind97 (possibly built with a different compiler or C library optimization).

Bug Fix

BZ#1059118

> Previously, the bind97 initscript did not check for the existence of the ROOTDIR variable when shutting down the named daemon. As a consequence, some parts of the file system that are mounted when using bind97 in a chroot environment were unmounted on daemon shut down, even if bind97 was not running in a chroot environment. With this update, the initscript has been fixed to check for the existence of the ROOTDIR variable when unmounting some parts of the file system on named daemon shut down. Now, when shutting down bind97 that is not running in a chroot environment, no parts of the file system are unmounted.

Note: The CVE-2014-0591 issue does not directly affect the version of bind97 shipped in Red Hat Enterprise Linux 5. This issue is being addressed however to assure it is not introduced in future builds of bind97 (possibly built with a different compiler or C library optimization).

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

3.6. clustermon

3.6.1. RHBA-2014:1216 — clustermon bug fix update

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

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

Bug Fix

BZ#1076714

The modcluter module is a ricci module shipped with the clustermon packages. Previously, modcluster mishandled requests with size in bytes divisible by 4096, which is the size of the read buffer in bytes. Consequently, modcluster incorrectly evaluated such requests as errors. This bug has been fixed and modcluster now processes all requests as expected. See also RHBA-2014:17045 for the information about the remaining ricci modules shipped with the ricci packages.

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

3.7. cman

3.7.1. RHBA-2014:0002 — cman bug fix update

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

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

Bug Fixes

BZ#1043484

Due to a regression, the fence_bladecenter fence agent was not able to login to fence devices. The login code for fencing.py has been fixed, and a fence agent now logins to fence devices as expected.

BZ#1043358

Previously, under some circumstances on a two-node cluster, both cluster nodes could be granted a lock on the same file at the same time on a GFS2 (Global File System 2) file system. A patch has been provided to fix this bug. With this update, only one cluster node is able to lock the file, the other cluster node waits till the lock is released.

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

3.7.2. RHBA-2013:1478 — 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#1021811

Previously, the fence_cisco_ucs fence agent did not respect the "delay" attribute, which could lead to the situation in which two nodes fence each other. With this update, a fence agent waits for given amount of time as expected.

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

3.7.3. RHBA-2014:0282 — 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#1073821

> Previously, the fence_vmware_soap fence agent did not respect the "delay" attribute, which could cause a situation where two nodes fenced each other at the same time. With this update, the agent waits for the given amount of time as expected, and race conditions no longer occur.

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

3.7.4. RHBA-2014:1211 — cman bug fix and enhancement update

Updated cman packages that fix several bugs and add one enhancement 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#994187

> Due to incorrect quorum disk configuration, some cluster nodes could display an incorrect "Member status" value if the cluster was restarted by the qdisk quorum daemon. This update amends the quorum disk configuration and cluster nodes now display the correct status in the scenario described.

BZ#994228

> Previously, the fence_cisco_ucs fence agent did not respect the "delay" attribute, which could lead to a situation in which two nodes fenced each other. This bug has been fixed and fence_cisco_ucs now waits for the given amount of time as expected.

BZ#1017916

> A node on a two-node cluster could, under some circumstances, fail to unlink a checkpoint. As a consequence, both cluster nodes on the cluster could simultaneously be granted a lock on the same file located on a GFS2 file system. With this update, checkpoints on two-node clusters are unlinked as intended, and only one cluster can now hold a lock to a file at a time.

BZ#1029191

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

BZ#1040099

> Due to errors in the login code for the fencing.py file, the fence_bladecenter fence agent was not able to log into fence devices. The login code for fencing.py has been fixed, and fence_bladecenter now logs into fence devices as expected.

BZ#1075691

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

In addition, this update adds the following

Enhancement

BZ#1072605

The support for the "--delay" option has been added to the fence_vmware_soap fencing agent. This option allows the user to avoid fence races, and thus prevents nodes from potentially fencing each other.

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

3.8. conga

3.8.1. RHSA-2014:1194 — [Moderate] security and bug fix update

Updated *conga* packages that fix multiple security issues and several bugs are now available for Red Hat Enterprise Linux 5.

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

The 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 Fixes

CVE-2014-3521

It was discovered that various components in the **`luci`** site extensions-related URLs were not properly restricted to administrative users. A remote, authenticated attacker could elevate their privileges to perform certain actions that should be restricted to administrative users, such as adding users and systems, and viewing log data.

CVE-2013-6496

Multiple information leak flaws were found in the way **`conga`** processed **`luci`** site extensions-related URL requests. A remote, unauthenticated attacker could issue a specially-crafted HTTP request that, when processed, would lead to unauthorized information disclosure.

CVE-2012-5500

It was discovered that **Plone**, included as part of **`luci`**, allowed a remote anonymous user to change titles of content items due to improper permissions checks.

CVE-2012-5499

It was discovered that **Plone**, included as part of **`luci`**, did not properly handle the processing of very large values passed to an internal utility function. A remote attacker could use a specially-crafted URL that, when processed, would lead to excessive memory consumption.

CVE-2012-5498

It was discovered that **Plone**, included as part of **`luci`**, did not properly handle the processing of requests for certain collections. A remote attacker could use a specially-crafted URL that, when processed, would lead to excessive I/O and/or cache resource consumption.

CVE-2012-5497

It was discovered that **Plone**, included as part of **`luci`**, did not properly enforce permissions checks on the membership database. A remote attacker could use a specially-crafted URL that, when processed, could allow the attacker to enumerate user account names.

CVE-2012-5485

It was discovered that **Plone**, included as part of **`luci`**, did not properly protect the administrator interface (control panel) which could allow a remote attacker to inject a specially-crafted Python statement or script into **Plone**'s restricted Python sandbox that, when the administrator interface was accessed, would be executed with the privileges of that admin user.

CVE-2012-5486

It was discovered that **Plone**, included as part of **`luci`**, did improper sanitization of HTTP headers provided within certain URL requests. A remote attacker would use a specially-crafted URL that, when processed, would lead to the injected HTTP headers being returned as part of the **Plone** HTTP response, which could lead to various negative consequences.

CVE-2012-5488

It was discovered that **Plone**, included as part of **`luci`**, improperly protected the privilege of running **`RestrictedPython`** scripts. A remote attacker could use a specially-crafted URL that, when processed, would allow the attacker to submit and perform expensive computations or, in conjunction with other attacks, be able to access or alter privileged information.

The CVE-2014-3521 issue was discovered by Radek Steiger of Red Hat, and the CVE-2013-6496 issue was discovered by Jan Pokorny of Red Hat.

Bug Fixes

BZ#970288

Due to a bug in the underlying source code that checks the return value when stopping the **`luci`** service, **`luci`** was reported as stopped even if it was not. This bug has been fixed and the return value is correctly checked, so that **`luci`** works properly in the described scenario.

BZ#106526

The ***`startup_wait`*** parameter has been added to the **`ostgreSQL 8`**P resource agent. For more information, see RHBA-2014:17291. With this update the **`luci`** service has been modified to reflect this change.

BZ#1072075

Previously, the **`luci`** service did not parse distribution release string from the remote **`ricci`** agent correctly; any minor version with two or more digits in that string was unexpectedly truncated to the initial digit. This behavior caused several regressions in offered configuration options starting with Red Hat Enterprise Linux 5.10 identification understood as version 5.1. This bug has been fixed with this update, and **`luci`** now correctly parses minor versions, thus no regressions occur.

BZ#1076711

Previously, **`ricci`** modules shipped directly with the *ricci* package mishandled requests with size in bytes divisible by 4096, which is the size of the read buffer in bytes. Consequently, these modules incorrectly evaluated such requests as errors. This bug has been fixed and the modules now process all requests as expected. See also RHBA-2014:17436 for the information about a remaining **`ricci`** module shipped with the *modcluster* package.

All *conga* users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the luci and ricci services will be restarted automatically.

3.9. coolkey

3.9.1. RHBA-2014:1233 — coolkey bug fix update

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

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

Bug Fix

BZ#995560

Previously, the number of encryption keys that the coolkey applet can process was increased from 8 to 24. However, this number was not increased in the coolkey library. As a consequence, a token running the coolkey application failed to recover the encryption key, when nine or more encryption keys were set by the coolkey applet. This update introduces the support for up to 24 encryption keys to the coolkey library, and recovering more than 8 encryption keys now proceeds correctly.

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

3.10. cpuspeed

3.10.1. RHBA-2014:0394 — cpuspeed bug fix update

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

The cpuspeed packages contain a daemon that dynamically changes the speed of processors depending upon their current workload. This package also allows users to enable CPU frequency scaling using in-kernel CPUfreq governors on Intel Centrino and AMD Athlon64/Opteron platforms.

Bug Fix

BZ#1078211

Previously, certain AMD processors were not entirely compatible with the CPU frequency scaling. As a consequence, a kernel panic could occur on some AMD-based Hardware Virtual Machine (HVM) guests when CPU frequency scaling was enabled. With this patch, the default CPU governor value has been set to "performance", which prevents this problem. Thus, unless the user changes the CPU governor setting, the kernel now no longer panics when CPU frequency scaling is enabled on HVM guests.

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

3.11. device-mapper-multipath

3.11.1. RHBA-2014:0410 — 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#1065229

Previously, if the user created duplicate aliases, or aliases that matched the user_friendly names, those devices switched their paths, and thus caused multipath device path corruption. The underlying code has been fixed, and the multipath utility now refuses to reload a device with an existing duplicate alias. In addition, multipath now issues a warning message on potentially conflicting aliases. As a result, multipath no longer corrupts data if users name two devices identically.

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

3.11.2. RHBA-2014:1228 — device-mapper-multipath bug fix update

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

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

Bug Fixes

BZ#1092603

A bug in Device Mapper Multipath (DM-Multipath) allowed the main multipathd thread to free memory that was still being used by other multipathd threads during system shutdown. Consequently, the multipathd daemon terminated unexpectedly due to use-after-free memory corruption. This update avoids this problem by ensuring that memory being used by multipathd threads is freed in the final cleanup upon the exit of multipathd.

BZ#1039935

DM-Multipath allowed configurations with duplicate name aliases mapped to different World Wide Identifiers (WWIDs). However, such configurations could result in path corruption when a device was reloaded and used the paths of another device. This update ensures that DM-Multipath refuses to reload a device if its alias matches another device. DM-Multipath now also warns the user on potentially conflicting aliases.

BZ#1086949

The multipathd daemon could attempt to reconfigure before it was completely set up after receiving the SIGHUP signal on startup. As a consequence, multipathd terminated unexpectedly with a segmentation fault. With this update, multipathd now blocks the SIGHUP signal until it has completed its initialization.

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

3.12. dmidecode

3.12.1. RHEA-2014:1208 — dmidecode enhancement update

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

The dmidecode packages provide utilities for extracting x86 and Intel Itanium hardware information from the system BIOS or EFI, depending on the SMBIOS/DMI standard. This information typically includes system manufacturer, model name, serial number, BIOS version, and asset tag.

Enhancement

BZ#1048920

The dmidecode package has been upgraded to version 2.12, which adds support for SMBIOS specification version 2.8 to Red Hat Enterprise Linux 5.

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

3.13. e2fsprogs

3.13.1. RHBA-2014:1222 — e2fsprogs bug fix update

Updated e2fsprogs packages that fix several 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 ext2 and ext3 file systems.

Bug Fixes

BZ#885073

Previously, under certain circumstances, the e2fsck utility handled incorrectly a file system error state stored in the journal superblock, which could cause the file system to be marked as "in error". With this update, such errors are properly propagated from the journal to the file system superblock, and e2fsck now clears errors from the journal properly if no recovery is required.

BZ#905027

Previously, the /usr/sbin/uuidd daemon was incorrectly assigned a user and group of root/root. Consequently, this deamon could gain root privileges and be directly executed by root. Moreover, the UID could have been reused in the passwd database, potentially causing a security leak. With this update, the uuidd daemon is assigned the "uuidd" user and group, thus fixing this bug.

BZ#910214

Previously, the chattr and lsattr commands did not properly return an error when operating on symbolic links. The underlying source code has been fixed, and performing these operations on symbolic links now correctly returns the "Operation not supported" message.

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

3.14. e4fsprogs

3.14.1. RHBA-2013:1789 — e4fsprogs bug fix update

Updated e4fsprogs packages that fix one bug are now available for Red Hat Enterprise Linux 5.

The e4fsprogs packages contain a number of utilities for creating, checking, modifying, and correcting inconsistencies in fourth extended (ext4 and ext4dev) file systems. e4fsprogs contains e4fsck (used to repair file system inconsistencies after an unclean shutdown), mke4fs (used to initialize a partition to contain an empty ext4 file system), tune4fs (used to modify file system parameters), and most other core ext4fs file system utilities.

Bug Fix

BZ#1033548

Previously, the resize4fs utility mishandled the resizing of an ext4 file system to a smaller size. As a consequence, files containing many extents could become corrupted if they were moved during the resize process. With this update, resize4fs now maintains a consistent extent tree when moving files containing many extents, and such files no longer become corrupted in this scenario.

Users of e4fsprogs are advised to upgrade to these updated packages, which fix this bug.

3.15. firefox

3.15.1. RHSA-2014:0741 — Critical: firefox security update

Updated firefox packages that fix several security issues are now available for Red Hat Enterprise Linux 5, 6, and 7.

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

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

Security Fix

CVE-2014-1533, CVE-2014-1538, CVE-2014-1541

> 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.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Gary Kwong, Christoph Diehl, Christian Holler, Hannes Verschore, Jan de Mooij, Ryan VanderMeulen, Jeff Walden, Kyle Huey, Abhishek Arya, and Nils as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 24.6.0 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 24.6.0 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

3.15.2. RHSA-2013:1812 — Critical: firefox security update

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

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

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

Security Fixes

CVE-2013-5609, CVE-2013-5616, CVE-2013-5618, CVE-2013-6671, CVE-2013-5613

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

CVE-2013-5612

> A flaw was found in the way Firefox rendered web content with missing character encoding information. An attacker could use this flaw to possibly bypass same-origin inheritance and perform cross-site scripting (XSS) attacks.

CVE-2013-5614

> It was found that certain malicious web content could bypass restrictions applied by sandboxed iframes. An attacker could combine this flaw with other vulnerabilities to execute arbitrary code with the privileges of the user running Firefox.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Ben Turner, Bobby Holley, Jesse Ruderman, Christian Holler, Masato Kinugawa, Daniel Veditz, Jesse Schwartzentruber, Nils, Tyson Smith, and Atte Kettunen as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 24.2.0 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 24.2.0 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

3.15.3. RHSA-2013:1476 — Critical: firefox security update

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

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

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

Security Fixes

CVE-2013-5590, CVE-2013-5597, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602

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

CVE-2013-5595

> It was found that the Firefox JavaScript engine incorrectly allocated memory for certain functions. An attacker could combine this flaw with other vulnerabilities to execute arbitrary code with the privileges of the user running Firefox.

CVE-2013-5604

> A flaw was found in the way Firefox handled certain Extensible Stylesheet Language Transformations (XSLT) files. An attacker could combine this flaw with other vulnerabilities to execute arbitrary code with the privileges of the user running Firefox.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Jesse Ruderman, Christoph Diehl, Dan Gohman, Byoungyoung Lee, Nils, and Abhishek Arya as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 17.0.10 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 17.0.10 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

3.15.4. RHSA-2014:0448 — Critical: firefox security update

An updated firefox package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Firefox is an open source web browser.

Security Fixes

CVE-2014-1518, CVE-2014-1524, CVE-2014-1529, CVE-2014-1531

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-2014-1532

A use-after-free flaw was found in the way Firefox resolved hosts in certain circumstances. An attacker could use this flaw to crash Firefox or, potentially, execute arbitrary code with the privileges of the user running Firefox.

CVE-2014-1523

An out-of-bounds read flaw was found in the way Firefox decoded JPEG images. Loading a web page containing a specially crafted JPEG image could cause Firefox to crash.

CVE-2014-1530

A flaw was found in the way Firefox handled browser navigations through history. An attacker could possibly use this flaw to cause the address bar of the browser to display a web page name while loading content from an entirely different web page, which could allow for cross-site scripting (XSS) attacks.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Bobby Holley, Carsten Book, Christoph Diehl, Gary Kwong, Jan de Mooij, Jesse Ruderman, Nathan Froyd, Christian Holler, Abhishek Arya, Mariusz Mlynski, moz_bug_r_a4, Nils, Tyson Smith, and Jesse Schwartzentrube as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 24.5.0 ESR.

All Firefox users should upgrade to this updated package, which contains Firefox version 24.5.0 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

3.15.5. RHSA-2014:0132 — Critical: firefox security update

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

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

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

Security Fixes

CVE-2014-1477, CVE-2014-1482, CVE-2014-1486

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-2014-1487

A flaw was found in the way Firefox handled error messages related to web workers. An attacker could use this flaw to bypass the same-origin policy, which could lead to cross-site scripting (XSS) attacks, or could potentially be used to gather authentication tokens and other data from third-party websites.

CVE-2014-1479

A flaw was found in the implementation of System Only Wrappers (SOW). An attacker could use this flaw to crash Firefox. When combined with other vulnerabilities, this flaw could have additional security implications.

CVE-2014-1481

It was found that the Firefox JavaScript engine incorrectly handled window objects. A remote attacker could use this flaw to bypass certain security checks and possibly execute arbitrary code.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Christian Holler, Terrence Cole, Jesse Ruderman, Gary Kwong, Eric Rescorla, Jonathan Kew, Dan Gohman, Ryan VanderMeulen, Sotaro Ikeda, Cody Crews, Fredrik "Flonka" Lönnqvist, Arthur Gerkis, Masato Kinugawa, and Boris Zbarsky as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 24.3.0 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 24.3.0 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

3.15.6. RHSA-2014:0310 — Critical: firefox security update

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

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

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

Security Fixes

CVE-2014-1493, CVE-2014-1510, CVE-2014-1511, CVE-2014-1512, CVE-2014-1513, CVE-2014-1514

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-2014-1497, CVE-2014-1508, CVE-2014-1505

Several information disclosure flaws were found in the way Firefox processed malformed web content. An attacker could use these flaws to gain access to sensitive information such as cross-domain content or protected memory addresses or, potentially, cause Firefox to crash.

CVE-2014-1509

> A memory corruption flaw was found in the way Firefox rendered certain PDF files. An attacker able to trick a user into installing a malicious extension could use this flaw to crash Firefox or, potentially, execute arbitrary code with the privileges of the user running Firefox.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Benoit Jacob, Olli Pettay, Jan Varga, Jan de Mooij, Jesse Ruderman, Dan Gohman, Christoph Diehl, Atte Kettunen, Tyson Smith, Jesse Schwartzentruber, John Thomson, Robert O'Callahan, Mariusz Mlynski, Jüri Aedla, George Hotz, and the security research firm VUPEN as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Firefox 24.4.0 ESR.

All Firefox users should upgrade to these updated packages, which contain Firefox version 24.4.0 ESR, which corrects these issues. After installing the update, Firefox must be restarted for the changes to take effect.

3.16. flash-plugin

3.16.1. RHSA-2013:1518 — 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. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2013-5329, CVE-2013-5330

> This update fixes multiple vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB13-26. 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 11.2.202.327.

3.16.2. RHSA-2014:0745 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fixes

CVE-2014-0534, CVE-2014-0535, CVE-2014-0536

> This update fixes multiple vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security Bulletin APSB14-16.
>
> Multiple 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 malicious SWF content.

CVE-2014-0531, CVE-2014-0532, CVE-2014-0533

> Multiple flaws in flash-plugin could allow an attacker to conduct cross-site scripting (XSS) attacks if a victim were tricked into visiting a specially crafted web page.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.378.

3.16.3. RHSA-2014:0447 — Critical: flash-plugin security update

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

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2014-0515

> This update fixes one vulnerability in Adobe Flash Player. This vulnerability is detailed in the Adobe Security Bulletin APSB14-13.
>
> 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 malicious SWF content.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.356.

3.16.4. RHSA-2014:0496 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fixes

CVE-2014-0510, CVE-2014-0517, CVE-2014-0518, CVE-2014-0519, CVE-2014-0520

> This update fixes multiple vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security Bulletin APSB14-14.
>
> Multiple 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 malicious SWF content.

CVE-2014-0516

> A flaw in flash-plugin could allow an attacker to bypass the same-origin policy.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.359.

3.16.5. RHSA-2014:0028 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes two security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2014-0491, CVE-2014-0492

> This update fixes multiple vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB14-02. 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 11.2.202.335.

3.16.6. RHSA-2014:0196 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes three security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2014-0498, CVE-2014-0499, CVE-2014-0502

> This update fixes multiple vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB14-07. 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 11.2.202.341.

3.16.7. RHSA-2014:0137 — 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. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2014-0497

> This update fixes one vulnerability in Adobe Flash Player. This vulnerability is detailed in the Adobe Security bulletin APSB14-04. Specially-crafted SWF content could cause flash-plugin to crash or, potentially, execute arbitrary code when a victim loads a page containing the malicious SWF content.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.336.

3.16.8. RHSA-2013:1818 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes two security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fix

CVE-2013-5331, CVE-2013-5332

> This update fixes multiple vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB13-28. 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 11.2.202.332.

3.16.9. RHSA-2014:0289 — Moderate: 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 Moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fixes

CVE-2014-0503

> This update fixes two vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security bulletin APSB14-08.
>
> A vulnerability was reported that could be used to bypass the same origin policy.

CVE-2014-0504

> A vulnerability was reported that could be used to read the contents of the clipboard.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.346.

3.16.10. RHSA-2014:0380 — Critical: flash-plugin security update

An updated Adobe Flash Player package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

The flash-plugin package contains a Mozilla Firefox compatible Adobe Flash Player web browser plug-in.

Security Fixes

CVE-2014-0506, CVE-2014-0507

> This update fixes multiple vulnerabilities in Adobe Flash Player. These vulnerabilities are detailed in the Adobe Security Bulletin APSB14-09.
>
> Two 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 malicious SWF content.

CVE-2014-0508

> 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.

CVE-2014-0509

> A flaw in flash-plugin could allow an attacker to conduct cross-site scripting (XSS) attacks if a victim were tricked into visiting a specially crafted web page.

All users of Adobe Flash Player should install this updated package, which upgrades Flash Player to version 11.2.202.350.

3.17. gcc

3.17.1. RHBA-2014:1209 — 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#799592

Due to corruption of internal GCC structures, GCC could terminate unexpectedly with a segmentation fault when compiling a certain code with optimizations and coverage options enabled, causing the Garbage Collector to fail. The related GCC code has been fixed and the crash no longer occurs.

BZ#901750

GCC could terminate unexpectedly when compiling a code with arithmetics on TI mode (16-byte integer mode) values on AMD64 and Intel 64 architectures. The relevant GCC code has been fixed so that the crash no longer occurs. Note that the 128-bit integer support in GCC version 4.1 has several deficiencies; this support is better implemented in the gcc44 packages.

BZ#1008819

Previously, GCC could terminate unexpectedly with a segmentation fault when compiling a code that initializes nested structures which define a type of an array of structures (using typedef). A fix has been applied and GCC now compiles such code correctly.

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

3.18. gfs2-utils

3.18.1. RHBA-2014:0569 — gfs2-utils bug fix update

Updated gfs2-utils packages that fix two bugs are now available for Red Hat Enterprise Linux 5.

The gfs2-utils packages contain utilities for creating, checking, modifying, and correcting any inconsistencies in GFS2 file systems.

Bug Fixes

BZ#1099592

Prior to this update, system logs did not log important context of system events concerning the running fsck.gfs2 utility. Consequently, users and system administrators had difficulties examining the circumstances under which a problem occurred. With this update, fsck.gfs2 adds an informative message to the system logs on its start and exit, which helps in further debugging processes and administrative actions.

BZ#1100803

Previously, GFS2 metadata dumps returned by the "gfs2_edit savemeta" command held no information about the time at which they were created. Without this information, users and system administrators could not easily find out when the GFS2 metadata was saved in relation to file system checks. With this update, "gfs2_edit savemeta" adds a header to the metadata file containing a time stamp relating to the creation of the file.

Users of gfs2-utils are advised to upgrade to these updated packages, which fix these bugs.

3.18.2. RHBA-2014:0438 — 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 contain utilities for creating, checking, modifying, and correcting any inconsistencies in GFS2 file systems.

Bug Fix

BZ#1086861

Prior to this update, when the gfs2_grow, gfs2_tool, gfs2_jadd and gfs2_quota utilities cleaned up the /etc/mtab file, the file's permissions were changed from the default of 644 to 600. As a consequence, non-root processes could not read /etc/mtab. This update fixes the code that cleans up the /etc/mtab file so that it no longer modifies the /etc/mtab file's permissions. As a result, processes are able to access the /etc/mtab file as expected.

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

3.18.3. RHBA-2014:1203 — gfs2-utils bug fix update

Updated gfs2-utils packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The gfs2-utils packages contain utilities for creating, checking, modifying, and correcting any inconsistencies in GFS2 file systems.

Bug Fixes

BZ#902918

Under rare circumstances, certain leaf blocks are written to the incorrect index nodes. Thus, some directories have improper leaf blocks attached. In certain cases, the fsck.gfs2 utility was unable to detect and repair this corruption. With this update, a patch has been provided to fix this bug and fsck.gfs2 now correctly detects and fixes the corruption.

BZ#1073384

After the gfs2_grow, gfs2_tool, gfs2_jadd, or gfs2_quota utilities cleaned up the /etc/mtab file, the file's permissions were changed from the default of 644 to 600. As a consequence, non-root processes could not read /etc/mtab. This update fixes the code that cleans up the /etc/mtab file so that it no longer modifies the /etc/mtab file's permissions. As a result, processes are able to access the /etc/mtab file as expected.

BZ#1084140

Under certain circumstances, an attempt to use the gfs2_convert utility caused the system to terminate unexpectedly with a segmentation fault. This update provides a patch to fix this bug so that the system no longer crashes in the described scenario.

BZ#1097348

Previously, the fsck.gfs2 utility did not log important context of system events. Consequently, users and system administrators had difficulties examining the circumstances under which a problem occurred. With this update, fsck.gfs2 adds an informative message to the system logs on its start and exit, which helps in further debugging processes and administrative actions.

BZ#1097349

Previously, GFS2 metadata dumps returned by the "gfs2_edit savemeta" command held no information about the time at which they were created. Without this information, users and system administrators could not easily find out when the GFS2 metadata was saved in relation to file system checks. With this update, "gfs2_edit savemeta" adds a header to the metadata file containing a time stamp.

Users of gfs2-utils are advised to upgrade to these updated packages, which fix these bugs.

3.19. gfs-kmod

3.19.1. RHBA-2014:1234 — gfs-kmod bug fix update

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

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

Bug Fix

BZ#1066181

Previously, the gfs utility was not synchronizing the inode attributes to disk along with the data for shared mmap() writes. Consequently, files did not have their mtime (modification time) value updated. With this update, gfs writes the inode time stamps to disk when the msync() function is called, and gfs now synchronizes the inode attributes to disk as intended.

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

3.20. gimp

3.20.1. RHSA-2013:1778 — Moderate: gimp security update

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

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

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

Security Fix

CVE-2012-5576, CVE-2013-1913, CVE-2013-1978

> A stack-based buffer overflow flaw, a heap-based buffer overflow, and an integer overflow flaw were found in the way GIMP loaded certain X Window System (XWD) image dump files. A remote attacker could provide a specially crafted XWD image file that, when processed, would cause the XWD plug-in to crash or, potentially, execute arbitrary code with the privileges of the user running the GIMP.

The CVE-2013-1913 and CVE-2013-1978 issues were discovered by Murray McAllister of the Red Hat Security Response Team.

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

3.21. glibc

3.21.1. RHSA-2013:1411 — 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 from the CVE link associated with the description below.

The glibc packages provide the standard C libraries (libc), POSIX thread libraries (libpthread), standard math libraries (libm), and the Name Server Caching Daemon (nscd) used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

Security Fix

CVE-2013-4332

> Multiple integer overflow flaws, leading to heap-based buffer overflows, were found in glibc's memory allocator functions (pvalloc, valloc, and memalign). If an application used such a function, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

Bug Fix

BZ#1011424

> Prior to this update, the size of the L3 cache in certain CPUs for SMP (Symmetric Multiprocessing) servers was not correctly detected. The incorrect cache size detection resulted in less than optimal performance for routines that used this information, including the memset() function. To fix this bug, the cache size detection has been corrected and core routines including memset() have their performance restored to expected levels.

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

3.21.2. RHBA-2014:1213 — glibc bug fix update

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

The glibc packages provide the standard C libraries (libc), POSIX thread libraries (libpthread), standard math libraries (libm), and the Name Server Caching Daemon (nscd) used by multiple programs on the system. Without these libraries, the Linux system cannot function correctly.

Bug Fixes

BZ#979413

An attempt to start an already running service by using the "service" command should result in a zero exit code. However, due to an error in the nscd init script, the "service nscd start" command returned a non-zero exit code. This update corrects the nscd init script and this command returns a zero exit code as expected in the described situation.

BZ#995207

The getgroups() function incorrectly accepted a negative size value and then terminated unexpectedly if a related program was compiled with optimizations enabled and the FORTIFY_SOURCE parameter was set to 2. This update corrects the getgroups() function to return an EINVAL error in such cases.

BZ#1003420

The size of the L3 cache in certain CPUs for SMP (Symmetric Multiprocessing) servers was not correctly detected. The incorrect cache size detection resulted in less than optimal performance for routines that used this information, including the memset() function. To fix this problem, the cache size detection has been corrected and core routines including memset() work with the expected efficiency.

BZ#1020486

The getnameinfo() function previously failed on a reverse lookup of an IP address that had a large number of PTR records associated with it. This problem has been corrected and getnameinfo() now correctly returns one of the PTR records as the response.

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

3.22. gnupg

3.22.1. RHSA-2013:1458 — Moderate: gnupg security update

An updated gnupg package that fixes multiple security issues is now available for Red Hat Enterprise Linux 5.

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

The GNU Privacy Guard (GnuPG or GPG) is a tool for encrypting data and creating digital signatures, compliant with the proposed OpenPGP Internet standard and the S/MIME standard.

Security Fixes

CVE-2013-4242

It was found that GnuPG was vulnerable to the Yarom/Falkner flush+reload cache side-channel attack on the RSA secret exponent. An attacker able to execute a process on the logical CPU that shared the L3 cache with the GnuPG process (such as a different local user or a user of a KVM guest running on the same host with the kernel same-page merging functionality enabled) could possibly use this flaw to obtain portions of the RSA secret key.

CVE-2013-4402

A denial of service flaw was found in the way GnuPG parsed certain compressed OpenPGP packets. An attacker could use this flaw to send specially crafted input data to GnuPG, making GnuPG enter an infinite loop when parsing data.

CVE-2012-6085

It was found that importing a corrupted public key into a GnuPG keyring database corrupted that keyring. An attacker could use this flaw to trick a local user into importing a specially crafted public key into their keyring database, causing the keyring to be corrupted and preventing its further use.

CVE-2013-4351

It was found that GnuPG did not properly interpret the key flags in a PGP key packet. GPG could accept a key for uses not indicated by its holder.

Red Hat would like to thank Werner Koch for reporting the CVE-2013-4402 issue. Upstream acknowledges Taylor R Campbell as the original reporter.

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

3.22.2. RHSA-2014:0016 — Moderate: gnupg security update

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

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

The GNU Privacy Guard (GnuPG or GPG) is a tool for encrypting data and creating digital signatures, compliant with the proposed OpenPGP Internet standard and the S/MIME standard.

Security Fix

CVE-2013-4576

It was found that GnuPG was vulnerable to side-channel attacks via acoustic cryptanalysis. An attacker in close range to a target system that is decrypting ciphertexts could possibly use this flaw to recover the RSA secret key from that system.

Red Hat would like to thank Werner Koch of GnuPG upstream for reporting this issue. Upstream acknowledges Genkin, Shamir, and Tromer as the original reporters.

All gnupg users are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

3.23. gnupg2

3.23.1. RHSA-2013:1459 — Moderate: gnupg2 security update

An updated gnupg2 package that fixes three 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. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability associated with each description below.

The GNU Privacy Guard (GnuPG or GPG) is a tool for encrypting data and creating digital signatures, compliant with the proposed OpenPGP Internet standard and the S/MIME standard.

Security Fixes

CVE-2013-4402

> A denial of service flaw was found in the way GnuPG parsed certain compressed OpenPGP packets. An attacker could use this flaw to send specially crafted input data to GnuPG, making GnuPG enter an infinite loop when parsing data.

CVE-2012-6085

> It was found that importing a corrupted public key into a GnuPG keyring database corrupted that keyring. An attacker could use this flaw to trick a local user into importing a specially crafted public key into their keyring database, causing the keyring to be corrupted and preventing its further use.

CVE-2013-4351

> It was found that GnuPG did not properly interpret the key flags in a PGP key packet. GPG could accept a key for uses not indicated by its holder.

Red Hat would like to thank Werner Koch for reporting the CVE-2013-4402 issue. Upstream acknowledges Taylor R Campbell as the original reporter.

All gnupg2 users are advised to upgrade to this updated package, which contains backported patches to correct these issues.

3.24. gnutls

3.24.1. RHSA-2014:0594 — Important: gnutls security update

Updated gnutls packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

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

The GnuTLS library provides support for cryptographic algorithms and for protocols such as Transport Layer Security (TLS). The gnutls packages also include the libtasn1 library, which provides Abstract Syntax Notation One (ASN.1) parsing and structures management, and Distinguished Encoding Rules (DER) encoding and decoding functions.

Security Fixes

CVE-2014-3466

> A flaw was found in the way GnuTLS parsed session IDs from ServerHello messages of the TLS/SSL handshake. A malicious server could use this flaw to send an excessively long session ID value, which would trigger a buffer overflow in a connecting TLS/SSL client application using GnuTLS, causing the client application to crash or, possibly, execute

arbitrary code.

CVE-2014-3468

It was discovered that the asn1_get_bit_der() function of the libtasn1 library incorrectly reported the length of ASN.1-encoded data. Specially crafted ASN.1 input could cause an application using libtasn1 to perform an out-of-bounds access operation, causing the application to crash or, possibly, execute arbitrary code.

CVE-2014-3467

Multiple incorrect buffer boundary check issues were discovered in libtasn1. Specially crafted ASN.1 input could cause an application using libtasn1 to crash.

CVE-2014-3469

Multiple NULL pointer dereference flaws were found in libtasn1's asn1_read_value() function. Specially crafted ASN.1 input could cause an application using libtasn1 to crash, if the application used the aforementioned function in a certain way.

Red Hat would like to thank GnuTLS upstream for reporting these issues. Upstream acknowledges Joonas Kuorilehto of Codenomicon as the original reporter of CVE-2014-3466.

Users of GnuTLS are advised to upgrade to these updated packages, which correct these issues. For the update to take effect, all applications linked to the GnuTLS or libtasn1 library must be restarted.

3.24.2. RHSA-2014:0247 — Important: gnutls security update

Updated gnutls packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

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

The GnuTLS library provides support for cryptographic algorithms and for protocols such as Transport Layer Security (TLS).

Security Fixes

CVE-2014-0092

It was discovered that GnuTLS did not correctly handle certain errors that could occur during the verification of an X.509 certificate, causing it to incorrectly report a successful verification. An attacker could use this flaw to create a specially crafted certificate that could be accepted by GnuTLS as valid for a site chosen by the attacker.

CVE-2009-5138

A flaw was found in the way GnuTLS handled version 1 X.509 certificates. An attacker able to obtain a version 1 certificate from a trusted certificate authority could use this flaw to issue certificates for other sites that would be accepted by GnuTLS as valid.

The CVE-2014-0092 issue was discovered by Nikos Mavrogiannopoulos of the Red Hat Security Technologies Team.

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

3.25. grub

3.25.1. RHBA-2013:1775 — grub bug fix update

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

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

Bug Fix

BZ#1034595

A regular expression in the grub-install program could not match multipath devices when the "user_friendly_name" option was set to "no". As a consequence, the user was not able to install the GRUB utility on a specified device. To fix this bug, the regular expression has been updated to match the requested device names. As a result, GRUB now installs successfully.

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

3.26. httpd

3.26.1. RHBA-2013:1433 — 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#1012892

Due to a bug in the mod_proxy_httpd module, the error message "proxy: error reading response" was logged into the global error log file even when there was a specific VirtualHost error log file configured. This bug is now fixed and the aforementioned error message is now logged into the correct log file.

Users of httpd are advised to upgrade to these updated packages, which fix this bug. After installing the updated packages, the httpd daemon will be restarted automatically.

3.26.2. RHSA-2014:0369 — Moderate: httpd security update

Updated httpd 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 scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server.

Security Fixes

CVE-2013-6438

It was found that the mod_dav module did not correctly strip leading white space from certain elements in a parsed XML. In certain httpd configurations that use the mod_dav module (for example when using the mod_dav_svn module), a remote attacker could send a specially crafted DAV request that would cause the httpd child process to crash or, possibly, allow the attacker to execute arbitrary code with the privileges of the "apache" user.

CVE-2014-0098

A buffer over-read flaw was found in the httpd mod_log_config module. In configurations where cookie logging is enabled (on Red Hat Enterprise Linux it is disabled by default), a remote attacker could use this flaw to crash the httpd child process via an HTTP request with a malformed cookie header.

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

3.26.3. RHBA-2014:1232 — httpd bug fix and enhancement update

Updated httpd packages that fix several bugs and add two enhancements 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#976465

Previously, the mod_proxy_connect module did not correctly handle signals while waiting for a backend server to close the connection. With this update, signals are ignored while processing connection closure, thus fixing the bug.

BZ#1003073

Due to a bug in the mod_proxy_http module, the "proxy: error reading response" error message was logged into the global error log even when there was a VirtualHost-specific error log configured. With this update, the aforementioned error message is logged into the correct log file.

BZ#1047319

Previously, a bug in handling the attribute values in the mod_ldap module could lead to a segmentation fault when LDAP dynamic groups were configured. The handling of attribute values has been fixed, and mod_ldap now works as intended.

BZ#1101385

Due to a bug in the lock handling in the mod_ldap module, httpd processes could enter a loop continually consuming CPU time in some LDAP configurations. A patch has been applied to correct the lock handling, and LDAP configurations now work correctly.

In addition, this update adds the following

Enhancements

BZ#1038276

The mod_authnz_ldap module can set environment variables based on LDAP attributes. However, these variables were only available when LDAP authentication was configured. With this update, environment variables are set for LDAP attributes if LDAP is used for authorization only.

BZ#1058426

A mod_ssl configuration with very large Certificate Revocation Lists (CRLs) could result in excessive memory consumption as the CRLs could be cached in the memory. A new configuration directive, "SSLDisableCRLCaching", which disables CRL caching and allows lower memory use in such configurations, has been added to mod_ssl.

Users of httpd are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. After installing the updated packages, the httpd daemon will be restarted automatically.

3.27. hwdata

3.27.1. RHEA-2014:1220 — hwdata enhancement update

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

The hwdata package contains files with hardware identification and configuration data.

Enhancement

BZ#1064366

The PCI, USB, and vendor ID files have been updated with data for the recently released hardware so it can be correctly identified by hardware identification tools.

Users of hwdata are advised to upgrade to this updated package, which adds this enhancement.

3.28. initscripts

3.28.1. RHBA-2014:1210 — initscripts bug fix and enhancement update

Updated initscripts packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

The initscripts packages contain basic system scripts to boot the system, change runlevels, activate and deactivate most network interfaces, and shut down the system cleanly.

Bug Fixes

BZ#1055573

Previously, the source code did not handle the network interface controller (NIC) coming up on layer 2 appropriately, which caused a race condition. As a consequence, the ifup-eth scripts failed to determine if a duplicate IP address existed. After this update, the user can now set a value of the "-w" option of the arping command to specify a timeout, and duplicate IP addresses are detected as expected.

BZ#836679

Prior to this update, the rc.sysinit script did not appropriately verify the conditions before executing the init_crypto() function. Consequently, a harmless error message was displayed when booting with an encrypted logical volume. With this update, rc.sysinit verifies the existence of the block devices listed in the /etc/crypttab file, and the error message no longer appears.

In addition, this update adds the following

Enhancement

BZ#662617

The bridge configuration options have been enhanced by adding a possibility to set bridge priorities and aging in a standardized way.

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

3.29. java-1.5.0-ibm

3.29.1. RHSA-2014:0136 — Important: java-1.5.0-ibm security update

Updated java-1.5.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM J2SE version 5.0 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

CVE-2013-5907, CVE-2014-0368, CVE-2014-0373, CVE-2014-0376, CVE-2014-0411, CVE-2014-0416, CVE-2014-0417, CVE-2014-0422, CVE-2014-0423, CVE-2014-0428

This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM J2SE 5.0 SR16-FP5 release. All running instances of IBM Java must be restarted for this update to take effect.

3.29.2. RHSA-2013:1509 — Important: java-1.5.0-ibm security update

Updated java-1.5.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM J2SE version 5.0 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

CVE-2013-3829, CVE-2013-4041, CVE-2013-5372, CVE-2013-5375, CVE-2013-5774, CVE-2013-5778, CVE-2013-5780, CVE-2013-5782, CVE-2013-5783, CVE-2013-5790, CVE-2013-5797, CVE-2013-5801, CVE-2013-5802, CVE-2013-5803, CVE-2013-5804, CVE-2013-5809, CVE-2013-5814, CVE-2013-5817, CVE-2013-5825, CVE-2013-5829, CVE-2013-5830, CVE-2013-5840, CVE-2013-5842, CVE-2013-5843, CVE-2013-5849

> This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM J2SE 5.0 SR16-FP4 release. All running instances of IBM Java must be restarted for this update to take effect.

3.29.3. RHSA-2014:0509 — Important: java-1.5.0-ibm security update

Updated java-1.5.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM J2SE version 5.0 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

CVE-2014-0457, CVE-2014-2421, CVE-2014-0429, CVE-2014-0446, CVE-2014-0451, CVE-2014-2427, CVE-2014-2412, CVE-2014-0460, CVE-2013-6629, CVE-2014-2401, CVE-2014-0453, CVE-2014-2398, CVE-2014-1876

> This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.5.0-ibm are advised to upgrade to these updated packages, containing the IBM J2SE 5.0 SR16-FP6 release. All running instances of IBM Java must be restarted for this update to take effect.

3.30. java-1.6.0-ibm

3.30.1. RHSA-2014:0508 — Critical: java-1.6.0-ibm security update

Updated java-1.6.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM Java SE version 6 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

CVE-2014-0457, CVE-2014-2421, CVE-2014-0429, CVE-2014-0461, CVE-2014-2428, CVE-2014-0446, CVE-2014-0452, CVE-2014-0451, CVE-2014-2423, CVE-2014-2427, CVE-2014-0458, CVE-2014-2414, CVE-2014-2412, CVE-2014-2409, CVE-2014-0460, CVE-2013-6954, CVE-2013-6629, CVE-2014-2401, CVE-2014-0449, CVE-2014-0453, CVE-2014-2398, CVE-2014-1876, CVE-2014-2420

This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM Java SE 6 SR16 release. All running instances of IBM Java must be restarted for the update to take effect.

3.30.2. RHSA-2014:0135 — Critical: java-1.6.0-ibm security update

Updated java-1.6.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM Java SE version 6 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

CVE-2013-5878, CVE-2013-5884, CVE-2013-5887, CVE-2013-5888, CVE-2013-5889, CVE-2013-5896, CVE-2013-5898, CVE-2013-5899, CVE-2013-5907, CVE-2013-5910, CVE-2014-0368, CVE-2014-0373, CVE-2014-0375, CVE-2014-0376, CVE-2014-0387, CVE-2014-0403, CVE-2014-0410, CVE-2014-0411, CVE-2014-0415, CVE-2014-0416, CVE-2014-0417, CVE-2014-0422, CVE-2014-0423, CVE-2014-0424, CVE-2014-0428

This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM Java SE 6 SR15-FP1 release. All running instances of IBM Java must be restarted for the update to take effect.

3.30.3. RHSA-2013:1508 — Critical: java-1.6.0-ibm security update

Updated java-1.6.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

IBM Java SE version 6 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit.

Security Fix

CVE-2013-3829, CVE-2013-4041, CVE-2013-5372, CVE-2013-5375, CVE-2013-5457, CVE-2013-5772, CVE-2013-5774, CVE-2013-5776, CVE-2013-5778, CVE-2013-5780, CVE-2013-5782, CVE-2013-5783, CVE-2013-5784, CVE-2013-5787, CVE-2013-5789, CVE-2013-5797, CVE-2013-5801, CVE-2013-5802, CVE-2013-5803, CVE-2013-5804, CVE-2013-5809, CVE-2013-5812, CVE-2013-5814, CVE-2013-5817, CVE-2013-5818, CVE-2013-5819, CVE-2013-5820, CVE-2013-5823, CVE-2013-5824, CVE-2013-5825, CVE-2013-5829, CVE-2013-5830, CVE-2013-5831, CVE-2013-5832, CVE-2013-5840, CVE-2013-5842, CVE-2013-5843, CVE-2013-5848, CVE-2013-5849, CVE-2013-5850, CVE-2013-5851

This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.6.0-ibm are advised to upgrade to these updated packages, containing the IBM Java SE 6 SR15 release. All running instances of IBM Java must be restarted for the update to take effect.

3.31. java-1.6.0-openjdk

3.31.1. RHSA-2014:0408 — Important: java-1.6.0-openjdk security and bug fix update

Updated java-1.6.0-openjdk packages that fix various 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 Important security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The java-1.6.0-openjdk packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Java Software Development Kit.

Security Fixes

CVE-2014-0429

An input validation flaw was discovered in the medialib library in the 2D component. A specially crafted image could trigger Java Virtual Machine memory corruption when processed. A remote attacker, or an untrusted Java application or applet, could possibly use this flaw to execute arbitrary code with the privileges of the user running the Java Virtual Machine.

CVE-2014-0456, CVE-2014-2397, CVE-2014-2421

Multiple flaws were discovered in the Hotspot and 2D components in OpenJDK. An untrusted Java application or applet could use these flaws to trigger Java Virtual Machine memory corruption and possibly bypass Java sandbox restrictions.

CVE-2014-0457, CVE-2014-0461

Multiple improper permission check issues were discovered in the Libraries component in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2014-2412, CVE-2014-0451, CVE-2014-0458, CVE-2014-2423, CVE-2014-0452, CVE-2014-2414, CVE-2014-0446, CVE-2014-2427

Multiple improper permission check issues were discovered in the AWT, JAX-WS, JAXB, Libraries, and Sound components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass certain Java sandbox restrictions.

CVE-2014-0460

Multiple flaws were identified in the Java Naming and Directory Interface (JNDI) DNS client. These flaws could make it easier for a remote attacker to perform DNS spoofing attacks.

CVE-2014-2403

It was discovered that the JAXP component did not properly prevent access to arbitrary files when a SecurityManager was present. This flaw could cause a Java application using JAXP to leak sensitive information, or affect application availability.

CVE-2014-0453

It was discovered that the Security component in OpenJDK could leak some timing information when performing PKCS#1 unpadding. This could possibly lead to the disclosure of some information that was meant to be protected by encryption.

CVE-2014-2398

It was discovered that the fix for CVE-2013-5797 did not properly resolve input sanitization flaws in javadoc. When javadoc documentation was generated from an untrusted Java source code and hosted on a domain not controlled by the code author, these issues could make it easier to perform cross-site scripting (XSS) attacks.

CVE-2014-1876

An insecure temporary file use flaw was found in the way the unpack200 utility created log files. A local attacker could possibly use this flaw to perform a symbolic link attack and overwrite arbitrary files with the privileges of the user running unpack200.

Bug Fix

BZ#1085373

The OpenJDK update to IcedTea version 1.13 introduced a regression related to the handling of the jdk_version_info variable. This variable was not properly zeroed out before being passed to the Java Virtual Machine, resulting in a memory leak in the java.lang.ref.Finalizer class. This update fixes this issue, and memory leaks no longer occur.

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.

3.31.2. RHSA-2014:0097 — Important: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

These packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Java Software Development Kit.

Security Fixes

CVE-2013-5907

An input validation flaw was discovered in the font layout engine in the 2D component. A specially crafted font file could trigger a Java Virtual Machine memory corruption when processed. An untrusted Java application or applet could possibly use this flaw to bypass Java sandbox restrictions.

CVE-2014-0428, CVE-2014-0422

Multiple improper permission check issues were discovered in the CORBA and JNDI components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2014-0373, CVE-2013-5878, CVE-2013-5910, CVE-2013-5896, CVE-2013-5884, CVE-2014-0416, CVE-2014-0376, CVE-2014-0368

Multiple improper permission check issues were discovered in the Serviceability, Security, CORBA, JAAS, JAXP, and Networking components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass certain Java sandbox restrictions.

CVE-2014-0423

It was discovered that the Beans component did not restrict processing of XML external entities. This flaw could cause a Java application using Beans to leak sensitive information, or affect application availability.

CVE-2014-0411

It was discovered that the JSSE component could leak timing information during the TLS/SSL handshake. This could possibly lead to a disclosure of information about the used encryption keys.

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.

3.31.3. RHSA-2013:1505 — Important: java-1.6.0-openjdk security update

Updated java-1.6.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 5 and 6.

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

The java-1.6.0-openjdk packages provide the OpenJDK 6 Java Runtime Environment and the OpenJDK 6 Java Software Development Kit.

Security Fixes

CVE-2013-5782

Multiple input checking flaws were found in the 2D component native image parsing code. A specially crafted image file could trigger a Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with the privileges of the user running the Java Virtual Machine.

CVE-2013-5830

The class loader did not properly check the package access for non-public proxy classes. A remote attacker could possibly use this flaw to execute arbitrary code with the privileges of the user running the Java Virtual Machine.

CVE-2013-5829, CVE-2013-5814, CVE-2013-5817, CVE-2013-5842, CVE-2013-5850

Multiple improper permission check issues were discovered in the 2D, CORBA, JNDI, and Libraries components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-5809

Multiple input checking flaws were discovered in the JPEG image reading and writing code in the 2D component. An untrusted Java application or applet could use these flaws to corrupt the Java Virtual Machine memory and bypass Java sandbox restrictions.

CVE-2013-5802

The FEATURE_SECURE_PROCESSING setting was not properly honored by the javax.xml.transform package transformers. A remote attacker could use this flaw to supply a crafted XML that would be processed without the intended security restrictions.

CVE-2013-5825, CVE-2013-4002, CVE-2013-5823

Multiple errors were discovered in the way the JAXP and Security components processes XML inputs. A remote attacker could create a crafted XML that would cause a Java application to use an excessive amount of CPU and memory when processed.

CVE-2013-3829, CVE-2013-5840, CVE-2013-5774, CVE-2013-5783, CVE-2013-5820, CVE-2013-5849, CVE-2013-5790, CVE-2013-5784

Multiple improper permission check issues were discovered in the Libraries, Swing, JAX-WS, JGSS, AWT, Beans, and Scripting components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass certain Java sandbox restrictions.

CVE-2013-5778

It was discovered that the 2D component image library did not properly check bounds when performing image conversions. An untrusted Java application or applet could use this flaw to disclose portions of the Java Virtual Machine memory.

CVE-2013-5804, CVE-2013-5797

Multiple input sanitization flaws were discovered in javadoc. When javadoc documentation was generated from an untrusted Java source code and hosted on a domain not controlled by the code author, these issues could make it easier to perform cross-site scripting attacks.

CVE-2013-5780

Various OpenJDK classes that represent cryptographic keys could leak private key information by including sensitive data in strings returned by toString() methods. These flaws could possibly lead to an unexpected exposure of sensitive key data.

CVE-2013-5772

The Java Heap Analysis Tool (jhat) failed to properly escape all data added into the HTML pages it generated. Crafted content in the memory of a Java program analyzed using jhat could possibly be used to conduct cross-site scripting attacks.

CVE-2013-5803

> The Kerberos implementation in OpenJDK did not properly parse KDC responses. A malformed packet could cause a Java application using JGSS to exit.

All users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

3.31.4. RHEA-2014:0116 — java-1.6.0-openjdk enhancement update

Updated java-1.6.0-openjdk packages that add an enhancement 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.

Enhancement

BZ#1059178

> An expired GlobalSign Certification Authority certificate was replaced by an updated certificate in the /usr/lib/jvm/java-1.6.0-openjdk-1.6.0.0[.x86_64]/jre/lib/security/cacerts file, which contains the certificates of trusted certification authorities.

Users of java-1.6.0-openjdk are advised to upgrade to these updated packages, which provide this enhancement. All running instances of OpenJDK Java must be restarted for the update to take effect.

3.32. java-1.7.0-ibm

3.32.1. RHSA-2014:0134 — Critical: java-1.7.0-ibm security update

Updated java-1.7.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

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

Security Fix

CVE-2013-5878, CVE-2013-5884, CVE-2013-5887, CVE-2013-5888, CVE-2013-5889, CVE-2013-5896, CVE-2013-5898, CVE-2013-5899, CVE-2013-5907, CVE-2013-5910, CVE-2014-0368, CVE-2014-0373, CVE-2014-0375, CVE-2014-0376, CVE-2014-0387, CVE-2014-0403, CVE-2014-0410, CVE-2014-0411, CVE-2014-0415, CVE-2014-0416, CVE-2014-0417, CVE-2014-0422, CVE-2014-0423, CVE-2014-0424, CVE-2014-0428

> This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.7.0-ibm are advised to upgrade to these updated packages, containing the IBM Java SE 7 SR6-FP1 release. All running instances of IBM Java must be restarted for the update to take effect.

3.32.2. RHSA-2013:1507 — Critical: java-1.7.0-ibm security update

Updated java-1.7.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

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

Security Fix

CVE-2013-3829, CVE-2013-4041, CVE-2013-5372, CVE-2013-5375, CVE-2013-5456, CVE-2013-5457, CVE-2013-5458, CVE-2013-5772, CVE-2013-5774, CVE-2013-5776, CVE-2013-5778, CVE-2013-5780, CVE-2013-5782, CVE-2013-5783, CVE-2013-5784, CVE-2013-5787, CVE-2013-5788, CVE-2013-5789, CVE-2013-5790, CVE-2013-5797, CVE-2013-5800, CVE-2013-5801, CVE-2013-5802, CVE-2013-5803, CVE-2013-5804, CVE-2013-5809, CVE-2013-5812, CVE-2013-5814, CVE-2013-5817, CVE-2013-5818, CVE-2013-5819, CVE-2013-5820, CVE-2013-5823, CVE-2013-5824, CVE-2013-5825, CVE-2013-5829, CVE-2013-5830, CVE-2013-5831, CVE-2013-5832, CVE-2013-5838, CVE-2013-5840, CVE-2013-5842, CVE-2013-5843, CVE-2013-5848, CVE-2013-5849, CVE-2013-5850, CVE-2013-5851

> This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.7.0-ibm are advised to upgrade to these updated packages, containing the IBM Java SE 7 SR6 release. All running instances of IBM Java must be restarted for the update to take effect.

3.32.3. RHSA-2014:0486 — Critical: java-1.7.0-ibm security update

Updated java-1.7.0-ibm packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

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

Security Fix

CVE-2014-0457, CVE-2014-2421, CVE-2014-0429, CVE-2014-0461, CVE-2014-0455, CVE-2014-2428, CVE-2014-0448, CVE-2014-0454, CVE-2014-0446, CVE-2014-0452, CVE-2014-0451, CVE-2014-2402, CVE-2014-2423, CVE-2014-2427, CVE-2014-0458, CVE-2014-2414, CVE-2014-2412, CVE-2014-2409, CVE-2014-0460, CVE-2013-6954, CVE-2013-6629, CVE-2014-2401, CVE-2014-0449, CVE-2014-0459, CVE-2014-0453, CVE-2014-2398, CVE-2014-1876, CVE-2014-2420

> This update fixes several vulnerabilities in the IBM Java Runtime Environment and the IBM Java Software Development Kit. Detailed vulnerability descriptions are linked from the IBM Security alerts page.

All users of java-1.7.0-ibm are advised to upgrade to these updated packages, containing the IBM Java SE 7 SR7 release. All running instances of IBM Java must be restarted for the update to take effect.

3.33. java-1.7.0-openjdk

3.33.1. RHSA-2014:0407 — Important: java-1.7.0-openjdk security update

Updated java-1.7.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 5.

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

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

Security Fixes

CVE-2014-0429

An input validation flaw was discovered in the medialib library in the 2D component. A specially crafted image could trigger Java Virtual Machine memory corruption when processed. A remote attacker, or an untrusted Java application or applet, could possibly use this flaw to execute arbitrary code with the privileges of the user running the Java Virtual Machine.

CVE-2014-0456, CVE-2014-2397, CVE-2014-2421

Multiple flaws were discovered in the Hotspot and 2D components in OpenJDK. An untrusted Java application or applet could use these flaws to trigger Java Virtual Machine memory corruption and possibly bypass Java sandbox restrictions.

CVE-2014-0457, CVE-2014-0455, CVE-2014-0461

Multiple improper permission check issues were discovered in the Libraries component in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2014-2412, CVE-2014-0451, CVE-2014-0458, CVE-2014-2423, CVE-2014-0452, CVE-2014-2414, CVE-2014-2402, CVE-2014-0446, CVE-2014-2413, CVE-2014-0454, CVE-2014-2427, CVE-2014-0459

Multiple improper permission check issues were discovered in the AWT, JAX-WS, JAXB, Libraries, Security, Sound, and 2D components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass certain Java sandbox restrictions.

CVE-2014-0460

Multiple flaws were identified in the Java Naming and Directory Interface (JNDI) DNS client. These flaws could make it easier for a remote attacker to perform DNS spoofing attacks.

CVE-2014-2403

It was discovered that the JAXP component did not properly prevent access to arbitrary files when a SecurityManager was present. This flaw could cause a Java application using JAXP to leak sensitive information, or affect application availability.

CVE-2014-0453

It was discovered that the Security component in OpenJDK could leak some timing information when performing PKCS#1 unpadding. This could possibly lead to the disclosure of some information that was meant to be protected by encryption.

CVE-2014-2398

It was discovered that the fix for CVE-2013-5797 did not properly resolve input sanitization flaws in javadoc. When javadoc documentation was generated from an untrusted Java source code and hosted on a domain not controlled by the code author, these issues could make it easier to perform cross-site scripting (XSS) attacks.

CVE-2014-1876

An insecure temporary file use flaw was found in the way the unpack200 utility created log files. A local attacker could possibly use this flaw to perform a symbolic link attack and overwrite arbitrary files with the privileges of the user running unpack200.

All users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

3.33.2. RHSA-2014:0027 — Important: java-1.7.0-openjdk security update

Updated java-1.7.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 5.

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

These packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Software Development Kit.

Security Fixes

CVE-2013-5907

An input validation flaw was discovered in the font layout engine in the 2D component. A specially crafted font file could trigger Java Virtual Machine memory corruption when processed. An untrusted Java application or applet could possibly use this flaw to bypass Java sandbox restrictions.

CVE-2014-0428, CVE-2014-0422, CVE-2013-5893

Multiple improper permission check issues were discovered in the CORBA, JNDI, and Libraries components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2014-0373, CVE-2013-5878, CVE-2013-5910, CVE-2013-5896, CVE-2013-5884, CVE-2014-0416, CVE-2014-0376, CVE-2014-0368

Multiple improper permission check issues were discovered in the Serviceability, Security, CORBA, JAAS, JAXP, and Networking components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass certain Java sandbox restrictions.

CVE-2014-0423

It was discovered that the Beans component did not restrict processing of XML external entities. This flaw could cause a Java application using Beans to leak sensitive entities. This flaw could cause a Java application using Beans to leak sensitive information, or affect application availability.

CVE-2014-0411

It was discovered that the JSSE component could leak timing information during the TLS/SSL handshake. This could possibly lead to disclosure of information about the used encryption keys.

All users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

3.33.3. RHSA-2013:1447 — Important: java-1.7.0-openjdk security update

Updated java-1.7.0-openjdk packages that fix various security issues are now available for Red Hat Enterprise Linux 5.

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

These packages provide the OpenJDK 7 Java Runtime Environment and the OpenJDK 7 Software Development Kit.

Security Fixes

CVE-2013-5782

Multiple input checking flaws were found in the 2D component native image parsing code. A specially crafted image file could trigger a Java Virtual Machine memory corruption and, possibly, lead to arbitrary code execution with the privileges of the user running the Java Virtual Machine.

CVE-2013-5830

The class loader did not properly check the package access for non-public proxy classes. A remote attacker could possibly use this flaw to execute arbitrary code with the privileges of the user running the Java Virtual Machine.

CVE-2013-5829, CVE-2013-5814, CVE-2013-5817, CVE-2013-5842, CVE-2013-5850, CVE-2013-5838

Multiple improper permission check issues were discovered in the 2D, CORBA, JNDI, and Libraries components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass Java sandbox restrictions.

CVE-2013-5809

Multiple input checking flaws were discovered in the JPEG image reading and writing code in the 2D component. An untrusted Java application or applet could use these flaws to corrupt the Java Virtual Machine memory and bypass Java sandbox restrictions.

CVE-2013-5802

The FEATURE_SECURE_PROCESSING setting was not properly honored by the javax.xml.transform package transformers. A remote attacker could use this flaw to supply a crafted XML that would be processed without the intended security restrictions.

CVE-2013-5825, CVE-2013-4002, CVE-2013-5823

Multiple errors were discovered in the way the JAXP and Security components processes XML inputs. A remote attacker could create a crafted XML that would cause a Java application to use an excessive amount of CPU and memory when processed.

CVE-2013-3829, CVE-2013-5840, CVE-2013-5774, CVE-2013-5783, CVE-2013-5820, CVE-2013-5851, CVE-2013-5800, CVE-2013-5849, CVE-2013-5790, CVE-2013-5784

Multiple improper permission check issues were discovered in the Libraries, Swing, JAX-WS, JAXP, JGSS, AWT, Beans, and Scripting components in OpenJDK. An untrusted Java application or applet could use these flaws to bypass certain Java sandbox restrictions.

CVE-2013-5778

It was discovered that the 2D component image library did not properly check bounds when performing image conversions. An untrusted Java application or applet could use this flaw to disclose portions of the Java Virtual Machine memory.

CVE-2013-5804, CVE-2013-5797

Multiple input sanitization flaws were discovered in javadoc. When javadoc documentation was generated from an untrusted Java source code and hosted on a domain not controlled by the code author, these issues could make it easier to perform cross-site scripting attacks.

CVE-2013-5780

Various OpenJDK classes that represent cryptographic keys could leak private key information by including sensitive data in strings returned by toString() methods. These flaws could possibly lead to an unexpected exposure of sensitive key data.

CVE-2013-5772

The Java Heap Analysis Tool (jhat) failed to properly escape all data added into the HTML pages it generated. Crafted content in the memory of a Java program analyzed using jhat could possibly be used to conduct cross-site scripting attacks.

CVE-2013-5803

The Kerberos implementation in OpenJDK did not properly parse KDC responses. A malformed packet could cause a Java application using JGSS to exit.

All users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which resolve these issues. All running instances of OpenJDK Java must be restarted for the update to take effect.

3.33.4. RHEA-2014:0115 — java-1.7.0-openjdk enhancement update

Updated java-1.7.0-openjdk packages that add an enhancement 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 Software Development Kit.

Enhancement

BZ#1059179

An expired GlobalSign Certification Authority certificate was replaced by an updated certificate in the /usr/lib/jvm/java-1.7.0-openjdk-1.7.0.51[.x86_64]/jre/lib/security/cacerts file, which contains the certificates of trusted certification authorities.

Users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which add this enhancement. All running instances of OpenJDK Java must be restarted for the update to take effect.

3.33.5. RHBA-2014:0571 — java-1.7.0-openjdk bug fix update

Updated java-1.7.0-openjdk packages that fix one bug 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.

Bug Fix

BZ#1101263

> Prior to this update, an error in the SSL socket code caused the write() and close() calls to be invoked simultaneously on the same socket, but in two different threads. As a consequence, the socket entered a deadlock. With this update, a measure has been implemented to ensure that calls to close() and read() do not interfere with each other, and the deadlock no longer occurs.

Users of java-1.7.0-openjdk are advised to upgrade to these updated packages, which fix this bug. All running instances of OpenJDK Java must be restarted for the update to take effect.

3.34. java-1.7.0-oracle

3.34.1. RHSA-2014:0030 — Critical: java-1.7.0-oracle security update

Updated java-1.7.0-oracle packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

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

Security Fix

CVE-2013-5870, CVE-2013-5878, CVE-2013-5884, CVE-2013-5887, CVE-2013-5888, CVE-2013-5889, CVE-2013-5893, CVE-2013-5895, CVE-2013-5896, CVE-2013-5898, CVE-2013-5899, CVE-2013-5902, CVE-2013-5904, CVE-2013-5905, CVE-2013-5906, CVE-2013-5907, CVE-2013-5910, CVE-2014-0368, CVE-2014-0373, CVE-2014-0375, CVE-2014-0376, CVE-2014-0382, CVE-2014-0387, CVE-2014-0403, CVE-2014-0410, CVE-2014-0411, CVE-2014-0415, CVE-2014-0416, CVE-2014-0417, CVE-2014-0418, CVE-2014-0422, CVE-2014-0423, CVE-2014-0424, CVE-2014-0428

> This update fixes several vulnerabilities in the Oracle Java Runtime Environment and the Oracle Java Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch Update Advisory page.

All users of java-1.7.0-oracle are advised to upgrade to these updated packages, which provide Oracle Java 7 Update 51 and resolve these issues. All running instances of Oracle Java must be restarted for the update to take effect.

3.34.2. RHSA-2014:0412 — Critical: java-1.7.0-oracle security update

Updated java-1.7.0-oracle packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

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

Security Fix

CVE-2013-6629, CVE-2013-6954, CVE-2014-0429, CVE-2014-0432, CVE-2014-0446, CVE-2014-0448, CVE-2014-0449, CVE-2014-0451, CVE-2014-0452, CVE-2014-0453, CVE-2014-0454, CVE-2014-0455, CVE-2014-0456, CVE-2014-0457, CVE-2014-0458, CVE-2014-0459, CVE-2014-0460, CVE-2014-0461, CVE-2014-1876, CVE-2014-2397, CVE-2014-2398, CVE-2014-2401, CVE-2014-2402, CVE-2014-2403, CVE-2014-2409, CVE-2014-2412, CVE-2014-2413, CVE-2014-2414, CVE-2014-2420, CVE-2014-2421, CVE-2014-2422, CVE-2014-2423, CVE-2014-2427, CVE-2014-2428

This update fixes several vulnerabilities in the Oracle Java Runtime Environment and the Oracle Java Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch Update Advisory page.

All users of java-1.7.0-oracle are advised to upgrade to these updated packages, which provide Oracle Java 7 Update 55 and resolve these issues. All running instances of Oracle Java must be restarted for the update to take effect.

3.34.3. RHSA-2013:1440 — Critical: java-1.7.0-oracle security update

Updated java-1.7.0-oracle packages that fix several security issues are now available for Red Hat Enterprise Linux 5 and 6 Supplementary.

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

[Updated 23rd October 2013] The package list in this erratum has been updated to make the packages available in the Red Hat Enterprise Linux 5 Desktop Supplementary channels on the Red Hat Network.

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

Security Fix

CVE-2013-3829, CVE-2013-4002, CVE-2013-5772, CVE-2013-5774, CVE-2013-5775, CVE-2013-5776, CVE-2013-5777, CVE-2013-5778, CVE-2013-5780, CVE-2013-5782, CVE-2013-5783, CVE-2013-5784, CVE-2013-5787, CVE-2013-5788, CVE-2013-5789, CVE-2013-5790, CVE-2013-5797, CVE-2013-5800, CVE-2013-5801, CVE-2013-5802, CVE-2013-5803, CVE-2013-5804, CVE-2013-5809, CVE-2013-5810, CVE-2013-5812, CVE-2013-5814, CVE-2013-5817, CVE-2013-5818, CVE-2013-5819, CVE-2013-5820, CVE-2013-5823, CVE-2013-5824, CVE-2013-5825, CVE-2013-5829, CVE-2013-5830, CVE-2013-5831, CVE-2013-5832, CVE-2013-5838, CVE-2013-5840, CVE-2013-5842, CVE-2013-5843, CVE-2013-5844, CVE-2013-5846, CVE-2013-5848, CVE-2013-5849, CVE-2013-5850, CVE-2013-5851, CVE-2013-5852, CVE-2013-5854

> This update fixes several vulnerabilities in the Oracle Java Runtime Environment and the Oracle Java Software Development Kit. Further information about these flaws can be found on the Oracle Java SE Critical Patch Update Advisory page.

All users of java-1.7.0-oracle are advised to upgrade to these updated packages, which provide Oracle Java 7 Update 45 and resolve these issues. All running instances of Oracle Java must be restarted for the update to take effect.

3.34.4. RHSA-2014:0477 — Oracle Java SE - Notification of Removal from Supplementary Channel

Oracle Java SE packages will be moved from the Red Hat Enterprise Linux 5 and 6 Supplementary Red Hat Network (RHN) channels to the Oracle Java for Red Hat Enterprise Linux 5 and 6 RHN channels.

Oracle Java SE development (JDK) and runtime (JRE) software packages will be removed from the Red Hat Enterprise Linux Supplementary media and RHN channels. These packages will be relocated to a new set of channels that are dedicated to delivering Oracle Java software. Customers are advised to reconfigure their systems to use the new channels to ensure that they are receiving the latest updates to Oracle Java software.

Oracle Java software packages will be removed from Red Hat Enterprise Linux Supplementary media and RHN channels on May 8, 2014. Oracle Java will be available for online download via the new RHN channels.

This change affects the following packages:

- Oracle Java SE 5 (java-1.5.0-sun)
- Oracle Java SE 6 (java-1.6.0-sun)
- Oracle Java SE 7 (java-1.7.0-oracle)

Red Hat Enterprise Linux includes OpenJDK as the default Java development and runtime environment. Java development and runtime is also available from IBM via the Supplementary media and RHN channels. Access to OpenJDK and IBM JDK are not affected by this change.

Users are required to enable the new repository on their systems to access Oracle Java software. Refer to Red Hat Customer Portal Knowledgebase Solution 732883 for instructions on how to subscribe your systems to the new Oracle Java RHN channels.

3.35. kdelibs

3.35.1. RHEA-2014:0165 — kdelibs enhancement update

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

The kdelibs packages contain a set of common libraries used by all applications written for the K Desktop Environment (KDE).

Enhancement

BZ#1063294

After this update, kdelibs is no longer maintaining its own list of GlobalSign Certification Authority (CA) certificate certificates. The expired kdelibs CA certificate has been replaced by an updated certificate from the openssl package in the /etc/pki/tls/certs/ca-bundle.crt file, which contains the certificates of trusted certification authorities.

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

3.35.2. RHBA-2014:1227 — kdelibs bug fix update

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

The kdelibs packages provide libraries for the K Desktop Environment (KDE).

Bug Fixes

BZ#1045457

Previously, the "up arrow" key triggered the KSnapshot tool on a konsole window instead of displaying command history. A patch has been applied to fix this bug, and when pressed on konsole screen, the "up arrow" key now displays the command history.

BZ#1058930

Prior to this update, the /usr/share/apps/kssl/ca-bundle.crt file contained an expired "GlobalSign Root CA" entry. The old ca-bundle.crt has been replaced with ca-bundle.crt from the openssl rpm, thus fixing this bug.

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

3.36. kernel

3.36.1. RHSA-2014:0433 — Moderate: kernel security, bug fix, and enhancement update

Updated kernel packages that fix two 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 scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

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

Security Fixes

CVE-2012-6638, Moderate

A flaw was found in the way the Linux kernel's TCP/IP protocol suite implementation handled TCP packets with both the SYN and FIN flags set. A remote attacker could use this flaw to consume an excessive amount of resources on the target system, potentially resulting in a denial of service.

CVE-2013-2888, Moderate

* A flaw was found in the way the Linux kernel handled HID (Human Interface Device) reports with an out-of-bounds Report ID. An attacker with physical access to the system could use this flaw to crash the system or, potentially, escalate their privileges on the system.

Bug Fixes

BZ#1073731

A previous change to the sunrpc code introduced a race condition between the rpc_wake_up_task() and rpc_wake_up_status() functions. A race between threads operating on these functions could result in a deadlock situation, subsequently triggering a "soft lockup" event and rendering the system unresponsive. This problem has been fixed by re-ordering tasks in the RPC wait queue.

BZ#1073953

Running a process in the background on a GFS2 file system could sometimes trigger a glock recursion error that resulted in a kernel panic. This happened when a readpage operation attempted to take a glock that had already been held by another function. To prevent this error, GFS2 now verifies whether the glock is already held when performing the readpage operation.

BZ#1077045

A previous patch backport to the IUCV (Inter User Communication Vehicle) code was incomplete. Consequently, when establishing an IUCV connection, the kernel could, under certain circumstances, dereference a NULL pointer, resulting in a kernel panic. A patch has been applied to correct this problem by calling the proper function when removing IUCV paths.

In addition, this update adds the following

Enhancement

BZ#1073123

The lpfc driver had a fixed timeout of 60 seconds for SCSI task management commands. With this update, the lpfc driver enables the user to set this timeout within the range from 5 to 180 seconds. The timeout can be changed by modifying the "lpfc_task_mgmt_tmo" parameter for the lpfc driver.

All kernel users are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement. The system must be rebooted for this update to take effect.

3.36.2. RHSA-2014:0108 — Moderate: kernel security and bug fix update

Updated kernel packages that fix one security issue and three bugs are now available for Red Hat Enterprise Linux 5.

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

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

Security Fix

CVE-2013-4494, Moderate

It was found that the Xen hypervisor did not always lock 'page_alloc_lock' and 'grant_table.lock' in the same order. This could potentially lead to a deadlock. A malicious guest administrator could use this flaw to cause a denial of service on the host.

Red Hat would like to thank the Xen project for reporting this issue.

Bug Fixes

BZ#1029865

A recent patch to the CIFS code that introduced the NTLMSSP (NT LAN Manager Security Support Provider) authentication mechanism caused a regression in CIFS behavior. As a result of the regression, an encryption key that is returned during the SMB negotiation protocol response was only used for the first session that was created on the SMB client. Any subsequent mounts to the same server did not use the encryption key returned by the initial negotiation with the server. As a consequence, it was impossible to mount multiple SMB shares with different credentials to the same server. A patch has been applied to correct this problem so that an encryption key or a server challenge is now provided for every SMB session during the SMB negotiation protocol response.

BZ#1041694

The igb driver previously used a 16-bit mask when writing values of the flow control high-water mark to hardware registers on a network device. Consequently, the values were truncated on some network devices, disrupting the flow control. A patch has been applied to the igb driver so that it now uses a 32-bit mask as expected.

BZ#1049731

The IPMI driver did not properly handle kernel panic messages. Consequently, when a kernel panic occurred on a system that was utilizing IPMI without Kdump being set up, a second kernel panic could be triggered. A patch has been applied to the IPMI driver to fix this problem, and a message handler now properly waits for a response to panic event messages.

Red Hat would like to thank the Xen project for reporting this issue.

All kernel users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

3.36.3. RHSA-2013:1449 — Moderate: kernel security and bug fix update

Updated kernel 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. 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-2013-0343, Moderate

A flaw was found in the way the Linux kernel handled the creation of temporary IPv6 addresses. If the IPv6 privacy extension was enabled

(/proc/sys/net/ipv6/conf/eth0/use_tempaddr is set to '2'), an attacker on the local network could disable IPv6 temporary address generation, leading to a potential information disclosure.

CVE-2013-4299, Moderate

* An information leak flaw was found in the way Linux kernel's device mapper subsystem, under certain conditions, interpreted data written to snapshot block devices. An attacker could use this flaw to read data from disk blocks in free space, which are normally inaccessible.

CVE-2013-4345, Moderate

* An off-by-one flaw was found in the way the ANSI CPRNG implementation in the Linux kernel processed non-block size aligned requests. This could lead to random numbers being generated with less bits of entropy than expected when ANSI CPRNG was used.

CVE-2013-4368, Moderate

* An information leak flaw was found in the way Xen hypervisor emulated the OUTS instruction for 64-bit paravirtualized guests. A privileged guest user could use this flaw to leak hypervisor stack memory to the guest.

Red Hat would like to thank Fujitsu for reporting CVE-2013-4299, Stephan Mueller for reporting CVE-2013-4345, and the Xen project for reporting CVE-2013-4368.

Bug Fix

BZ#1014714

A bug in the GFS2 code prevented glock work queues from freeing glock-related memory while the glock memory shrinker repeatedly queued a large number of demote requests, for example when performing a simultaneous backup of several live GFS2 volumes with a large file count. As a consequence, the glock work queues became overloaded which resulted in a high CPU usage and the GFS2 file systems being unresponsive for a significant amount of time. A patch has been applied to alleviate this problem by calling the yield() function after scheduling a certain amount of tasks on the glock work queues. The problem can now occur only with extremely high work loads.

Red Hat would like to thank Fujitsu for reporting CVE-2013-4299, Stephan Mueller for reporting CVE-2013-4345, and the Xen project for reporting CVE-2013-4368.

All kernel users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

3.36.4. RHSA-2014:0740 — Important: kernel security and bug fix update

Updated kernel packages that fix three security issues and several bugs are now available for Red Hat Enterprise Linux 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-2014-1737, Important

A flaw was found in the way the Linux kernel's floppy driver handled user space provided data in certain error code paths while processing FDRAWCMD IOCTL commands. A local user with write access to /dev/fdX could use this flaw to free (using the kfree() function) arbitrary kernel memory.

CVE-2014-1738, Low

* It was found that the Linux kernel's floppy driver leaked internal kernel memory addresses to user space during the processing of the FDRAWCMD IOCTL command. A local user with write access to /dev/fdX could use this flaw to obtain information about the kernel heap arrangement.

CVE-2014-1737, CVE-2014-1738

Note: A local user with write access to /dev/fdX could use these two flaws

CVE-2013-7339, Moderate

to escalate their privileges on the system.

* A NULL pointer dereference flaw was found in the rds_ib_laddr_check() function in the Linux kernel's implementation of Reliable Datagram Sockets (RDS). A local, unprivileged user could use this flaw to crash the system.

Red Hat would like to thank Matthew Daley for reporting CVE-2014-1737 and CVE-2014-1738.

Bug Fixes

BZ#1091832

A bug in the futex system call could result in an overflow when passing a very large positive timeout. As a consequence, the FUTEX_WAIT operation did not work as intended and the system call was timing out immediately. A backported patch fixes this bug by limiting very large positive timeouts to the maximal supported value.

BZ#1092869

A new Linux Security Module (LSM) functionality related to the setrlimit hooks should produce a warning message when used by a third party module that could not cope with it. However, due to a programming error, the kernel could print this warning message when a process was setting rlimits for a different process, or if rlimits were modified by another than the main thread even though there was no incompatible third party module. This update fixes the relevant code and ensures that the kernel handles this warning message correctly.

BZ#1094152

Previously, the kernel was unable to detect KVM on system boot if the Hyper-V emulation was enabled. A patch has been applied to ensure that both KVM and Hyper-V hypervisors are now correctly detected during system boot.

BZ#1095062

A function in the RPC code responsible for verifying whether cached credentials match the current process did not perform the check correctly. The code checked only whether the groups in the current process credentials appear in the same order as in the cached credentials but did not ensure that no other groups are present in the cached credentials. As a consequence, when accessing files in NFS mounts, a process with the same UID and

GID as the original process but with a non-matching group list could have been granted an unauthorized access to a file, or under certain circumstances, the process could have been wrongly prevented from accessing the file. The incorrect test condition has been fixed and the problem can no longer occur.

BZ#1096061

When being under heavy load, some Fibre Channel storage devices, such as Hitachi and HP Open-V series, can send a logout (LOGO) message to the host system. However, due to a bug in the lpfc driver, this could result in a loss of active paths to the storage and the paths could not be recovered without manual intervention. This update corrects the lpfc driver to ensure automatic recovery of the lost paths to the storage in this scenario.

Red Hat would like to thank Matthew Daley for reporting CVE-2014-1737 and CVE-2014-1738.

All kernel users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

3.36.5. RHSA-2013:1790 — Moderate: 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

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

Security Fix

CVE-2013-4355, Moderate

An information leak flaw was found in the way the Xen hypervisor handled error conditions when reading guest memory during certain guest-originated operations, such as port or memory mapped I/O writes. A privileged user in a fully-virtualized guest could use this flaw to leak hypervisor stack memory to a guest.

Red Hat would like to thank the Xen project for reporting this issue.

Bug Fixes

BZ#1014715

A previous fix to the kernel did not contain a memory barrier in the percpu_up_write() function. Consequently, under certain circumstances, a race condition could occur leading to memory corruption and a subsequent kernel panic. This update introduces a new memory barrier pair, light_mb() and heavy_mb(), for per-CPU basis read and write semaphores (percpu-rw-semaphores) ensuring that the race condition can no longer occur. In addition, the read path performance of "percpu-rw-semaphores" has been improved.

BZ#1014973

Due to a bug in the tg3 driver, systems that had the Wake-on-LAN (WOL) feature enabled on their NICs could not have been woken up from suspension or hibernation using WOL. A missing pci_wake_from_d3() function call has been added to the tg3 driver, which ensures that WOL functions properly by setting the PME_ENABLE bit.

BZ#1018458

Due to an incorrect test condition in the mpt2sas driver, the driver was unable to catch failures to map a SCSI scatter-gather list. The test condition has been corrected so that the mpt2sas driver now handles SCSI scatter-gather mapping failures as expected.

BZ#1023348

A previous patch to the kernel introduced the "VLAN tag re-insertion" workaround to resolve a problem with incorrectly handled VLAN-tagged packets with no assigned VLAN group while the be2net driver was in promiscuous mode. However, this solution led to packet corruption and a subsequent kernel oops if such a processed packed was a GRO packet. Therefore, a patch has been applied to restrict VLAN tag re-insertion only to non-GRO packets. The be2net driver now processes VLAN-tagged packets with no assigned VLAN group correctly in this situation.

Red Hat would like to thank the Xen project for reporting this issue.

All kernel users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. The system must be rebooted for this update to take effect.

3.36.6. RHSA-2014:0285 — Important: kernel security, bug fix, and enhancement update

Updated kernel packages that fix multiple security issues, several bugs, and add one enhancement are now available for Red Hat Enterprise Linux 5.

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

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

Security Fixes

CVE-2013-6381, Important

A buffer overflow flaw was found in the way the qeth_snmp_command() function in the Linux kernel's QETH network device driver implementation handled SNMP IOCTL requests with an out-of-bounds length. A local, unprivileged user could use this flaw to crash the system or, potentially, escalate their privileges on the system.

CVE-2013-4483, Moderate

* A flaw was found in the way the ipc_rcu_putref() function in the Linux kernel's IPC implementation handled reference counter decrementing. A local, unprivileged user could use this flaw to trigger an Out of Memory (OOM) condition and, potentially, crash the system.

CVE-2013-4554, Moderate

* It was found that the Xen hypervisor implementation did not correctly check privileges of hypercall attempts made by HVM guests, allowing hypercalls to be invoked from protection rings 1 and 2 in addition to ring 0. A local attacker in an HVM guest able to execute code on privilege levels 1 and 2 could potentially use this flaw to further escalate their privileges in that guest. Note: Xen HVM guests running unmodified versions of Red Hat Enterprise Linux and Microsoft Windows are not affected by this issue because they are known to only use protection rings 0 (kernel) and 3 (userspace).

CVE-2013-6383, Moderate

> * A flaw was found in the way the Linux kernel's Adaptec RAID controller (aacraid) checked permissions of compat IOCTLs. A local attacker could use this flaw to bypass intended security restrictions.

CVE-2013-6885, Moderate

> * It was found that, under specific circumstances, a combination of write operations to write-combined memory and locked CPU instructions may cause a core hang on certain AMD CPUs (for more information, refer to AMD CPU erratum 793). A privileged user in a guest running under the Xen hypervisor could use this flaw to cause a denial of service on the host system. This update adds a workaround to the Xen hypervisor implementation, which mitigates the AMD CPU issue. Note: this issue only affects AMD Family 16h Models 00h-0Fh Processors. Non-AMD CPUs are not vulnerable.

CVE-2013-7263, Low

> * It was found that certain protocol handlers in the Linux kernel's networking implementation could set the addr_len value without initializing the associated data structure. A local, unprivileged user could use this flaw to leak kernel stack memory to user space using the recvmsg, recvfrom, and recvmmsg system calls.

CVE-2013-2929, Low

> * A flaw was found in the way the get_dumpable() function return value was interpreted in the ptrace subsystem of the Linux kernel. When 'fs.suid_dumpable' was set to 2, a local, unprivileged local user could use this flaw to bypass intended ptrace restrictions and obtain potentially sensitive information.

Red Hat would like to thank Vladimir Davydov of Parallels for reporting CVE-2013-4483 and the Xen project for reporting CVE-2013-4554 and CVE-2013-6885. Upstream acknowledges Jan Beulich as the original reporter of CVE-2013-4554 and CVE-2013-6885.

This update also fixes several bugs and adds one enhancement. Documentation for these changes is available in the Technical Notes.

All kernel users are advised to upgrade to these updated packages, which contain backported patches to correct these issues and add this enhancement. The system must be rebooted for this update to take effect.

3.36.7. RHBA-2014:1196 — Red Hat Enterprise Linux 5 kernel update

Updated *kernel* packages that fix several bugs, and add various enhancements are now available as part of the ongoing support and maintenance of Red Hat Enterprise Linux version 5. This is the eleventh regular update.

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

Bug fixes

BZ#1026388

> A previous patch backport to the IUCV (Inter User Communication Vehicle) code was incomplete. Consequently, when establishing an IUCV connection, the kernel could, under certain circumstances, dereference a NULL pointer, resulting in a kernel panic. A patch has been applied to correct this problem by calling the proper function when removing IUCV paths.

BZ#1013469

Due to a bug in the cifs module, the calculation of the number of virtual circuits was handled incorrectly when establishing SMB sessions. As a consequence in environments with multiple TCP connections between the same SMB client and SMB server, each time a TCP connection was established, all other TCP connections from the client to the server were reset, resulting in an endless loop. With this update, the number of virtual circuits is constantly set to 1, which ensures the correct behavior of the cifs module in this situation.

BZ#1036115

The igb driver previously used a 16-bit mask when writing values of the flow control high-water mark to hardware registers on a network device. Consequently, the values were truncated on some network devices, disrupting the flow control. A patch has been applied to the igb driver so that it now uses 32-bit mask as expected.

BZ#1008691

A previous patch to the kernel introduced the "VLAN tag re-insertion" workaround to resolve a problem with incorrectly handled VLAN-tagged packets with no assigned VLAN group while the be2net driver was in promiscuous mode. However, this solution led to packet corruption and a subsequent kernel oops if such a processed packed was a GRO packet. Therefore, a patch has been applied to restrict VLAN tag re-insertion only to non-GRO packets. The be2net driver now processes VLAN-tagged packets with no assigned VLAN group correctly in this situation.

BZ#867570

The NFSv4 server did not handle multiple OPEN operations to the same file separately, which could cause the NFSv4 client to repeatedly send CLOSE requests with the same state ID, even though the NFS server rejected the request with an NFS4ERR_OLD_STATEID (10024) error code. This update ensures that the NFSv4 client no longer re-sends the same CLOSE request after receiving NFS4ERR_OLD_STATEID.

BZ#867997

A previous fix to the kernel did not contain a memory barrier in the percpu_up_write() function. Consequently, under certain circumstances, a race condition could occur leading to memory corruption and a subsequent kernel panic. This update introduces a new memory barrier pair, light_mb() and heavy_mb(), for per-CPU basis read and write semaphores (percpu-rw-semaphores) ensuring that the race condition can no longer occur. In addition, the read path performance of "percpu-rw-semaphores" has been improved.

BZ#1063434

Running a process in the background on a GFS2 file system could sometimes trigger a glock recursion error that resulted in a kernel panic. This happened when a readpage operation attempted to take a glock that had already been held by another function. To prevent this error, GFS2 now verifies whether the glock is already held when performing the readpage operation.

BZ#1075228

When being under heavy load, some Fibre Channel storage devices, such as Hitachi and HP Open-V series, can send a logout (LOGO) message to the host system. However, due to a bug in the lpfc driver, this could result in a loss of active paths to the storage and the paths could not be recovered without manual intervention. This update corrects the lpfc driver to ensure automatic recovery of the lost paths to the storage in this scenario.

BZ#1080194

Due to a bug in the page writeback code, the system could become unresponsive when being under memory pressure and heavy NFS load. This update fixes the code responsible for handling of dirty pages, and dirty page write outs no longer flood the work queue.

BZ#924590

A workaround to a DMA read problem in the tg3 driver was incorrectly applied to the whole Broadcom 5719 and 5720 chipset family. This workaround is valid only to the A0 revision of the 5719 chips and for other revisions and chips causes occasional Tx timeouts. This update correctly applies the aforementioned workaround only to the A0 revision of the 5719 chips.

BZ#928518

A bug in the GFS2 code prevented glock work queues from freeing glock-related memory while the glock memory shrinker repeatedly queued a large number of demote requests, for example when performing a simultaneous backup of several live GFS2 volumes with a large file count. As a consequence, the glock work queues became overloaded which resulted in a high CPU usage and the GFS2 file systems being unresponsive for a significant amount of time. A patch has been applied to alleviate this problem by calling the yield() function after scheduling a certain amount of tasks on the glock work queues. The problem can now occur only with extremely high work loads.

BZ#1080606

Recent changes in the d_splice_alias() function introduced a bug that allowed d_splice_alias() to return a dentry from a different directory than was the directory being looked up. As a consequence in cluster environment, a kernel panic could be triggered when a directory was being removed while a concurrent cross-directory operation was performed on this directory on another cluster node. This update avoids the kernel panic in this situation by correcting the search logic in the d_splice_alias() function so that the function can no longer return a dentry from an incorrect directory.

BZ#998126

A previous change to the sunrpc code introduced a race condition between the rpc_wake_up_task() and rpc_wake_up_status() functions. A race between threads operating on these functions could result in a deadlock situation, subsequently triggering a "soft lockup" event and rendering the system unresponsive. This problem has been fixed by ensuring that entries in the RPC wait queue that are being woken up do not block the entire queue.

BZ#956132

Certain storage device or storage environment failures could cause all SCSI commands and task management functions that were sent to a SCSI target to time out, without any other indication of an error. As a consequence, the Linux SCSI error handling code stopped issuing any I/O operations on the entire HBA adapter until the recovery operations completed. Additionally when using DM Multipath, I/O operations did not fail over to a working path in this situation. To resolve this problem, a new sysfs parameter, "eh_deadline", has been added to the SCSI host object. This parameter allows to set the maximum amount of time for which the SCSI error handling attempts to perform error recovery before resetting the entire HBA adapter. This timeout is disabled by default. The default value of this timeout can be reset for all SCSI HBA adapters on the system using the "eh_deadline" kernel parameter. The described scenario no longer occurs if eh_deadline is properly used.

BZ#956330

Due to an incorrect test condition in the mpt2sas driver, the driver was unable to catch failures to map a SCSI scatter-gather list. The test condition has been corrected so that the mpt2sas driver now handles SCSI scatter-gather mapping failures as expected.

BZ#995293

The IPMI driver did not properly handle kernel panic messages. Consequently, when a kernel panic occurred on a system that was utilizing IPMI without Kdump being set up, a second kernel panic could be triggered. A patch has been applied to the IPMI driver to fix this problem, and a message handler now properly waits for a response to panic event messages.

BZ#1090806

After a statically defined gateway became unreachable and its corresponding neighbor entry entered a FAILED state, the gateway stayed in the FAILED state even after it became reachable again. As a consequence, traffic was not routed through that gateway. This update allows probing such a gateway automatically so that the traffic can be routed through this gateway again once it becomes reachable.

BZ#976201

A function in the RPC code responsible for verifying whether the cached credentials match the current process did not perform the check correctly. The code checked only whether the groups in the current process credentials appear in the same order as in the cached credentials but did not ensure that no other groups are present in the cached credentials. As a consequence, when accessing files in NFS mounts, a process with the same UID and GID as the original process but with a non-matching group list could have been granted an unauthorized access to a file, or under certain circumstances, the process could have been wrongly prevented from accessing the file. The incorrect test condition has been fixed and the problem can no longer occur.

BZ#995277

Due to an incorrect condition check in the IPv6 code, the ipv6 driver was unable to correctly assemble incoming packet fragments, which resulted in a high IPv6 packet loss rate. This update fixes the said check for a fragment overlap and ensures that incoming IPv6 packet fragments are now processed as expected.

BZ#980268

A bug in the journaling block device (jbd and jbd2) code could, under certain circumstances, trigger a BUG_ON() assertion and result in a kernel oops. This happened when an application performed an extensive number of commits to the journal of the ext3 file system and there was no currently active transaction while synchronizing the file's in-core state. This problem has been resolved by correcting respective test conditions in the jbd and jbd2 code.

BZ#1081785

A bug in the journaling code (jbd and jbd2) could, under very heavy workload of fsync() operations, trigger a BUG_ON and result in a kernel oops. Also, fdatasync() could fail to immediately write out changes in the file size only. These problems have been resolved by backporting a series of patches that fixed these problems in the respective code on Red Hat Enterprise Linux 6. This update also improves performance of ext3 and ext4 file systems.

BZ#1084168

A bug in the futex system call could result in an overflow when passing a very large positive timeout. As a consequence, the FUTEX_WAIT operation did not work as intended and the system call was timing out immediately. A backported patch fixes the bug by limiting very large positive timeouts to the maximal supported value.

BZ#996331

Due to a bug in the tg3 driver, systems that had the Wake-on-LAN (WOL) feature enabled on their NICs could not have been woken up from suspension or hibernation using WOL. A missing pci_wake_from_d3() function call has been added to the tg3 driver, which ensures that WOL functions properly by setting the PME_ENABLE bit.

BZ#916235

A new Linux Security Module (LSM) functionality related to the setrlimit hooks should produce a warning message when used by a third party module that could not cope with it. However, due to a programming error, the kernel could print this warning message when a process was setting rlimits for a different process, or if rlimits were modified by another than the main thread even though there was no incompatible third party module. This update fixes the relevant code and ensures that the kernel handles this warning message correctly.

BZ#1102768

Due to a bug in the ext4 code, the fdatasync() system call did not force the inode size change to be written to the disk if it was the only metadata change in the file. This could result in the wrong inode size and possible data loss if the system terminated unexpectedly. The code handling inode updates has been fixed and fdatasync() now writes data to the disk as expected in this situation.

BZ#1018286

A recent patch to the CIFS code that introduced the NTLMSSP (NT LAN Manager Security Support Provider) authentication mechanism caused a regression in CIFS behavior. As a result of the regression, an encryption key that is returned during the SMB negotiation protocol response was only used for the first session that was created on the SMB client. Any subsequent mounts to the same server did not use the encryption key returned by the initial negotiation with the server. As a consequence, it was impossible to mount multiple SMB shares with different credentials to the same server. A patch has been applied to correct this problem so that an encryption key or a server challenge is now provided for every SMB session during the SMB negotiation protocol response.

BZ#985767

Previously, the kernel was unable to detect KVM on system boot if the Hyper-V emulation was enabled. A patch has been applied to ensure that both KVM and Hyper-V hypervisors are now correctly detected during system boot.

BZ#1007995

A previous change that corrected a bug preventing communication between NICs using be2net introduced a memory leak in the be2net transmitter (Tx) code path. The memory leak has been fixed by applying a series of patches that corrects handling of socket buffers (SKBs) in the Tx code path.

Enhancements

BZ#1061120

The lpfc driver had a fixed timeout of 60 seconds for SCSI task management commands. With this update, the lpfc driver enables the user to set this timeout within the range from 5 to 180 seconds. The timeout can be changed by modifying the "lpfc_task_mgmt_tmo" parameter for the lpfc driver.

BZ#662558

Support for a kernel symbol that allows printing a binary blob of data as a hex dump to syslog has been added to kABI (Kernel Application Binary Interface).

BZ#826060

This update introduces the "eh_timeout" variable to the SCSI error handling code in order to allow users to control the timeout value for I/O error recovery commands.

All Red Hat Enterprise Linux 5 users are advised to install these updated packages, which fix the bugs and add the enhancements noted in the Red Hat Enterprise Linux 5.11 Release Notes and Technical Notes. The system must be rebooted for this update to take effect.

3.37. kexec-tools

3.37.1. RHBA-2014:1204 — kexec-tools bug fix update

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

The kexec-tools packages contain the /sbin/kexec binary and utilities that together form the user-space component of the kernel's kexec feature. The /sbin/kexec binary facilitates a new kernel to boot using the kernel's kexec feature either on a normal or a panic reboot. The kexec fastboot mechanism allows booting a Linux kernel from the context of an already running kernel.

Bug Fix

BZ#1028595

Previously, kdump did not support custom names for network devices. As a consequence, kdump failed to capture a core file on a remote target over a network if the respective network device had a custom name. This update modifies the mkdumprd utility to recognize bridge, bonding and VLAN devices with custom names, thus allowing to dump a core file to a remote target over such a device.

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

3.38. krb5

3.38.1. RHBA-2014:0494 — krb5 bug fix update

Updated krb5 packages that fix one bug are now available for Red Hat Enterprise Linux 5.

Kerberos is an authentication system which allows clients and services to authenticate to each other with the help of a trusted third party, a Kerberos KDC.

Bug Fix

BZ#1095364

> Previously, when the krb5 client library was waiting for a response from a server, the timeout variable in certain cases became a negative number. Consequently, the client could enter a loop while checking for responses. With this update, the client logic has been modified and the described error no longer occurs.

Users of krb5 are advised to upgrade to these updated packages, which fix this bug.

3.38.2. RHSA-2014:1255 — Moderate: krb5 security update

Updated krb5 packages that fix one security issue are now available for Red Hat Enterprise Linux 5.

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

Kerberos is an authentication system which allows clients and services to authenticate to each other with the help of a trusted third party, a Kerberos Key Distribution Center (KDC).

Security Fix

CVE-2014-4345

> A buffer overflow was found in the KADM5 administration server (kadmind) when it was used with an LDAP back end for the KDC database. A remote, authenticated attacker could potentially use this flaw to execute arbitrary code on the system running kadmind.

All krb5 users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, the krb5kdc and kadmind daemons will be restarted automatically.

3.38.3. RHSA-2014:1245 — Moderate: krb5 security and bug fix update

Updated krb5 packages that fix multiple security issues and two bugs are now available for Red Hat Enterprise Linux 5.

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

Kerberos is an authentication system which allows clients and services to authenticate to each other with the help of a trusted third party, a Kerberos Key Distribution Center (KDC).

Security Fixes

CVE-2013-1418, CVE-2013-6800

> It was found that if a KDC served multiple realms, certain requests could cause the setup_server_realm() function to dereference a NULL pointer. A remote, unauthenticated attacker could use this flaw to crash the KDC using a specially crafted request.

CVE-2014-4344

> A NULL pointer dereference flaw was found in the MIT Kerberos SPNEGO acceptor for continuation tokens. A remote, unauthenticated attacker could use this flaw to crash a GSSAPI-enabled server application.

CVE-2014-4341

A buffer over-read flaw was found in the way MIT Kerberos handled certain requests. A man-in-the-middle attacker with a valid Kerberos ticket who is able to inject packets into a client or server application's GSSAPI session could use this flaw to crash the application.

Bug Fixes

BZ#1004632

Prior to this update, the libkrb5 library occasionally attempted to free already freed memory when encrypting credentials. As a consequence, the calling process terminated unexpectedly with a segmentation fault. With this update, libkrb5 frees memory correctly, which allows the credentials to be encrypted appropriately and thus prevents the mentioned crash.

BZ#1089732

Previously, when the krb5 client library was waiting for a response from a server, the timeout variable in certain cases became a negative number. Consequently, the client could enter a loop while checking for responses. With this update, the client logic has been modified and the described error no longer occurs.

All krb5 users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the krb5kdc daemon will be restarted automatically.

3.39. ksh

3.39.1. RHBA-2014:0317 — ksh bug fix update

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

KornShell (KSH) is a Unix shell developed by AT&T Bell Laboratories, which is backward-compatible with the Bourne shell (Bash) and includes many features of the C shell. The most recent version is KSH-93. KornShell complies with the POSIX.2 standard (IEEE Std 1003.2-1992).

Bug Fix

BZ#1076215

Prior to this update, a fix was introduced for a bug where, under some circumstances, ksh did not execute command substitution in here-documents. However, this fix caused a regression. As a consequence, scripts in which command substitution was used after the pipe character ("|") did not function properly. With this patch, the fix for the previous bug has been reverted, and command substitution now works in combination with pipes as intended. Nevertheless, the reversion also reintroduces the previous bug, which may cause loss of content in here-documents.

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

3.39.2. RHBA-2014:1214 — ksh bug fix update

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

KornShell (KSH) is a Unix shell developed by AT&T Bell Laboratories, which is backward-compatible with the Bourne shell (Bash) and includes many features of the C shell. The most recent version is KSH-93. KornShell complies with the POSIX.2 standard (IEEE Std 1003.2-1992).

Bug Fixes

BZ#1058563

Previously, the ksh shell forking during variable assignment failed to close the file descriptors in the child process 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#1079947

Previously, the brace expansion, a mechanism by which arbitrary strings may be generated, could not be disabled using the "set +B" command. The underlying source code has been fixed, and now it is possible to disable brace expansion when needed.

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

3.40. kvm

3.40.1. RHSA-2014:0163 — Important: kvm security update

Updated kvm packages that fix two security issues are now available for Red Hat Enterprise Linux 5.

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

KVM (Kernel-based Virtual Machine) is a full virtualization solution for Linux on AMD64 and Intel 64 systems. KVM is a Linux kernel module built for the standard Red Hat Enterprise Linux kernel.

Security Fixes

CVE-2013-6367

A divide-by-zero flaw was found in the apic_get_tmcct() function in KVM's Local Advanced Programmable Interrupt Controller (LAPIC) implementation. A privileged guest user could use this flaw to crash the host.

CVE-2013-6368

A memory corruption flaw was discovered in the way KVM handled virtual APIC accesses that crossed a page boundary. A local, unprivileged user could use this flaw to crash the system or, potentially, escalate their privileges on the system.

Red Hat would like to thank Andrew Honig of Google for reporting these issues.

All kvm users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. Note: the procedure in the Solution section must be performed before this update will take effect.

3.40.2. RHBA-2014:1221 — kvm bug fix and enhancement update

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

The kvm packages have been updated to work with the version of the Linux kernel shipped with Red Hat Enterprise Linux 5.11.

Users of kvm are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. Note: The procedure in the Solution section must be performed before this update will take effect.

3.41. libgcrypt

3.41.1. RHSA-2013:1457 — Moderate: libgcrypt security update

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

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

The libgcrypt library provides general-purpose implementations of various cryptographic algorithms.

Security Fix

CVE-2013-4242

> It was found that GnuPG was vulnerable to the Yarom/Falkner flush+reload cache side-channel attack on the RSA secret exponent. An attacker able to execute a process on the logical CPU that shared the L3 cache with the GnuPG process (such as a different local user or a user of a KVM guest running on the same host with the kernel same-page merging functionality enabled) could possibly use this flaw to obtain portions of the RSA secret key.

All libgcrypt users are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

3.42. libjpeg

3.42.1. RHSA-2013:1804 — Moderate: libjpeg security update

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

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

The libjpeg package contains a library of functions for manipulating JPEG images. It also contains simple client programs for accessing the libjpeg functions.

Security Fix

CVE-2013-6629

> An uninitialized memory read issue was found in the way libjpeg decoded images with missing Start Of Scan (SOS) JPEG markers. A remote attacker could create a specially

crafted JPEG image that, when decoded, could possibly lead to a disclosure of potentially sensitive information.

All libjpeg users are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

3.43. libtiff

3.43.1. RHSA-2014:0223 — Moderate: libtiff security update

Updated libtiff 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 scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

The libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

Security Fixes

CVE-2013-1960, CVE-2013-4232

A heap-based buffer overflow and a use-after-free flaw 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.

CVE-2013-4231, CVE-2013-4243, CVE-2013-4244

Multiple buffer overflow flaws were found in the gif2tiff tool. An attacker could use these flaws to create a specially crafted GIF file that could cause gif2tiff to crash or, possibly, execute arbitrary code.

CVE-2013-1961

Multiple buffer overflow flaws 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.

Red Hat would like to thank Emmanuel Bouillon of NCI Agency for reporting CVE-2013-1960 and CVE-2013-1961. The CVE-2013-4243 issue was discovered by Murray McAllister of the Red Hat Security Response Team, and the CVE-2013-4244 issue was discovered by Huzaifa Sidhpurwala of the Red Hat Security Response Team.

All libtiff users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. All running applications linked against libtiff must be restarted for this update to take effect.

3.44. libXfont

3.44.1. RHSA-2014:0018 — Important: libXfont security update

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

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

The libXfont packages provide the X.Org libXfont runtime library. X.Org is an open source implementation of the X Window System.

Security Fix

CVE-2013-6462

> A stack-based buffer overflow flaw was found in the way the libXfont library parsed Glyph Bitmap Distribution Format (BDF) fonts. A malicious, local user could exploit this issue to potentially execute arbitrary code with the privileges of the X.Org server.

Users of libXfont should upgrade to these updated packages, which contain a backported patch to resolve this issue. All running X.Org server instances must be restarted for the update to take effect.

3.45. lvm2-cluster

3.45.1. RHBA-2014:1219 — lvm2-cluster bug fix update

Updated lvm2-cluster packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

The lvm2-cluster packages contain support for Logical Volume Management (LVM) in a clustered environment.

Bug Fixes

BZ#966283

> Incorrect validation of the clvmd daemon request could lead to a failure with numerous error messages logged. This bug also caused considerable CPU consumption, locking up all logical volume (LVM) commands due to false interpretation of the requests and exhaustive logging. A set of patches has been provided to improve the clvmd request validation, thus fixing the aforementioned bug.

BZ#1005408

> When one of the logical volume (LVM) client processes was killed, the clvmd daemon had to wait for a mutual exclusion (mutex) to stop the LVM client thread. Consequently, lvm utility commands in a cluster became indefinitely blocked. This update introduces a patch which fixes the deadlock, and lvm utility commands now work correctly.

BZ#1025881

> Due to a regression, the "clvmd -R" command failed to execute with the following error message:
>
> "EOF reading CLVMD"
>
> The underlying source code has been fixed, and "clvmd -R" now works as intended.

Users of lvm2-cluster are advised to upgrade to these updated packages, which fix these bugs.

3.46. lvm2

3.46.1. RHBA-2014:1218 — lvm2 bug fix and enhancement update

Updated lvm2 packages that fix two bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

The lvm2 packages provide support for Logical Volume Management (LVM).

Bug Fixes

BZ#204997

Prior to this update, the user had to specify major number together with minor number when using persistent (-My/--persistent y) device numbers for logical volumes (LVs). However, in kernel versions higher than 2.4, the "--major" option is ignored because the kernel now assigns major numbers by itself. This behavior cannot be overridden. Now, when specifying the persistent minor number with the "lvcreate/lvchange -My/--persistent y --minor !" command, the user no longer needs to specify the major number with the "--major" argument. If the "--major" argument is used, the user is now informed by the following message:

"Ignoring supplied major number - kernel assigns major numbers dynamically. Using major number <major number assigned by kernel> instead."

BZ#1053849

Previously, if the pvmove command was executed on clustered volume groups, temporarily activated pvmove devices were activated on all nodes. This was incorrect and in some situations, such as using tags or HA-LVM configuration, it caused pvmove failures. With this update, pvmove activates all needed pvmove devices exclusively when moving logical volumes are already exclusively activated.

In addition, this update adds the following

Enhancement

BZ#569511

Previously, the lvm-dumpconfig utility displayed the whole configuration but without the logical volume (LVM) configuration tags set for the host. This update introduces the "lvm tags" command which displays the configuration tags set for the current host including the tag configuration which is used on the host.

Users of lvm2 are advised to upgrade to these updated packages, which fix these bugs and add this enhancement.

3.47. microcode_ctl

3.47.1. RHEA-2014:1236 — 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 utility code and microcode data to assist the kernel in updating the CPU microcode at system boot time. This microcode supports all current x86-based, Intel 64-based, and AMD64-based CPU models. It takes advantage of the mechanism built-in to Linux that allows microcode to be updated after system boot. When loaded, the updated microcode corrects the behavior of various processors, as described in processor specification updates issued by Intel and AMD for those processors.

Enhancement

BZ#1064359

With this update, the Intel CPU microcode has been updated to version 20140430.

Users of microcode_ctl are advised to upgrade to these updated packages, which add this enhancement. Note that a system reboot is necessary for this update to take effect.

3.48. mkinitrd

3.48.1. RHBA-2014:1224 — mkinitrd bug fix and enhancement update

Updated mkinitrd packages that fix several bugs and add one enhancement are now available for 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#1006058

A previous fix to a related security issue introduced to the libnss library a new run-time dependency on the libsqlite library. However, libsqlite was not included in the initrd.img file. As a consequence, the kernel verification was not successful and caused the system boot to fail with a kernel panic. With this update, the mkinitrd utility verifies that libsqlite is included when building a new initrd image and the kernel panic no longer occurs.

BZ#978245

Prior to this update, the Advanced Host Controller Interface (AHCI) driver was not included in the initrd.img file. As a consequence, a Red Hat Enterprise Linux 5 guest in some cases failed to boot on a Red Hat Enterprise Linux 7 hypervisor. With this update, installing Red Hat Enterprise Linux 5 as a guest now always includes the AHCI driver, and the guest is therefore able to boot as expected.

BZ#988020

Previously, mkinitrd searched an incorrect path for the cciss block driver device and the findstoragedriver() function could therefore not find cciss in the /sys/block directory. Consequently, the kernel failed to boot after it was updated. This update amends the cciss path and findstoragedriver() is thus able to detect cciss devices correctly. As a result, the kernel now boots as expected.

In addition, this update adds the following

Enhancement

BZ#472764

In order to simplify the process of adding a new direct access storage device (DASD), running a mkinitrd command without parameters now prompts the user to re-create the initial RAM disk for the currently running kernel in the /boot/ directory.

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

3.49. mod_nss

3.49.1. RHSA-2013:1779 — Moderate: mod_nss security update

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

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

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.

Security Fix

CVE-2013-4566

> A flaw was found in the way mod_nss handled the NSSVerifyClient setting for the per-directory context. When configured to not require a client certificate for the initial connection and only require it for a specific directory, mod_nss failed to enforce this requirement and allowed a client to access the directory when no valid client certificate was provided.

Red Hat would like to thank Albert Smith of OUSD(AT&L) for reporting this issue.

All mod_nss users should upgrade to this updated package, which contains a backported patch to correct this issue. The httpd service must be restarted for this update to take effect.

3.50. mysql55-mysql

3.50.1. RHSA-2014:0536 — Moderate: mysql55-mysql security update

Updated mysql55-mysql 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 Moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

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-2014-2436, CVE-2014-2440, CVE-2014-0384, CVE-2014-2419, CVE-2014-2430, CVE-2014-2431, CVE-2014-2432, CVE-2014-2438

> This update fixes several vulnerabilities in the MySQL database server. Information about these flaws can be found on the Oracle Critical Patch Update Advisory page.

These updated packages upgrade MySQL to version 5.5.37. Refer to the MySQL Release Notes for a complete list of changes.

All MySQL users should upgrade to these updated packages, which correct these issues. After installing this update, the MySQL server daemon (mysqld) will be restarted automatically.

3.50.2. RHSA-2014:0186 — Moderate: mysql55-mysql security update

Updated mysql55-mysql 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 moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

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

Security Fixes

CVE-2013-5807, CVE-2013-5891, CVE-2014-0386, CVE-2014-0393, CVE-2014-0401, CVE-2014-0402, CVE-2014-0412, CVE-2014-0420, CVE-2014-0437, CVE-2013-3839, CVE-2013-5908

> This update fixes several vulnerabilities in the MySQL database server. Information about these flaws can be found on the Oracle Critical Patch Update Advisory January 2014 page and October 2014 page.

CVE-2014-0001

> A buffer overflow flaw was found in the way the MySQL command line client tool (mysql) processed excessively long version strings. If a user connected to a malicious MySQL server via the mysql client, the server could use this flaw to crash the mysql client or, potentially, execute arbitrary code as the user running the mysql client.

The CVE-2014-0001 issue was discovered by Garth Mollett of the Red Hat Security Response Team.

These updated packages upgrade MySQL to version 5.5.36. Refer to the MySQL Release Notes for a complete list of changes.

All MySQL users should upgrade to these updated packages, which correct these issues. After installing this update, the MySQL server daemon (mysqld) will be restarted automatically.

3.51. net-snmp

3.51.1. RHSA-2014:0322 — Moderate: net-snmp security update

Updated net-snmp 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 scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

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.

Security Fixes

CVE-2012-6151

A denial of service flaw was found in the way snmpd, the Net-SNMP daemon, handled subagent timeouts. A remote attacker able to trigger a subagent timeout could use this flaw to cause snmpd to loop infinitely or crash.

CVE-2014-2285

A denial of service flaw was found in the way the snmptrapd service, which receives and logs SNMP trap messages, handled SNMP trap requests with an empty community string when the Perl handler (provided by the net-snmp-perl package) was enabled. A remote attacker could use this flaw to crash snmptrapd by sending a trap request with an empty community string.

All net-snmp users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the snmpd and snmptrapd services will be restarted automatically.

3.52. net-tools

3.52.1. RHBA-2013:1424 — net-tools bug fix update

An updated net-tools package that fixes multiple bugs is now available for Red Hat Enterprise Linux 5.

The net-tools package contains basic networking tools, including ifconfig, netstat, or route. Netstat, for example, prints information about the Linux networking subsystem.

Bug Fixes

BZ#1015547

When the "netstat --sctp -n" command was run on a system with large number of Stream Control Transmission Protocol (SCTP) connections, the netstat utility terminated unexpectedly with a segmentation fault. A patch that makes netstat sanitize input has been applied and netstat no longer crashes.

BZ#1015550

Running the "netstat --sctp -n" command caused netstat to print IP addresses incorrectly for the SCTP protocol. A patch has been back-ported from Red Hat Enterprise Linux 6 and netstat now shows correct IP addresses for SCTP protocol.

All users of net-tools are advised to upgrade to this updated package, which fixes these bugs.

3.53. nfs-utils

3.53.1. RHBA-2014:1235 — nfs-utils bug fix update

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

The nfs-utils packages provide a daemon for the kernel Network File System (NFS) server and related tools, 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.

Bug Fixes

BZ#513217

Previously, the summary string in the nfs-utils RPM contained a typo. The text has been fixed, and the string describing the nfs-utils utility is now spelled correctly.

BZ#863241

The rpc.gssd daemon always tried to use a compiler cache (ccache) which had higher mtime but did not verify whether a new ccache is expired or not. Consequently, as rpc.gssd kept on sticking with the ccache until it was deleted, secure NFS context was not created. With this update, rpc.gssd uses a ccache with higher mtime, and if the current is expired, marks it as expired and uses the current valid ccache.

Users of nfs-utils are advised to upgrade to these updated packages, which fix these bugs. After installing this update, the nfs service will be restarted automatically.

3.54. nss

3.54.1. RHSA-2013:1861 — Moderate: nss security update

Updated nss 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.

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications.

All NSS users should upgrade to these updated packages, which correct this issue. After installing the update, applications using NSS must be restarted for the changes to take effect.

3.55. nss and nspr

3.55.1. RHSA-2013:1791 — Important: nss and nspr security, bug fix, and enhancement update

Updated nss and nspr packages that fix multiple 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 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.

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications. Netscape Portable Runtime (NSPR) provides platform independence for non-GUI operating system facilities.

Security Fixes

CVE-2013-5605

A flaw was found in the way NSS handled invalid handshake packets. A remote attacker could use this flaw to cause a TLS/SSL client using NSS to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

CVE-2013-1739

It was found that the fix for CVE-2013-1620 released via RHSA-2013:1135 introduced a regression causing NSS to read uninitialized data when a decryption failure occurred. A remote attacker could use this flaw to cause a TLS/SSL server using NSS to crash.

CVE-2013-1741, CVE-2013-5607

An integer overflow flaw was discovered in both NSS and NSPR's implementation of certification parsing on 64-bit systems. A remote attacker could use these flaws to cause an application using NSS or NSPR to crash.

CVE-2013-5606

It was discovered that NSS did not reject certificates with incompatible key usage constraints when validating them while the verifyLog feature was enabled. An application using the NSS certificate validation API could accept an invalid certificate.

Red Hat would like to thank the Mozilla project for reporting CVE-2013-1741, CVE-2013-5606, and CVE-2013-5607. Upstream acknowledges Tavis Ormandy as the original reporter of CVE-2013-1741, Camilo Viecco as the original reporter of CVE-2013-5606, and Pascal Cuoq, Kamil Dudka, and Wan-Teh Chang as the original reporters of CVE-2013-5607.

In addition, the nss package has been upgraded to upstream version 3.15.3, and the nspr package has been upgraded to upstream version 4.10.2. These updates provide a number of bug fixes and enhancements over the previous versions. (BZ#1033478, BZ#1020520)

Bug Fix

BZ#1033499

The RHBA-2013:1318 update introduced a regression that prevented the use of certificates that have an MD5 signature. This update fixes this regression and certificates that have an MD5 signature are once again supported. To prevent the use of certificates that have an MD5 signature, set the "NSS_HASH_ALG_SUPPORT" environment variable to "-MD5".

Red Hat would like to thank the Mozilla project for reporting CVE-2013-1741, CVE-2013-5606, and CVE-2013-5607. Upstream acknowledges Tavis Ormandy as the original reporter of CVE-2013-1741, Camilo Viecco as the original reporter of CVE-2013-5606, and Pascal Cuoq, Kamil Dudka, and Wan-Teh Chang as the original reporters of CVE-2013-5607.

In addition, the nss package has been upgraded to upstream version 3.15.3, and the nspr package has been upgraded to upstream version 4.10.2. These updates provide a number of bug fixes and enhancements over the previous versions. (BZ#1033478, BZ#1020520)

Users of NSS and NSPR are advised to upgrade to these updated packages, which fix these issues and add these enhancements. After installing this update, applications using NSS or NSPR must be restarted for this update to take effect.

3.55.2. RHSA-2014:1246 — Moderate: nss and nspr security, bug fix, and enhancement update

Updated nss and nspr packages that fix multiple security issues, several bugs, and add various enhancements are now available for Red Hat Enterprise Linux 5.

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

Network Security Services (NSS) is a set of libraries designed to support the cross-platform development of security-enabled client and server applications.

Security Fixes

CVE-2013-1740

A flaw was found in the way TLS False Start was implemented in NSS. An attacker could use this flaw to potentially return unencrypted information from the server.

CVE-2014-1490

A race condition was found in the way NSS implemented session ticket handling as specified by RFC 5077. An attacker could use this flaw to crash an application using NSS or, in rare cases, execute arbitrary code with the privileges of the user running that application.

CVE-2014-1491

It was found that NSS accepted weak Diffie-Hellman Key exchange (DHKE) parameters. This could possibly lead to weak encryption being used in communication between the client and the server.

CVE-2014-1545

An out-of-bounds write flaw was found in NSPR. A remote attacker could potentially use this flaw to crash an application using NSPR or, possibly, execute arbitrary code with the privileges of the user running that application. This NSPR flaw was not exposed to web content in any shipped version of Firefox.

CVE-2014-1492

It was found that the implementation of Internationalizing Domain Names in Applications (IDNA) hostname matching in NSS did not follow the RFC 6125 recommendations. This could lead to certain invalid certificates with international characters to be accepted as valid.

Red Hat would like to thank the Mozilla project for reporting the CVE-2014-1490, CVE-2014-1491, and CVE-2014-1545 issues. Upstream acknowledges Brian Smith as the original reporter of CVE-2014-1490, Antoine Delignat-Lavaud and Karthikeyan Bhargavan as the original reporters of CVE-2014-1491, and Abhishek Arya as the original reporter of CVE-2014-1545.

The nss and nspr packages have been upgraded to upstream version 3.16.1 and 4.10.6 respectively, which provide a number of bug fixes and enhancements over the previous versions. (BZ#1110857, BZ#1110860)

Bug Fixes

BZ#1035281

Previously, when the output.log file was not present on the system, the shell in the Network Security Services (NSS) specification handled test failures incorrectly as false positive test results. Consequently, certain utilities, such as "grep", could not handle failures properly. This update improves error detection in the specification file, and "grep" and other utilities now handle missing files or crashes as intended.

BZ#1042684

Prior to this update, a subordinate Certificate Authority (CA) of the ANSSI agency incorrectly issued an intermediate certificate installed on a network monitoring device. As a consequence, the monitoring device was enabled to act as an MITM (Man in the Middle) proxy performing traffic management of domain names or IP addresses that the certificate holder did not own or control. The trust in the intermediate certificate to issue the certificate for an MITM device has been revoked, and such a device can no longer be used for MITM attacks.

BZ#11015864

Due to a regression, MD5 certificates were rejected by default because Network Security Services (NSS) did not trust MD5 certificates. With this update, MD5 certificates are supported in Red Hat Enterprise Linux 5.

Red Hat would like to thank the Mozilla project for reporting the CVE-2014-1490, CVE-2014-1491, and CVE-2014-1545 issues. Upstream acknowledges Brian Smith as the original reporter of CVE-2014-1490, Antoine Delignat-Lavaud and Karthikeyan Bhargavan as the original reporters of CVE-2014-1491, and Abhishek Arya as the original reporter of CVE-2014-1545.

The nss and nspr packages have been upgraded to upstream version 3.16.1 and 4.10.6 respectively, which provide a number of bug fixes and enhancements over the previous versions. (BZ#1110857, BZ#1110860)

Users of nss and nspr are advised to upgrade to these updated packages, which correct these issues and add these enhancements.

3.56. ntp

3.56.1. RHBA-2013:1800 — ntp bug fix update

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

The Network Time Protocol (NTP) is used to synchronize a computer's time with another referenced time source. This package includes the ntpd daemon which continuously adjusts system time and utilities used to query and configure the ntpd daemon.

Bug Fix

BZ#1037272

Previously, with a complex Name Service Switch (NSS) configured and large NTP request rate, the ntpd daemon needed more memory than was allowed by the memory locking limit. As a consequence, the ntpd process could terminate unexpectedly. To fix this bug, the memory locking limit has been doubled. As a result, ntpd no longer crashes.

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

3.57. openldap

3.57.1. RHSA-2014:0206 — Moderate: openldap security update

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

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

OpenLDAP is an open source suite of Lightweight Directory Access Protocol (LDAP) applications and development tools. LDAP is a set of protocols used to access and maintain distributed directory information services over an IP network. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.

Security Fix

CVE-2013-4449

> A denial of service flaw was found in the way the OpenLDAP server daemon (slapd) performed reference counting when using the rwm (rewrite/remap) overlay. A remote attacker able to query the OpenLDAP server could use this flaw to crash the server by immediately unbinding from the server after sending a search request.

Red Hat would like to thank Michael Vishchers from Seven Principles AG for reporting this issue.

All openldap users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue.

3.57.2. RHBA-2014:0502 — 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 Lightweight Directory Access Protocol (LDAP) applications and development tools. LDAP is a set of protocols used to access and maintain distributed directory information services over an IP network. The openldap package contains configuration files, libraries, and documentation for OpenLDAP.

Bug Fix

BZ#1096634

> Previously, the replication process in LDAP did not function correctly. As a consequence, replicated data could be inconsistent and, under some circumstances, the Stand-alone LDAP Daemon, slapd, terminated unexpectedly. With this update, LDAP has been modified to properly lock critical sections. Therefore, the replicated data now stays consistent and slapd no longer crashes.

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

3.58. openmotif

3.58.1. RHBA-2014:0128 — openmotif bug fix update

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

The openmotif packages include the Motif shared libraries needed to run applications which are dynamically linked against Motif, as well as MWM, the Motif Window Manager.

* Previously, when the window manager was set as MWM (Motif Window Manager) and the Mwm*freezeOnConfig and Mwm*moveOpaque options were set to "False", only icons appeared while moving a window anywhere on the screen, and no frame border was drawn. Consequently, users were having problems navigating the applications on their touch screen monitors. A patch has been provided to fix this bug, and windows are now displayed correctly when being moved anywhere on the screen. (BZ#1055235)

Bug Fix

BZ#1055235

> Previously, when the window manager was set as MWM (Motif Window Manager) and the Mwm*freezeOnConfig and Mwm*moveOpaque options were set to "False", only icons appeared while moving a window anywhere on the screen, and no frame border was drawn. Consequently, users were having problems navigating the applications on their touch screen monitors. A patch has been provided to fix this bug, and windows are now displayed correctly when being moved anywhere on the screen.

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

3.58.2. RHBA-2014:1231 — openmotif bug fix update

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

The openmotif packages include the Motif shared libraries needed to run applications which are dynamically linked against Motif, as well as MWM, the Motif Window Manager.

Bug Fix

BZ#997241

> Previously, when the window manager was set to Motif Window Manager (MWM) and the "Mwm*freezeOnConfig" and "Mwm*moveOpaque" options were set to "False", only icons appeared while moving a window anywhere on the screen, and no frame border was drawn. Consequently, users were having problems navigating the applications on their touch screen monitors. A patch has been provided to fix this bug, and windows are now displayed correctly when being moved anywhere on the screen.

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

3.59. openscap

3.59.1. RHBA-2014:0444 — openscap bug fix and enhancement update

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

OpenSCAP is an open source project, which enables integration of the SCAP line of standards. Security Content Automation Protocol (SCAP) is a line of standards managed by the National Institute of Standards and Technology (NIST). It was created to provide a standardized approach to maintaining the security of enterprise systems, such as automatically verifying presence of patches, checking system security configuration settings, and examining systems for signs of compromise.

> **Upgrade to an upstream version**
>
> The openscap packages have been upgraded to upstream version 1.0.8, which provides a number of bug fixes and enhancements over the previous version. Namely, the new version provides an authenticated scanner that meets the National Institute of Standards and Technology's (NIST) SCAP 1.2 certification requirements. (BZ#1013458)

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

3.60. openssl

3.60.1. RHEA-2014:0104 — openssl enhancement update

Updated openssl packages that add an enhancement are now available for Red Hat Enterprise Linux 5.

OpenSSL is a toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, as well as a full-strength general-purpose cryptography library.

Users of openssl are advised to upgrade to these updated packages, which add this enhancement. For the update to take effect, all services linked to the OpenSSL library must be restarted, or the system rebooted.

3.60.2. RHSA-2014:0624 — Important: openssl security update

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

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

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-2014-0224

> It was found that OpenSSL clients and servers could be forced, via a specially crafted handshake packet, to use weak keying material for communication. A man-in-the-middle attacker could use this flaw to decrypt and modify traffic between a client and a server.

Note: In order to exploit this flaw, both the server and the client must be using a vulnerable version of OpenSSL; the server must be using OpenSSL version 1.0.1 and above, and the client must be using any version of OpenSSL. For more information about this flaw, refer to: https://access.redhat.com/site/articles/904433

Red Hat would like to thank the OpenSSL project for reporting this issue. Upstream acknowledges KIKUCHI Masashi of Lepidum as the original reporter of this issue.

All OpenSSL users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. For the update to take effect, all services linked to the OpenSSL library (such as httpd and other SSL-enabled services) must be restarted or the system rebooted.

3.61. openssl097a and openssl098e

3.61.1. RHSA-2014:0626 — Important: openssl097a and openssl098e security update

Updated openssl097a and openssl098e 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 associated with the 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-2014-0224

> It was found that OpenSSL clients and servers could be forced, via a specially crafted handshake packet, to use weak keying material for communication. A man-in-the-middle attacker could use this flaw to decrypt and modify traffic between a client and a server.

Note: In order to exploit this flaw, both the server and the client must be using a vulnerable version of OpenSSL; the server must be using OpenSSL version 1.0.1 and above, and the client must be using any version of OpenSSL. For more information about this flaw, refer to: https://access.redhat.com/site/articles/904433

Red Hat would like to thank the OpenSSL project for reporting this issue. Upstream acknowledges KIKUCHI Masashi of Lepidum as the original reporter of this issue.

All OpenSSL users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. For the update to take effect, all services linked to the OpenSSL library (such as httpd and other SSL-enabled services) must be restarted or the system rebooted.

3.62. openswan

3.62.1. RHSA-2014:0185 — Moderate: openswan security update

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

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

Openswan is a free implementation of Internet Protocol Security (IPsec) and Internet Key Exchange (IKE). IPsec uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks.

Security Fix

CVE-2013-6466

> A NULL pointer dereference flaw was discovered in the way Openswan's IKE daemon processed IKEv2 payloads. A remote attacker could send specially crafted IKEv2 payloads that, when processed, would lead to a denial of service (daemon crash), possibly causing existing VPN connections to be dropped.

All openswan users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue.

3.62.2. RHBA-2014:1223 — openswan bug fix update

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

Openswan is an implementation of Internet Protocol Security (IPsec) and Internet Key Exchange (IKE). IPsec uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks.

Bug Fix

BZ#1070358

Previously, Openswan supported a NAT-T negotiation method which used a notification number that was assigned by the Internet Assigned Numbers Authority (IANA) for another option. This incorrect option was therefore removed. As a consequence, clients supporting non-RFC versions of NAT-T could not establish an Openswan connection. With this update, Openswan has been modified to fully ignore that option, and clients can send both the incorrect option and the draft or the RFC option to connect to Openswan successfully.

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

3.63. perl

3.63.1. RHBA-2014:1198 — perl bug fix update

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

Perl is a high-level programming language that is commonly used for system administration utilities and web programming.

Bug Fixes

BZ#991854

When a Perl script was installing a custom signal handler and then received a signal while exiting, the code tried to access the interpreter structure which had already been torn down. As a consequence, Perl terminated with a segmentation fault. With this update, the code resets the signal handler to SIG_DFL before calling the perl_destruct() function, so it does not request thread-specific interpreter structure. Now, Perl scripts no longer crash in the described situation.

BZ#1018721

An incorrect implementation of the NDBM_File module caused using the exists() function on dbmopen()-bound variables to fail with the following warning:

AnyDBM_File doesn't define an EXISTS method

The database preference list has been modified to move the NDBM_File module to a less significant place. Now, Perl code which uses dbmopen() defaults to the Berkeley DB database type and no longer fails in the described situation.

BZ#1029016

The Perl Locale::Maketext localization framework did not properly translate the backslash (\) characters. As a consequence, Perl rendered the backslashes as double (\\). With this update, Perl no longer escapes the backslashes in literal output strings, and they appear correctly.

BZ#1057047

Previously, it was not possible to convert dates beyond year 2038 using the timegm() function on 64-bit systems. After this update, Perl detects 64-bit systems correctly and timegm() successfully converts calendar time into seconds since the Unix epoch. Note that using timegm() with dates beyond year 2038 is still not possible on a 32-bit system, because the time_t type is not large enough.

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

3.64. php

3.64.1. RHSA-2013:1814 — Critical: 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 critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fixes

CVE-2013-6420

A memory corruption flaw was found in the way the openssl_x509_parse() function of the PHP openssl extension parsed X.509 certificates. A remote attacker could use this flaw to provide a malicious self-signed certificate or a certificate signed by a trusted authority to a PHP application using the aforementioned function, causing the application to crash or, possibly, allow the attacker to execute arbitrary code with the privileges of the user running the PHP interpreter.

CVE-2011-1398

It was found that PHP did not check for carriage returns in HTTP headers, allowing intended HTTP response splitting protections to be bypassed. Depending on the web browser the victim is using, a remote attacker could use this flaw to perform HTTP response splitting attacks.

CVE-2012-2688

An integer signedness issue, leading to a heap-based buffer underflow, was found in the PHP scandir() function. If a remote attacker could upload an excessively large number of files to a directory the scandir() function runs on, it could cause the PHP interpreter to crash or, possibly, execute arbitrary code.

CVE-2013-1643

It was found that the PHP SOAP parser allowed the expansion of external XML entities during SOAP message parsing. A remote attacker could possibly use this flaw to read arbitrary files that are accessible to a PHP application using a SOAP extension.

Red Hat would like to thank the PHP project for reporting CVE-2013-6420. Upstream acknowledges Stefan Esser as the original reporter.

All php users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

3.64.2. RHSA-2014:0311 — Critical: php security update

Updated php 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 Critical security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fixes

CVE-2009-0689

A buffer overflow flaw was found in the way PHP parsed floating point numbers from their text representation. If a PHP application converted untrusted input strings to numbers, an attacker able to provide such input could cause the application to crash or, possibly, execute arbitrary code with the privileges of the application.

CVE-2006-7243

It was found that PHP did not properly handle file names with a NULL character. A remote attacker could possibly use this flaw to make a PHP script access unexpected files and bypass intended file system access restrictions.

All php users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

3.65. php53 and php

3.65.1. RHSA-2013:1813 — Critical: php53 and php security update

Updated php53 and php 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 critical security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link associated with the description below.

PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server.

Security Fix

CVE-2013-6420

A memory corruption flaw was found in the way the openssl_x509_parse() function of the PHP openssl extension parsed X.509 certificates. A remote attacker could use this flaw to provide a malicious self-signed certificate or a certificate signed by a trusted authority to a PHP application using the aforementioned function, causing the application to crash or, possibly, allow the attacker to execute arbitrary code with the privileges of the user running the PHP interpreter.

Red Hat would like to thank the PHP project for reporting this issue. Upstream acknowledges Stefan Esser as the original reporter of this issue.

All php53 and php users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. After installing the updated packages, the httpd daemon must be restarted for the update to take effect.

3.66. pidgin

3.66.1. RHSA-2014:0139 — Moderate: pidgin security update

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

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

Pidgin is an instant messaging program which can log in to multiple accounts on multiple instant messaging networks simultaneously.

Security Fixes

CVE-2013-6485

A heap-based buffer overflow flaw was found in the way Pidgin processed certain HTTP responses. A malicious server could send a specially crafted HTTP response, causing Pidgin to crash or potentially execute arbitrary code with the permissions of the user running Pidgin.

CVE-2013-6487, CVE-2013-6489, CVE-2013-6490

Multiple heap-based buffer overflow flaws were found in several protocol plug-ins in Pidgin (Gadu-Gadu, MXit, SIMPLE). A malicious server could send a specially crafted message, causing Pidgin to crash or potentially execute arbitrary code with the permissions of the user running Pidgin.

CVE-2012-6152, CVE-2013-6477, CVE-2013-6481, CVE-2013-6482, CVE-2013-6484, CVE-2014-0020

Multiple denial of service flaws were found in several protocol plug-ins in Pidgin (Yahoo!, XMPP, MSN, stun, IRC). A remote attacker could use these flaws to crash Pidgin by sending a specially crafted message.

CVE-2013-6483

It was found that the Pidgin XMPP protocol plug-in did not verify the origin of "iq" replies. A remote attacker could use this flaw to spoof an "iq" reply, which could lead to injection of fake data or cause Pidgin to crash via a NULL pointer dereference.

CVE-2013-6479

A flaw was found in the way Pidgin parsed certain HTTP response headers. A remote attacker could use this flaw to crash Pidgin via a specially crafted HTTP response header.

CVE-2013-6478

It was found that Pidgin crashed when a mouse pointer was hovered over a long URL. A remote attacker could use this flaw to crash Pidgin by sending a message containing a remote attacker could use this flaw to crash Pidgin by sending a message containing a long URL string.

Red Hat would like to thank the Pidgin project for reporting these issues. Upstream acknowledges Thijs Alkemade, Robert Vehse, Jaime Breva Ribes, Jacob Appelbaum of the Tor Project, Daniel Atallah, Fabian Yamaguchi and Christian Wressnegger of the University of Goettingen, Matt Jones of Volvent, and Yves Younan, Ryan Pentney, and Pawel Janic of Sourcefire VRT as the original reporters of these issues.

All pidgin users are advised to upgrade to these updated packages, which contain backported patches to correct these issues. Pidgin must be restarted for this update to take effect.

3.67. pixman

3.67.1. RHSA-2013:1869 — Important: pixman security update

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

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

Pixman is a pixel manipulation library for the X Window System and Cairo.

Security Fix

CVE-2013-6425

> An integer overflow, which led to a heap-based buffer overflow, was found in the way pixman handled trapezoids. If a remote attacker could trick an application using pixman into rendering a trapezoid shape with specially crafted coordinates, it could cause the application to crash or, possibly, execute arbitrary code with the privileges of the user running the application.

Users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. All applications using pixman must be restarted for this update to take effect.

3.68. postfix

3.68.1. RHBA-2014:1226 — postfix bug fix update

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

Postfix is a Mail Transport Agent (MTA), supporting LDAP, SMTP AUTH (SASL), and TLS.

Bug Fixes

BZ#915901

> Previously, the postfix packages had redundant explicitly specified dependencies. This could block from installing third party packages which fulfilled the implicit dependencies. To fix this bug, the redundant explicit dependencies have been removed. As a result, any third party packages can now be used.

BZ#977629

Previously, the Transport Layer Security (TLS) session cache was created in the /var/spool/postfix/ directory with the root user as owner. This could cause various problems if the cache was accessed by an unprivileged process of the tlsmgr daemon, including a tlsmgr failure. With this update, the TLS session cache I/O operations are redirected and the cache is now created in /var/lib/postfix/ with the correct Postfix owner.

Users of postfix are advised to upgrade to these updated packages, which fix these bugs. After installing this update, the postfix service will be restarted automatically.

3.69. postgresql

3.69.1. RHSA-2014:0249 — Important: postgresql security update

Updated postgresql packages that fix multiple security issues are now available for Red Hat Enterprise Linux 5.

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

PostgreSQL is an advanced object-relational database management system (DBMS).

Security Fixes

CVE-2014-0063

Multiple stack-based buffer overflow flaws were found in the date/time implementation of PostgreSQL. An authenticated database user could provide a specially crafted date/time value that, when processed, could cause PostgreSQL to crash or, potentially, execute arbitrary code with the permissions of the user running PostgreSQL.

CVE-2014-0064

Multiple integer overflow flaws, leading to heap-based buffer overflows, were found in various type input functions in PostgreSQL. An authenticated database user could possibly use these flaws to crash PostgreSQL or, potentially, execute arbitrary code with the permissions of the user running PostgreSQL.

CVE-2014-0065

Multiple potential buffer overflow flaws were found in PostgreSQL. An authenticated database user could possibly use these flaws to crash PostgreSQL or, potentially, execute arbitrary code with the permissions of the user running PostgreSQL.

CVE-2014-0060

It was found that granting an SQL role to a database user in a PostgreSQL database without specifying the "ADMIN" option allowed the grantee to remove other users from their granted role. An authenticated database user could use this flaw to remove a user from an SQL role which they were granted access to.

CVE-2014-0061

A flaw was found in the validator functions provided by PostgreSQL's procedural languages (PLs). An authenticated database user could possibly use this flaw to escalate their privileges.

CVE-2014-0062

A race condition was found in the way the CREATE INDEX command performed multiple independent lookups of a table that had to be indexed. An authenticated database user could possibly use this flaw to escalate their privileges.

CVE-2014-0066

It was found that the chkpass extension of PostgreSQL did not check the return value of the crypt() function. An authenticated database user could possibly use this flaw to crash PostgreSQL via a null pointer dereference.

Red Hat would like to thank the PostgreSQL project for reporting these issues. Upstream acknowledges Noah Misch as the original reporter of CVE-2014-0060 and CVE-2014-0063, Heikki Linnakangas and Noah Misch as the original reporters of CVE-2014-0064, Peter Eisentraut and Jozef Mlich as the original reporters of CVE-2014-0065, Andres Freund as the original reporter of CVE-2014-0061, Robert Haas and Andres Freund as the original reporters of CVE-2014-0062, and Honza Horak and Bruce Momjian as the original reporters of CVE-2014-0066.

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.

3.70. postgresql and postgresql84

3.70.1. RHSA-2013:1475 — Moderate: postgresql and postgresql84 security update

Updated postgresql and postgresql84 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 scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

PostgreSQL is an advanced object-relational database management system (DBMS).

Security Fixes

CVE-2013-0255

An array index error, leading to a heap-based out-of-bounds buffer read flaw, was found in the way PostgreSQL performed certain error processing using enumeration types. An unprivileged database user could issue a specially crafted SQL query that, when processed by the server component of the PostgreSQL service, would lead to a denial of service (daemon crash) or disclosure of certain portions of server memory.

CVE-2013-1900

A flaw was found in the way the pgcrypto contrib module of PostgreSQL (re)initialized its internal random number generator. This could lead to random numbers with less bits of entropy being used by certain pgcrypto functions, possibly allowing an attacker to conduct other attacks.

Red Hat would like to thank the PostgreSQL project for reporting these issues. Upstream acknowledges Sumit Soni via Secunia SVCRP as the original reporter of CVE-2013-0255, and Marko Kreen as the original reporter of CVE-2013-1900.

These updated packages upgrade PostgreSQL to version 8.4.18, 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-8-4-18.html

After installing this update, it is advisable to rebuild, using the REINDEX command, Generalized Search Tree (GiST) indexes that meet one or more of the following conditions:

- GiST indexes on box, polygon, circle, or point columns

- GiST indexes for variable-width data types, that is text, bytea, bit, and numeric

- GiST multi-column indexes

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.

3.71. postgresql84 and postgresql

3.71.1. RHSA-2014:0211 — Important: postgresql84 and postgresql security update

Updated postgresql84 and postgresql packages that fix multiple 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 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.

PostgreSQL is an advanced object-relational database management system (DBMS).

Security Fixes

CVE-2014-0063

> Multiple stack-based buffer overflow flaws were found in the date/time implementation of PostgreSQL. An authenticated database user could provide a specially crafted date/time value that, when processed, could cause PostgreSQL to crash or, potentially, execute arbitrary code with the permissions of the user running PostgreSQL.

CVE-2014-0064

> Multiple integer overflow flaws, leading to heap-based buffer overflows, were found in various type input functions in PostgreSQL. An authenticated database user could possibly use these flaws to crash PostgreSQL or, potentially, execute arbitrary code with the permissions of the user running PostgreSQL.

CVE-2014-0065

> Multiple potential buffer overflow flaws were found in PostgreSQL. An authenticated database user could possibly use these flaws to crash PostgreSQL or, potentially, execute arbitrary code with the permissions of the user running PostgreSQL.

CVE-2014-0060

It was found that granting an SQL role to a database user in a PostgreSQL database without specifying the "ADMIN" option allowed the grantee to remove other users from their granted role. An authenticated database user could use this flaw to remove a user from an SQL role which they were granted access to.

CVE-2014-0061

A flaw was found in the validator functions provided by PostgreSQL's procedural languages (PLs). An authenticated database user could possibly use this flaw to escalate their privileges.

CVE-2014-0062

A race condition was found in the way the CREATE INDEX command performed multiple independent lookups of a table that had to be indexed. An authenticated database user could possibly use this flaw to escalate their privileges.

CVE-2014-0066

It was found that the chkpass extension of PostgreSQL did not check the return value of the crypt() function. An authenticated database user could possibly use this flaw to crash PostgreSQL via a null pointer dereference.

Red Hat would like to thank the PostgreSQL project for reporting these issues. Upstream acknowledges Noah Misch as the original reporter of CVE-2014-0060 and CVE-2014-0063, Heikki Linnakangas and Noah Misch as the original reporters of CVE-2014-0064, Peter Eisentraut and Jozef Mlich as the original reporters of CVE-2014-0065, Andres Freund as the original reporter of CVE-2014-0061, Robert Haas and Andres Freund as the original reporters of CVE-2014-0062, and Honza Horak and Bruce Momjian as the original reporters of CVE-2014-0066.

These updated packages upgrade PostgreSQL to version 8.4.20, 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-8-4-19.html
http://www.postgresql.org/docs/8.4/static/release-8-4-20.html

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.

3.72. qspice

3.72.1. RHSA-2013:1474 — Important: qspice security update

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

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

The Simple Protocol for Independent Computing Environments (SPICE) is a remote display protocol for virtual environments. SPICE users can access a virtualized desktop or server from the local system or any system with network access to the server. SPICE is used in Red Hat Enterprise Linux for viewing virtualized guests running on the Kernel-based Virtual Machine (KVM) hypervisor or on Red Hat Enterprise Virtualization Hypervisors.

Security Fix

CVE-2013-4282

> A stack-based buffer overflow flaw was found in the way the reds_handle_ticket() function in the spice-server library handled decryption of ticket data provided by the client. A remote user able to initiate a SPICE connection to an application acting as a SPICE server could use this flaw to crash the application.

This issue was discovered by Tomas Jamrisko of Red Hat.

All qspice users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue.

3.73. redhat-release-notes

3.73.1. RHEA-2014:1238 — redhat-release-notes enhancement update

An updated redhat-release-notes package is now available for Red Hat Enterprise Linux 5.11 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 5.11 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 5.11.

The online Red Hat Enterprise Linux 5.11 Release Notes, which are located online at https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/5/html/5.11_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.

3.74. redhat-release

3.74.1. RHEA-2014:1230 — redhat-release enhancement update

Updated and enhanced redhat-release packages are now available for Red Hat Enterprise Linux 5.11.

The redhat-release packages contain licensing information regarding, and identifies the installed version of, Red Hat Enterprise Linux.

These updated redhat-release packages reflect changes made for the release of Red Hat Enterprise Linux 5.11.

Users of Red Hat Enterprise Linux 5.11 are advised to upgrade to these updated redhat-release packages.

3.75. redhat-support-lib-python

3.75.1. RHBA-2014:1202 — redhat-support-lib-python and redhat-support-tool update

Updated redhat-support-lib-python and redhat-support-tool packages that fix one bug and add one enhancement are now available for Red Hat Enterprise Linux 5.

The redhat-support-lib-python package provides a Python library that developers can use to easily write software solutions that leverage Red Hat Access subscription services.

The redhat-support-tool utility facilitates console-based access to Red Hat's subscriber services and gives Red Hat subscribers more venues for accessing the content and services available to them as Red Hat customers. Further, it enables our customers to integrate and automate their helpdesk services with our subscription services.

This update fixes the following bug:

Bug Fix

BZ#996553

Due to insufficient logs produced by the kernel download code, non-root users were not informed about lacking the necessary root privileges to download kernel debug symbols. To fix this bug, a log message which explains that root privileges are required to execute the findkerneldebugs and getkerneldebug commands has been added. In addition, the help for these two commands has been expanded to indicate that root privileges are required. Now, the non-root user has a better indication of which commands require root permissions.

The redhat-support-tool utility facilitates console-based access to Red Hat's subscriber services and gives Red Hat subscribers more venues for accessing the content and services available to them as Red Hat customers. Further, it enables our customers to integrate and automate their helpdesk services with our subscription services.

In addition, this update adds the following

Enhancement

BZ#995103

Issues such as low disk space or connectivity problems can interrupt the downloading of kernel debug symbols from Red Hat Network. Nevertheless, the user was not informed properly about the cause of this failure. With this update, error messages explaining why the kernel debug symbols failed to download are returned.

Users of redhat-support-lib-python and redhat-support-tool are advised to upgrade to these updated packages, which fix this bug and add this enhancement.

3.76. rgmanager

3.76.1. RHBA-2014:1207 — rgmanager bug fix and enhancement update

Updated rgmanager packages that fix several bugs and add one enhancement are now available for Red Hat Enterprise Linux 5.

The rgmanager packages contain the Red Hat Resource Group Manager, which is used to create and manage high-availability server applications in the event of system downtime.

Bug Fixes

BZ#853083

When a cluster configuration file was invalid, an attempt to run the "clustat" command failed with a segmentation fault. This bug has been fixed with this update and "clustat" no longer crashes in the described scenario.

BZ#997546

Previously, the cluster services file system failed over from one node to another if the /tmp/ directory filled up. A patch has been provided to fix this bug and cluster services no longer fail over.

BZ#1016784

Recent changes in the lvm_by_lv script introduced a bug that caused all Logical Volume Management (LVM) status checks to fail. Consequently, when using high availability LVM (HA-LVM) with tagging made by LV, multiple warning and error messages were emitted while attempting to start a configured LVM resource. The LVM resource subsequently failed to start with a "vg/lv should not be active" error message. With this update, lvm_by_lv has been modified to remove white spaces from lvm commands that determine the resource owner. LVM status checks now succeed as expected and LVM resources are started properly.

BZ#1020279

Due to a syntax error in the underlying source code, the "find" command failed to find files whose names ended with the ".img" suffix. This update applies a patch to fix this bug and the command now works as expected.

BZ#1022723

If the "listener_name" attribute was omitted for the oracledb.sh resource agent script, the oracledb resources failed to start. With this update, oracledb.sh has been modified to operate correctly when no "listener_name" is given, and thus now starts as expected.

BZ#1035023

In certain environments, the hard-coded sleep time used in the agent process before trying to connect to the postmaster process was not long enough. As a consequence, the postgres-8 service terminated unexpectedly. With this update, the postgres-8.sh script has been modified to allow users to configure the sleep time according to their needs.

BZ#1035034

Under certain conditions, the postgres-8 service did not shut down gracefully and left the PID file populated. Consequently, the service failed to start after the reboot. The underlying source code has been modified and postgres-8 now works as expected.

BZ#1047989

Previously, the oralistener resource agent failed to stop when the listener process was no longer running. This update provides a patch to fix this bug and oralistener works correctly in the described scenario.

In addition, this update adds the following

Enhancement

BZ#924694

This update adds the possibility to specify the "timeout" parameter for the Xen virtual machines when using the "xm" command.

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

3.77. rhn-client-tools

3.77.1. RHBA-2014:1215 — rhn-client-tools bug fix update

Updated rhn-client-tools packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

Red Hat Network Client Tools provide programs and libraries that allow a system to receive software updates from Red Hat Network.

Bug Fixes

BZ#1093157

Red Hat Network Client Tools did not count the CPU socket information on certain systems properly. With this update, rhn-client-tools parse the /proc/cpuinfo file correctly and thus provide the correct CPU socket information for all systems.

BZ#751294

The error logging module did not correctly determine sub-classes of YUM errors, causing such errors to throw a traceback rather than being correctly logged or reported on the command line. This update ensures that all errors are logged and reported properly by correcting the error inheritance structure.

BZ#919432

The rhn-client-tools sub-package did not correctly mark itself as conflicting with old versions of the rhn-virtualization-host package, which allowed the rhn-client-tools to be installed on the system with such an old package. As a consequence, the rhn-profile-sync utility returned an "exceptions.TypeError: refresh() takes no arguments (1 given)" traceback when it was run. With this update, the conflicting package versions are correctly marked in the rhn-client-tools spec file, which prevents installations of incompatible packages.

Users of rhn-client-tools are advised to upgrade to these updated packages, which fix these bugs.

3.78. samba

3.78.1. RHSA-2014:0305 — Moderate: samba security update

Updated samba 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 Moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Samba is an open-source implementation of the Server Message Block (SMB) or Common Internet File System (CIFS) protocol, which allows PC-compatible machines to share files, printers, and other information.

Security Fixes

CVE-2013-0213

It was discovered that the Samba Web Administration Tool (SWAT) did not protect against being opened in a web page frame. A remote attacker could possibly use this flaw to conduct a clickjacking attack against SWAT users or users with an active SWAT session.

CVE-2013-0214

A flaw was found in the Cross-Site Request Forgery (CSRF) protection mechanism implemented in SWAT. An attacker with the knowledge of a victim's password could use this flaw to bypass CSRF protections and conduct a CSRF attack against the victim SWAT user.

CVE-2013-4124

An integer overflow flaw was found in the way Samba handled an Extended Attribute (EA) list provided by a client. A malicious client could send a specially crafted EA list that triggered an overflow, causing the server to loop and reprocess the list using an excessive amount of memory.

Note: This issue did not affect the default configuration of the Samba server.

Red Hat would like to thank the Samba project for reporting CVE-2013-0213 and CVE-2013-0214. Upstream acknowledges Jann Horn as the original reporter of CVE-2013-0213 and CVE-2013-0214.

All users of Samba are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the smb service will be restarted automatically.

3.78.2. RHBA-2014:1241 — samba bug fix update

Updated samba packages that fix one 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#1132425

Dropbox is a directory with permission 0733. Previously, when the user was trying to store a file in a dropbox directory, the file could not be created. As a consequence, an ACCESS_DENIED error was returned. The permissions to such a directory are now correctly processed by the smbd daemon, and the user can save files to a dropbox directory again.

Users of samba are advised to upgrade to these updated packages, which fix this bug. After installing this update, the smb service will be restarted automatically.

3.79. samba and samba3x

3.79.1. RHSA-2013:1806 — Important: samba and samba3x security update

Updated samba3x and samba 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 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.

Samba is an open-source implementation of the Server Message Block (SMB) or Common Internet File System (CIFS) protocol, which allows PC-compatible machines to share files, printers, and other information.

Security Fixes

CVE-2013-4408

> A heap-based buffer overflow flaw was found in the DCE-RPC client code in Samba. A specially crafted DCE-RPC packet could cause various Samba programs to crash or, possibly, execute arbitrary code when parsed. A malicious or compromised Active Directory Domain Controller could use this flaw to compromise the winbindd daemon running with root privileges.

CVE-2013-4475

> A flaw was found in the way Samba performed ACL checks on alternate file and directory data streams. An attacker able to access a CIFS share with alternate stream support enabled could access alternate data streams regardless of the underlying file or directory ACL permissions.

Red Hat would like to thank the Samba project for reporting CVE-2013-4408. Upstream acknowledges Stefan Metzmacher and Michael Adam of SerNet as the original reporters of this issue.

All users of Samba are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the smb service will be restarted automatically.

3.79.2. RHSA-2014:0330 — Moderate: samba and samba3x security update

Updated samba3x and samba 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 scores, which give detailed severity ratings, are available for each vulnerability from the CVE links 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 Fixes

CVE-2013-4496

> It was found that certain Samba configurations did not enforce the password lockout mechanism. A remote attacker could use this flaw to perform password guessing attacks on Samba user accounts. Note: this flaw only affected Samba when deployed as a Primary Domain Controller.

CVE-2012-6150

A flaw was found in the way the pam_winbind module handled configurations that specified a non-existent group as required. An authenticated user could possibly use this flaw to gain access to a service using pam_winbind in its PAM configuration when group restriction was intended for access to the service.

Red Hat would like to thank the Samba project for reporting CVE-2013-4496 and Sam Richardson for reporting CVE-2012-6150. Upstream acknowledges Andrew Bartlett as the original reporter of CVE-2013-4496.

All users of Samba are advised to upgrade to these updated packages, which contain backported patches to correct these issues. After installing this update, the smb service will be restarted automatically.

3.79.3. RHBA-2014:1212 — samba3x bug fix and enhancement update

Updated samba3x packages that fix several 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.

This update also fixes the following bugs:

> **Upgrade to an upstream version**
>
> The samba3x packages have been upgraded to upstream version 3.6.23, which provides a number of bug fixes and enhancements over the previous version. Note that this also changes the format of the Trivial Database (TDB) files, and the existing TDB files are updated to conform to the new format when you upgrade your Samba packages. In addition, earlier versions of Samba are not compatible with the new TDB file format. In order to successfully downgrade to an earlier version of Samba, you must use a backed up version of your TDB files, which uses the previous formatting. (BZ#1035006)

This update also fixes the following bugs:

Bug Fixes

BZ#1109436

Due to incorrect Security Identifier (SID) mappings for Access Control List (ACL) files, generating a user access token previously sometimes failed. With this update, the conversion of SID values for ACL files has been amended and user access tokens are created as expected.

BZ#981369

Prior to this update, an incorrect return value check caused the fallback from TCP/IP to a named pipe to fail. As a consequence, it was not possible to create a Local Security Authority (LSA) query for user and group information. This update fixes the check of the above return value, allowing the fallback to a named pipe to occur. As a result, LSA querying over a named pipe now works as expected.

BZ#1033773

Prior to this update, the search string of the function encoding the Lightweight Directory Access Protocol (LDAP) binary, ldb_binary_encode(), detected the used character set incorrectly. As a consequence, Samba generated invalid search strings. This update fixes the encoding of the local string, and Samba now generates valid LDAP search strings.

BZ#1081002

Previously, Samba always wrote a negative cache entry for the user map. As a consequence, user name mapping did not function consistently. With this update, Samba only writes a negative cache entry if the mapping fails, and user name mapping now works correctly.

BZ#996656

When the smbd server daemon executed spooling for a print action, it previously did not include the job ID in the generated spool-file path. As a consequence, the spool check could not validate the spool-file's existence, and the printing thus failed. With this update, smbd includes the job ID in the spool-file path and parsing the file name succeeds. As a result, printing via Samba now works as expected.

The samba3x packages have been upgraded to upstream version 3.6.23, which provides a number of bug fixes and enhancements over the previous version. Note that this also changes the format of the Trivial Database (TDB) files, and the existing TDB files are updated to conform to the new format when you upgrade your Samba packages. In addition, earlier versions of Samba are not compatible with the new TDB file format. In order to successfully downgrade to an earlier version of Samba, you must use a backed up version of your TDB files, which uses the previous formatting. (BZ#1035006)

In addition, this update adds the following

Enhancements

BZ#1037273

A timeout option has been added to the smbclient command-line tool. This allows users to customize the timeout value for Samba file operations by using the "smbclient --help | grep timeout" command.

BZ#1101922

It is now possible to set a different OS version for the Spool Subsystem (spoolss) configuration. This allows users to work around situations where printing drivers do not interact with the printing server because they detect that the version of the printing server is too old.

Users of Samba are advised to upgrade to these updated packages, which fix these bugs and add these enhancements. After installing this update, the smb service will be restarted automatically.

3.80. sblim

3.80.1. RHBA-2014:1201 — sblim bug fix update

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

Standards-Based Linux Instrumentation for Manageability (SBLIM) consists of a set of standards-based, Web-Based Enterprise Management (WBEM) modules that use the Common Information Model (CIM) standard to gather and provide systems management information, events, and methods to local or networked consumers via an CIM object services broker using the CMPI (Common

Manageability Programming Interface) standard. This package provides a set of core providers and development tools for systems management applications.

Bug Fixes

BZ#921485

Previously, if the /etc/fstab file entry used symbolic link, UUID, or LABEL for identifying a device or a file system, these file systems or devices were reported to be disabled although they were mounted. A patch has been applied to fix this bug, and file systems and devices are now correctly reported as mounted.

BZ#959892

Previously, the wbemcli CIM Client did not accept full stop (.) as a password character on the command line. With the updated source code, the user is no longer limited in the use of full stops because passwords containing this character are now accepted.

BZ#971056

While enumerating the Linux_Processor class instances on systems with dynamic CPU frequencies, the MaxClockSpeed property was determined incorrectly. It showed the same value as the CurrentClockSpeed property, which is supposed to be lower. The underlying source code has been modified, and the value of MaxClockSpeed now correctly shows the real maximum processor clock speed.

BZ#974075

Prior to this update, the sblim-cmpi-base provider was scanning wrong fields of the /proc/[pid]/stat file. Consequently, the values for UserModeTime and KernelModeTime properties in CIM class Linux_UnixProcess were incorrectly calculated. With this update, correct fields are read, and UserModeTime and KernelModeTime are calculated correctly.

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

3.81. scl-utils

3.81.1. RHBA-2014:1229 — scl-utils bug fix and enhancement update

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

The scl-utils packages provide a runtime utility and RPM packaging macros for packaging Software Collections. Software Collections allow users to concurrently install multiple versions of the same RPM packages on the system. Using the scl utility, users may enable specific versions of RPMs, which are installed into the /opt directory.

Bug Fixes

BZ#1040859

In previous versions of scl-utils, the working directory was changed during package build time, which caused complications to package maintainers. These complications ranged from mild inconveniences to build failures if the code in the spec file worked with the working directory. This bug has been fixed, and the working directory no longer changes during build time.

BZ#1040860

When building the SCL "noarch" meta packages on a 64-bit machine, the build failed with an error message. To fix this bug, the "%ifarch" conditionals have been changed, and affected packages are now built correctly.

In addition, this update adds the following

Enhancements

BZ#1040861

This update introduces a new way to call the "scl enable" command. The scl utility now supports the double dash (--) as a separator between collections and the command; using the separator makes calling the "scl enable" command more convenient.

BZ#1040858

Previously, it was impossible to specify runtime dependencies between collections. For example, if one collection depended on another, the user had to enable both of them manually. With this update, a collection can enable another collection implicitly during startup.

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

3.82. selinux-policy

3.82.1. RHBA-2014:1205 — selinux-policy bug fix update

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

The selinux-policy packages contain the rules that govern how confined processes run on the system.

Bug Fixes

BZ#959217

Due to missing rules in the SELinux policy, the sssd_t domain could not connect to port 464. With this update, the appropriate rules have been added to the policy and sssd_t now connects to that port as expected.

BZ#984453

Previously, SELinux prevented the fence_xvm agent from fencing nodes even if the fenced_can_network_connect Boolean was enabled. The SELinux policy has been modified to fix this bug and SELinux no longer blocks fence_xvm in the described scenario.

BZ#997710

Due to missing rules in the SELinux policy, SELinux did not allow the dovecot_deliver_t process to send the SIGNULL signal. With this update, the SELinux rules have been modified accordingly and SELinux no longer prevents dovecot_deliver_t from sending SIGNULL.

BZ#1005589

Previously, SELinux prevented the iptables_t process from using the inotify utility to monitor file system activity. This update adds appropriate SELinux rules and iptables_t can use inotify as expected.

BZ#1008472

When SELinux was in enforcing mode, the glibc library was unable to update the /etc/localtime file. The SELinux policy has been modified to fix this bug and glibc can now update the file as expected.

BZ#1053050

Due to missing SELinux rules, the automount utility could not read symbolic links, which caused the AVC denial messages to return. With this update, the SELinux policy has been modified and SELinux no longer prevents automount from reading symbolic links.

BZ#1078357

Previously, the restorecon command failed to restore the SELinux context on a file located in a symbolically linked directory. The underlying source code has been modified to fix this bug and restorecon now works correctly in the described scenario.

BZ#1083491

Previously, the smbd daemon service was unable to connect to the nmbd service using a Unix stream socket, which caused AVC messages to be logged in the /var/log/audit/audit.log file. To fix this bug, a set of new rules has been added to the SELinux policy to allow smbd to connect to nmbd.

BZ#1089006

An attempt to start a clustered service with the postgres-8 resource script failed due to a bug in the SELinux policy. With this update, the policy has been modified and the service now starts as expected.

BZ#1096891

Due to missing rules in the SELinux policy, the radiusd daemon was unable to write to the /tmp/ directory. Consequently, when radiusd was integrated with the Kerberos network authentication system, an attempt to authenticate a user failed. This update applies a new SELinux policy module so that radiusd works correctly in the described scenario.

BZ#1098031

The zarafa-indexer package has been replaced with the zarafa-search package. Previously, the zarafa-search utility was not labeled with the same SELinux context as the zarafa-indexer utility. With this update, the appropriate SELinux policy rules have been modified and zarafa-search now runs in the zarafa_indexer_t domain as expected.

Users of selinux-policy are advised to upgrade to these updated packages, which fix these bugs.

3.83. shadow-utils

3.83.1. RHBA-2014:1217 — shadow-utils bug fix update

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

The shadow-utils packages include programs for converting UNIX password files to the shadow password format, as well as utilities for managing user and group accounts.

Bug Fix

BZ#985475

Due to the previously added support for the split groups, the newgrp command searched all groups on the system for a given GID. This behavior could cause high network traffic on systems pulling user and group information from a Lightweight Directory Access Protocol (LDAP) server. The underlying source code has been modified, so that this exhaustive search is not performed if the user is a member of a group whose name is specified with newgrp.

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

3.84. sos

3.84.1. RHBA-2014:1200 — sos bug fix update

The updated sos package that fixes several bugs is now available for Red Hat Enterprise Linux 5.

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

Bug Fixes

BZ#833406

Previously, the sosreport utility did not include the output of the "brctl show" command for all systems. Consequently, information on bridged network configurations was only available in the report tarball on systems using Xen for virtualization. With this update, the networking module collects the output of "brctl show" as well as "brctl showstp" commands for each configured bridge, and thus bridged network configuration information is now available in the report tarball for all hosts.

BZ#980177

Previous versions of the sosreport utility used the legacy ifconfig command to detect network interfaces, but ifconfig did not support interfaces named via biosdevname. As a consequence, no information on biosdevname interfaces was present in the report tarball. With this update, the sosreport networking plug-in now uses the "ip" command to detect interfaces of all types, and full information on biosdevname interfaces is now included.

BZ#1029017

Previously, the sosreport utility collected the krb5.keytab file from Kerberos installations. Although encrypted, this file can contain sensitive key material. With this update, sosreport collects a summary of krb5.keytab using the klist command but does not collect the krb5.keytab file itself. As a result, krb5.keytab data is still available but no sensitive information is included in the report tarball.

BZ#1086736

Previously, the sosreport "ds" plug-in collected all directory server logs by default. Depending on the log configuration, this could lead to very large report sizes. With this update, sosreport collects by default only the current version of the directory server logs regarding to "access", "errors" and "audit", and rotated logs are not collected by default. In addition, the plug-in now supports an "all_logs" option that can be used to request the old behavior. As a result, the default report size for directory server hosts is now smaller and more consistent unless full log data is explicitly requested.

BZ#1107751

Prior to this update, the sosreport utility could include password material in the grub.conf and fstab files collected by the boot loader and file system plug-ins if present on the collection system. Consequently, passwords, either plain text or hashed, could be included in the report tarball. With this bug fix update, password and other secrets are now removed during collection, and passwords from the fstab or grub.conf files can no longer appear in the report tarball.

Users of sos are advised to upgrade to this updated package, which fixes these bugs.

3.85. sssd

3.85.1. RHBA-2014:1237 — sssd bug fix update

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

The System Security Services Daemon (SSSD) provides a set of daemons to manage access to remote directories and authentication mechanisms. It provides the Name Service Switch (NSS) and the Pluggable Authentication Modules (PAM) interfaces toward the system and a pluggable back-end system to connect to multiple different account sources.

Bug Fix

BZ#1000205

Prior to this update, when a dynamic Domain Name System (DNS) update operation timed out, it unintentionally freed specific data related to the update. Consequently, a child_handler() call attempted to access this data, which caused the sssd_be process to terminate unexpectedly with a segmentation fault. With this update, child_handler() is destroyed when a dynamic DNS update times out and sssd_be thus no longer crashes in the described scenario.

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

3.86. struts

3.86.1. RHSA-2014:0474 — Important: struts security update

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

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

Apache Struts is a framework for building web applications with Java.

Security Fix

CVE-2014-0114

> It was found that the Struts 1 ActionForm object allowed access to the 'class' parameter, which is directly mapped to the getClass() method. A remote attacker could use this flaw to manipulate the ClassLoader used by an application server running Struts 1. This could lead to remote code execution under certain conditions.

All struts users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. All running applications using struts must be restarted for this update to take effect.

3.87. subscription-manager

3.87.1. RHBA-2014:1225 — subscription-manager bug fix and enhancement update

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

The Subscription Manager packages provide programs and libraries to allow users to manage subscriptions and yum repositories from the Red Hat entitlement platform.

This update fixes multiple bugs and adds various enhancements, the most notable of which are detailed below.

* This update adds support for repository overrides to the Subscription Manager. Repositories are now written with server-side overrides taken into account. This feature gives more control in managed environments. (BZ#1086316)

* This update adds the "Quantity Needed" field in the output of the "subscription-manager list --available" command. The value in this field is the suggested quantity of subscription instances needed to achieve compliance. Note that the maximum suggested quantity is the number of subscriptions available for the user, even if more are required for compliance. This feature prevents the Subscription Manager from using "1" as a default quantity and also ensures better parity with the GUI tool. (BZ#1088372)

* This update adds the "Subscription Type" field in the output of the "subscription-manager list --available" command. This field displays the subscription type, for example "Instance Based", and also supports new types on old clients. (BZ#1086290)

* This update adds the rhsm-debug tool to the subscription-manager packages to improve debugging of subscription-related problems. (BZ#1039653)

Bug Fixes

BZ#1086316

> This update adds support for repository overrides to the Subscription Manager. Repositories are now written with server-side overrides taken into account. This feature gives more control in managed environments.

BZ#1088372

> This update adds the "Quantity Needed" field in the output of the "subscription-manager list --available" command. The value in this field is the suggested quantity of subscription instances needed to achieve compliance. Note that the maximum suggested quantity is the number of subscriptions available for the user, even if more are required for compliance. This feature prevents the Subscription Manager from using "1" as a default quantity and also ensures better parity with the GUI tool.

BZ#1086290

This update adds the "Subscription Type" field in the output of the "subscription-manager list --available" command. This field displays the subscription type, for example "Instance Based", and also supports new types on old clients.

BZ#1039653

This update adds the rhsm-debug tool to the subscription-manager packages to improve debugging of subscription-related problems.

This update fixes multiple bugs and adds various enhancements, the most notable of which are detailed below.

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

3.88. subversion

3.88.1. RHSA-2014:0255 — Moderate: subversion security update

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

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

Subversion (SVN) is a concurrent version control system which enables one or more users to collaborate in developing and maintaining a hierarchy of files and directories while keeping a history of all changes. The mod_dav_svn module is used with the Apache HTTP Server to allow access to Subversion repositories via HTTP.

Security Fixes

CVE-2014-0032

A flaw was found in the way the mod_dav_svn module handled OPTIONS requests. A remote attacker with read access to an SVN repository served via HTTP could use this flaw to cause the httpd process that handled such a request to crash.

CVE-2013-1968

A flaw was found in the way Subversion handled file names with newline characters when the FSFS repository format was used. An attacker with commit access to an SVN repository could corrupt a revision by committing a specially crafted file.

CVE-2013-2112

A flaw was found in the way the svnserve tool of Subversion handled remote client network connections. An attacker with read access to an SVN repository served via svnserve could use this flaw to cause the svnserve daemon to exit, leading to a denial of service.

All subversion users should upgrade to these updated packages, which contain backported patches to correct these issues. After installing the updated packages, for the update to take effect, you must restart the httpd daemon, if you are using mod_dav_svn, and the svnserve daemon, if you are serving Subversion repositories via the svn:// protocol.

3.89. sudo

3.89.1. RHSA-2014:0266 — Moderate: sudo security update

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

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

The sudo (superuser do) utility allows system administrators to give certain users the ability to run commands as root.

Security Fix

CVE-2014-0106

> A flaw was found in the way sudo handled its blacklist of environment variables. When the "env_reset" option was disabled, a user permitted to run certain commands via sudo could use this flaw to run such a command with one of the blacklisted environment variables set, allowing them to run an arbitrary command with the target user's privileges.

Note: This issue does not affect the default configuration of the sudo package as shipped with Red Hat Enterprise Linux 5.

Red Hat would like to thank Todd C. Miller for reporting this issue. Upstream acknowledges Sebastien Macke as the original reporter.

All sudo users are advised to upgrade to this updated package, which contains a backported patch to correct this issue.

3.90. sysstat

3.90.1. RHBA-2014:1199 — sysstat bug fix update

Updated sysstat packages that fix several 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#804890, BZ#885571

> Previously, the sysstat packages did not support dynamically attributed major device numbers. Consequently, devices with these numbers were not listed in sar reports under their real names. With this update, support for dynamically attributed major device numbers has been added to sysstat. As a result, all devices now appear with their correct names in sar reports.

BZ#837238

Previously, the "sar -dp" command did not translate device-mapper device names. As a consequence, block devices under device-mapper were listed as "nodev" instead of their proper names. The underlying source has been modified to fix this bug and the devices are now displayed with the proper names as expected.

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

3.91. system-config-network

3.91.1. RHBA-2014:1195 — system-config-network bug fix update

Updated *system-config-network* packages that fix several bugs are now available for Red Hat Enterprise Linux 5.

`System-config-network` is the user interface of the network configuration tool, supporting Ethernet, Wireless, TokenRing, ADSL, ISDN and PPP.

Bug Fixes

BZ#445958

Previously, the **`system-config-network`** service failed to recognize the **`Monitor`** mode configuration of a WIFI device and as a consequence, the service terminated unexpectedly with a traceback. This update provides a patch to fix this bug and **`system-config-network`** no longer crashes in the described scenario.

BZ#452446

In certain cases, when the user dismissed a dialog immediately when it popped up, the **`system-config-network`** service could terminate unexpectedly. The service has been modified to verify properly if the dialog has been dismissed already, thus it no longer fails in such a case.

BZ#452776

Previously, the **`system-config-network-cmd --import`** command did not correctly handle bonding interfaces. Consequently, when using this command to import a setting generated with the **`system-config-network-cmd --export`** command, the configuration for bonding interfaces was lost. This bug has been fixed and **`system-config-network-cmd --import`** now works as expected.

BZ#474515

Due to a bug in the GUI handling, the **`system-config-network`** service occasionally terminated unexpectedly when displaying the interfaces. The underlying source code has been modified to fix this bug and **`system-config-network`** no longer fails in the described scenario.

BZ#514534

When creating several device aliases for the same interfaces, the **`system-config-network`** service did not store the correct device name in the configuration file. As a consequence, the interface was started with an incorrect interface name. With this update, **`system-config-network`** now correctly stores the device aliases and interfaces are named properly.

BZ#516496

Previously, the **system-config-network** service did not handle correctly those entries in the **/etc/hosts/** directory that were specified only with an IP address and with no host name. Consequently, **system-config-network** failed. This bug has been fixed and **system-config-network** now works properly in the described scenario.

BZ#545286

When interface aliases were not specified using numbers only, the **system-config-network** service terminated unexpectedly. This update applies a patch that modifies **system-config-network** to warn the user when the interface aliases are not specified using numbers only.

BZ#656529, BZ#805806, BZ#919656, BZ#950988

Early versions of the Python programming language do not switch to the UTF-8 format correctly. This behavior led to a failure of the **system-config-network** service when some UTF-8 character were presented in configuration files. With this update, **system-config-network** now resets the Python internals to properly handle UTF-8 so that **system-config-network** no longer crashes in the described scenario.

BZ#679000

Previously, when changing host names with the **system-config-network** service, the service did not remove the old host name from the **/etc/hosts/** directory and did not add the new host name. This update applies a patch to fix this bug so that **/etc/hosts** now contains the updated host name as expected.

BZ#765727

Certain **system-config-network** user interface elements were not marked as translatable and therefore they were not translated. This bug has been fixed and all user elements are now correctly translated to the language set by the user if a translation exits for it.

BZ#791335

The text user interface version of the **system-config-network** service, **system-config-network-tui**, did not store the network configuration correctly after the system was cleaned with the **sys-unconfig** command. As a consequence, no network configuration was stored in the **/etc/sysconfig/network-scripts/** directory. With this update, even if no previous configuration exists, **system-config-network-tui** stores the configuration in that directory as expected. As a result, a network configured with **system-config-network-tui** works after executing **sys-unconfig**.

BZ#825767

Previously, the *dbus-python* package was missing from the **system-config-network-tui** dependency list. Consequently, when the *system-config-network-tui* package was installed on a system with a minimal installation of Red Hat Enterprise Linux, the **system-config-network-tui** utility failed to start. The missing dependency has been added to the dependency list of **system-config-network-tui**, thus the utility works as expected in the described scenario.

BZ#955310

Due to a typo in the underlying source code, the **system-config-network** service was unable to configure anything else than Ethernet devices, which led to the service terminate unexpectedly on any other hardware devices. With this update, the typo has been fixed and **system-config-network** no longer crashes in such a case.

Users of *system-config-network* are advised to upgrade to these updated packages, which fix these bugs.

3.92. thunderbird

3.92.1. RHSA-2014:0742 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fix

CVE-2014-1533, CVE-2014-1538, CVE-2014-1541

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

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Gary Kwong, Christoph Diehl, Christian Holler, Hannes Verschore, Jan de Mooij, Ryan VanderMeulen, Jeff Walden, Kyle Huey, Abhishek Arya, and Nils as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

For technical details regarding these flaws, refer to the Mozilla security advisories for Thunderbird 24.6.0.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 24.6.0, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

3.92.2. RHSA-2014:0133 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2014-1477, CVE-2014-1482, CVE-2014-1486

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-2014-1487

A flaw was found in the way Thunderbird handled error messages related to web workers. An attacker could use this flaw to bypass the same-origin policy, which could lead to cross-site scripting (XSS) attacks, or could potentially be used to gather authentication tokens and other data from third-party websites.

CVE-2014-1479

A flaw was found in the implementation of System Only Wrappers (SOW). An attacker could use this flaw to crash Thunderbird. When combined with other vulnerabilities, this flaw could have additional security implications.

CVE-2014-1481

It was found that the Thunderbird JavaScript engine incorrectly handled window objects. A remote attacker could use this flaw to bypass certain security checks and possibly execute arbitrary code.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Christian Holler, Terrence Cole, Jesse Ruderman, Gary Kwong, Eric Rescorla, Jonathan Kew, Dan Gohman, Ryan VanderMeulen, Sotaro Ikeda, Cody Crews, Fredrik "Flonka" Lönnqvist, Arthur Gerkis, Masato Kinugawa, and Boris Zbarsky as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

For technical details regarding these flaws, refer to the Mozilla security advisories for Thunderbird 24.3.0.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 24.3.0, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

3.92.3. RHSA-2013:1480 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-5590, CVE-2013-5597, CVE-2013-5599, CVE-2013-5600, CVE-2013-5601, CVE-2013-5602

Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-5595

> It was found that the Thunderbird JavaScript engine incorrectly allocated memory for certain functions. An attacker could combine this flaw with other vulnerabilities to execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-5604

> A flaw was found in the way Thunderbird handled certain Extensible Stylesheet Language Transformations (XSLT) files. An attacker could combine this flaw with other vulnerabilities to execute arbitrary code with the privileges of the user running Thunderbird.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Jesse Ruderman, Christoph Diehl, Dan Gohman, Byoungyoung Lee, Nils, and Abhishek Arya as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

For technical details regarding these flaws, refer to the Mozilla security advisories for Thunderbird 17.0.10 ESR.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 17.0.10 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

3.92.4. RHSA-2014:0316 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2014-1493, CVE-2014-1510, CVE-2014-1511, CVE-2014-1512, CVE-2014-1513, CVE-2014-1514

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

CVE-2014-1497, CVE-2014-1508, CVE-2014-1505

> Several information disclosure flaws were found in the way Thunderbird processed malformed web content. An attacker could use these flaws to gain access to sensitive information such as cross-domain content or protected memory addresses or, potentially, cause Thunderbird to crash.

CVE-2014-1509

A memory corruption flaw was found in the way Thunderbird rendered certain PDF files. An attacker able to trick a user into installing a malicious extension could use this flaw to crash Thunderbird or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Benoit Jacob, Olli Pettay, Jan Varga, Jan de Mooij, Jesse Ruderman, Dan Gohman, Christoph Diehl, Atte Kettunen, Tyson Smith, Jesse Schwartzentruber, John Thomson, Robert O'Callahan, Mariusz Mlynski, Jüri Aedla, George Hotz, and the security research firm VUPEN as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially-crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

For technical details regarding these flaws, refer to the Mozilla security advisories for Thunderbird 24.4.0.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 24.4.0, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

3.92.5. RHSA-2014:0449 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2014-1518, CVE-2014-1524, CVE-2014-1529, CVE-2014-1531

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

CVE-2014-1532

A use-after-free flaw was found in the way Thunderbird resolved hosts in certain circumstances. An attacker could use this flaw to crash Thunderbird or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2014-1523

An out-of-bounds read flaw was found in the way Thunderbird decoded JPEG images. Loading an email or a web page containing a specially crafted JPEG image could cause Thunderbird to crash.

CVE-2014-1530

A flaw was found in the way Thunderbird handled browser navigations through history. An attacker could possibly use this flaw to cause the address bar of the browser to display a web page name while loading content from an entirely different web page, which could allow for cross-site scripting (XSS) attacks.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Bobby Holley, Carsten Book, Christoph Diehl, Gary Kwong, Jan de Mooij, Jesse Ruderman, Nathan Froyd, Christian Holler, Abhishek Arya, Mariusz Mlynski, moz_bug_r_a4, Nils, Tyson Smith and Jesse Schwartzentrube as the original reporters of these issues.

Note: All of the above issues cannot be exploited by a specially crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

For technical details regarding these flaws, refer to the Mozilla security advisories for Thunderbird 24.5.0.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 24.5.0, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

3.92.6. RHSA-2013:1823 — Important: thunderbird security update

An updated thunderbird package that fixes several security issues is now available for Red Hat Enterprise Linux 5 and 6.

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

Mozilla Thunderbird is a standalone mail and newsgroup client.

Security Fixes

CVE-2013-5609, CVE-2013-5616, CVE-2013-5618, CVE-2013-6671, CVE-2013-5613

> Several flaws were found in the processing of malformed content. Malicious content could cause Thunderbird to crash or, potentially, execute arbitrary code with the privileges of the user running Thunderbird.

CVE-2013-5612

> A flaw was found in the way Thunderbird rendered web content with missing character encoding information. An attacker could use this flaw to possibly bypass same-origin inheritance and perform cross site-scripting (XSS) attacks.

CVE-2013-5614

> It was found that certain malicious web content could bypass restrictions applied by sandboxed iframes. An attacker could combine this flaw with other vulnerabilities to execute arbitrary code with the privileges of the user running Thunderbird.

Note: All of the above issues cannot be exploited by a specially crafted HTML mail message as JavaScript is disabled by default for mail messages. They could be exploited another way in Thunderbird, for example, when viewing the full remote content of an RSS feed.

Red Hat would like to thank the Mozilla project for reporting these issues. Upstream acknowledges Ben Turner, Bobby Holley, Jesse Ruderman, Christian Holler, Masato Kinugawa, Daniel Veditz, Jesse Schwartzentruber, Nils, Tyson Smith, and Atte Kettunen as the original reporters of these issues.

For technical details regarding these flaws, refer to the Mozilla security advisories for Thunderbird 24.2.0 ESR.

All Thunderbird users should upgrade to this updated package, which contains Thunderbird version 24.2.0 ESR, which corrects these issues. After installing the update, Thunderbird must be restarted for the changes to take effect.

3.93. tzdata

3.93.1. RHBA-2014:0295 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 4, 5, and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#1065930, BZ#1065928, BZ#1065926

The Turkish government decided to delay the start of daylight saving time (DST) in Turkey this year. DST will begin at 3 a.m. on Monday, March 31 instead of 3 a.m. on Sunday, March 30. The respective tzdata rules have been updated to reflect this change.

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

3.93.2. RHEA-2013:1867 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 3, 4, 5, and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#1043502, BZ#1043508, BZ#1043511, BZ#1043512

The Jordanian government has reversed its decision to observe daylight saving time (DST) all year and in the year 2014, Jordan is going to resume to the transition schedule from the years 2006 - 2011. This year, Jordan will switch back to Arabia Standard Time (AST) at 00:00 on December the 20th.

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

3.93.3. RHEA-2013:1432 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 3, 4, 5, and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#1013527, BZ#1013875, BZ#1013876, BZ#1014720

Morocco extended DST by one month requiring an update to these packages. This update includes resynchronization with the latest upstream release in order to pick up the Moroccan DST change.

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

3.93.4. RHBA-2014:0101 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 3, 4, 5, and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#1054919, BZ#1054921, BZ#1054922, BZ#1054923

> This update retroactively changes the Daylight Saving Time (DST) rules for Fiji, which entered DST at 2:00 a.m. on Sunday, 19th of January, 2014 instead of the previously-scheduled 3:00 a.m.

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

3.93.5. RHEA-2014:0592 — tzdata enhancement update

Updated tzdata packages that add several enhancements are now available for Red Hat Enterprise Linux 4, 5, and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#1099943, BZ#1099944, BZ#1099946, BZ#1102371, BZ#1102372, BZ#1102373

> The Egyptian government decided that Egypt will observe daylight saving time (DST) in 2014, starting on May 15 at 24:00. The DST period will be interrupted during Ramadan. The respective tzdata rules have been updated to reflect this change.
>
> * The zic time zone compiler can now generate correct time zone transitions for minimal time values, and thus generates files with valid time stamps.

All users of tzdata are advised to upgrade to these updated packages, which add these enhancements.

3.93.6. RHEA-2014:0499 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 4, 5, and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#1097154, BZ#1097156, BZ#1097158

> The Egyptian government decided that Egypt will observe daylight saving time (DST) in 2014, starting on May 15 at 24:00. The DST period will be interrupted during Ramadan. The respective tzdata rules have been updated to reflect this change.

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

3.93.7. RHEA-2014:0774 — tzdata enhancement update

Updated tzdata packages that add an enhancement are now available for Red Hat Enterprise Linux 4, 5, 6 and 7.

The tzdata packages contain data files with rules for various time zones.

The following two changes are included in this update: * Based on the official government announcement, Egypt's 2014 Ramadan-based transitions were updated to June 26 and July 31 at 24:00. * Morocco's Ramadan transitions were also updated to June 28 at 03:00 and August 2 at 02:00.

(BZ#1104977, BZ#1104979, BZ#1104982, BZ#1104980)

All users of tzdata are advised to upgrade to these updated packages, which add these enhancements.

3.93.8. RHEA-2014:0338 — tzdata enhancement update

Updated tzdata packages that add one enhancement are now available for Red Hat Enterprise Linux 4, 5, and 6.

The tzdata packages contain data files with rules for various time zones.

Enhancement

BZ#1080526, BZ#1080527, BZ#1080528

Crimea is switching to the Moscow time zone on March 30, 2014 at 2 a.m. local time. The respective tzdata rules have been updated to reflect this change.

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

3.94. udev

3.94.1. RHBA-2014:1239 — 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, providing only the devices present on the system. This dynamic directory runs in user space, dynamically creates and removes devices, and provides consistent naming, as well as a user-space API. The udev packages replace the devfs package and provide better hot plug functionality.

Bug Fixes

BZ#214639

Previously, a default udev rule for the udev utility led to ignoring device mapper devices and prevented access to incomplete snapshot devices. With recent kernels, this rule can now be safely removed, so that device mapper devices now show up correctly in applications detecting udev events, such as gnome-volume-manager.

BZ#405021

Due to the scsi_id utility returning also the port of a Storage Area Network (SAN) in the World Wide Identification (WWID), WWID could not limit its results to only the ID of the intended drive. With this update, the "-x" command-line option yields an additional ID_SERIAL_SHORT key/value pair, the value of which does not include the ports of the SAN.

BZ#481349

Previously, the udev(8) man page contained grammatical mistakes. With this update, the man page is grammatically correct.

BZ#573785

Prior to this update, the udev utility did not report syntax errors in udev rules caused by missing quotation marks. The underlying source code has been fixed, and syntax errors are now logged as intended.

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

3.95. vino

3.95.1. RHSA-2013:1452 — Moderate: vino security update

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

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

Vino is a Virtual Network Computing (VNC) server for GNOME. It allows remote users to connect to a running GNOME session using VNC.

Security Fix

CVE-2013-5745

A denial of service flaw was found in the way Vino handled certain authenticated requests from clients that were in the deferred state. A remote attacker could use this flaw to make the vino-server process enter an infinite loop when processing those incoming requests.

All vino users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue. The GNOME session must be restarted (log out, then log back in) for this update to take effect.

3.96. virt-who

3.96.1. RHBA-2014:1206 — virt-who bug fix and enhancement update

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

The virt-who package provides an agent that collects information about virtual guests present in the system and reports them to the subscription manager.

This update also fixes the following bugs:

Upgrade to an upstream version

The virt-who package has been upgraded to upstream version 0.9, which provides a number of bug fixes and enhancements over the previous version. Notably, the permissions for the configuration file has been changed from world-readable to root-only readable. This change is only for new installations of virt-who; existing installations should be fixed manually by setting the permission of the /etc/sysconfig/virt-who file to 600. (BZ#861552)

This update also fixes the following bugs:

Bug Fixes

BZ#1088756

Prior to this update, the configuration file for virt-who contained incorrect permissions and was world-readable, although this file can contain passwords. As a consequence, any user could read the passwords from the configuration file. To fix this bug, the permissions have been changed to be root-readable only, and non-root users can no longer read passwords from the virt-who configuration file.

BZ#1124732

Previously, the virt-who utility did not report the state of virtual guests to the Subscription Asset Manager (SAM) server. To fix this bug, the info() method from libvirt has been used, and the state of a virtual machine is now reported to the SAM server.

The virt-who package has been upgraded to upstream version 0.9, which provides a number of bug fixes and enhancements over the previous version. Notably, the permissions for the configuration file has been changed from world-readable to root-only readable. This change is only for new installations of virt-who; existing installations should be fixed manually by setting the permission of the /etc/sysconfig/virt-who file to 600. (BZ#861552)

In addition, this update adds the following

Enhancements

BZ#1009401

With this update, support for Red Hat Enterprise Virtualization Manager virtualization back end has been added to virt-who. Now, the user can use virt-who on Red Hat Enterprise Linux 5.11.0 to gather host/guest associations from Red Hat Enterprise Virtualization Manager.

BZ#1078858

Although virt-who worked properly with VMware ESX software, the support for VMware ESXi software was not functional due to differences between ESX and ESXi. With this update, support for ESXi as virtualization back end has been provided for virt-who, which can now use both ESX and ESXi as virtualization back ends.

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

3.97. wireshark

3.97.1. RHSA-2014:0341 — Moderate: wireshark security update

Updated wireshark 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 scores, which give detailed severity ratings, are available for each vulnerability from the CVE links associated with each description below.

Wireshark is a network protocol analyzer. It is used to capture and browse the traffic running on a computer network.

Security Fixes

CVE-2013-3559, CVE-2013-4083, CVE-2014-2281, CVE-2014-2299

> Multiple flaws were found in Wireshark. If Wireshark read a malformed packet off a network or opened a malicious dump file, it could crash or, possibly, execute arbitrary code as the user running Wireshark.

CVE-2012-5595, CVE-2012-5598, CVE-2012-5599, CVE-2012-5600, CVE-2012-6056, CVE-2012-6060, CVE-2012-6061, CVE-2012-6062, CVE-2013-3557, CVE-2013-4081, CVE-2013-4927, CVE-2013-4931, CVE-2013-4932, CVE-2013-4933, CVE-2013-4934, CVE-2013-4935, CVE-2013-5721, CVE-2013-7112

> 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.

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

3.98. xalan-j2

3.98.1. RHSA-2014:0348 — Important: xalan-j2 security update

Updated xalan-j2 packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

Xalan-Java is an XSLT processor for transforming XML documents into HTML, text, or other XML document types.

Security Fix

CVE-2014-0107

> It was found that the secure processing feature of Xalan-Java had insufficient restrictions defined for certain properties and features. A remote attacker able to provide Extensible Stylesheet Language Transformations (XSLT) content to be processed by an application using Xalan-Java could use this flaw to bypass the intended constraints of the secure processing feature. Depending on the components available in the classpath, this could lead to arbitrary remote code execution in the context of the application server running the application that uses Xalan-Java.

All xalan-j2 users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue.

3.99. xorg-x11-server

3.99.1. RHSA-2013:1426 — Important: xorg-x11-server security update

Updated xorg-x11-server packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

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

Security Fix

CVE-2013-4396

> A use-after-free flaw was found in the way the X.Org server handled ImageText requests. A malicious, authorized client could use this flaw to crash the X.Org server or, potentially, execute arbitrary code with root privileges.

Red Hat would like to thank the X.Org security team for reporting this issue. Upstream acknowledges Pedro Ribeiro as the original reporter.

All xorg-x11-server users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue.

3.99.2. RHSA-2013:1868 — Important: xorg-x11-server security update

Updated xorg-x11-server packages that fix one security issue are now available for Red Hat Enterprise Linux 5 and 6.

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

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

Security Fix

CVE-2013-6424

> An integer overflow, which led to a heap-based buffer overflow, was found in the way X.Org server handled trapezoids. A malicious, authorized client could use this flaw to crash the X.Org server or, potentially, execute arbitrary code with root privileges.

All xorg-x11-server users are advised to upgrade to these updated packages, which contain a backported patch to correct this issue.

3.99.3. RHBA-2014:0361 — xorg-x11-server bug fix update

Updated xorg-x11-server packages that fix one bug are now available for Red Hat Enterprise Linux 5.

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

Bug Fix

BZ#1080497

> Due to a logic error in timestamp comparison, resolution changes using the xrandr utility or other RANDR clients failed under various conditions, including long uptime or wall time going backwards. A patch has been implemented to fix this bug. As a result, changing resolution now works correctly when the date is out of synchronization with the original time.

Users of xorg-x11-server are advised to upgrade to these updated packages, which fix this bug.

Revision History

Revision 0.0-0.4	**Mon Sep 15 2014**	**Milan Navrátil**

Release of the Red Hat Enterprise Linux 5.11 Technical Notes.