Record ID: VID10338-0001-ACMR-2013

CCEVS Approved Assurance Continuity Maintenance Report

Product:	Red Hat Enterprise Linux (RHEL) 5.6
EAL:	2 augmented with ALC_FLR.2
Date of Activity:	25 February 2013
References:	Common Criteria Evaluation and Validation Scheme - Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 2.0 , September 8, 2008 Impact Analysis Report for Red Hat Enterprise Linux (RHEL) 5.6, Version 0.3, October 9, 2012
Documentation Updated:	Security Target: Red Hat Enterprise Linux Version 5.6 Security Target for CAPP Compliance on DELL 11th Generation PowerEdge Servers Evaluated Configuration: EAL4 Evaluated Configuration Guide for Red Hat Enterprise Linux on DELL hardware, October 9, 2012; v2.0 Updated initialization package: lspp-eal4-config-dell-0.3-1.noarch.rpm

I. Introduction

On 9 October 2012, Dell submitted an Impact Analysis Report (IAR) for Red Hat Enterprise Linux 5.6 to CCEVS for approval. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme - Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 2.0 , September 8, 2008. In accordance with those requirements, the IAR describes the changes made to the certified TOE, Red Hat Enterprise Linux 5.3, the evidence updated as a result of the changes and the security impact of the changes.

II. Changes to the TOE

For RHEL 5.4:

1. Support for identifying DSCP added.
2. The debug mechanism of Systemtap is added.

For RHEL 5.5:

1. The kernel has been updated to utilize new processor platforms.

2. Device drivers have been added.
3. The GNU Debugger has been updated.
4. Systemtap functionality, a tracing and probing tool, has been updated.

For RHEL 5.6:

1. Some minor convenience features of the installer mechanism have been updated.
2. Paravirtualized drivers have been added.
3. Red Hat added the DNS BIND server.
4. The ext4 file system was added to the TOE.
5. System Security Services Daemon adds functionality similar to single-sign-on (excluded from the evaluated configuration).
6. Trusted Platform Module support was added but is not enabled for the evaluated TOE.

III. Analysis and Testing

For RHEL 5.4:

1. Support for DSCP

   The packet filter support is not covered with SFR-claims, therefore this change is irrelevant for the evaluation

2. Systemtap

   The trace mechanism of Systemtap supports the analysis of the kernel for performance and development problems. This mechanism is disabled by default and not used in the evaluated configuration.

For RHEL 5.5:

1. Kernel update to use new processor platforms

   The kernel has been updated to utilize new processor platforms, including support for Intel's new platforms, code-named Boxboro-EX and Boxboro-MC, AMD's new processor family, code-named Magny-Cours and IBM's Power7 processor.

   The kernel now has the ability to recognize kernel threads that are impossible to wake up. This allows those threads to be handled appropriately and freeing their resources.

2. New device drivers

   New device drivers were added to handle new kinds of hardware:

   - Wireless driver cards

- Drivers for Ethernet cards
- Storage device drivers

These new device drivers do not affect any SFRs

3. GNU Debugger update.

   The GNU Debugger has been updated to a newer version with several feature enhancements, however, the GDB is not considered security-relevant.

4. SystemTap updated

   The trace mechanism of Systemtap supports the analysis of the kernel for performance and development problems. This mechanism is disabled by default and not used in the evaluated configuration.

For RHEL 5.6:

1. Installer mechanism updated

   Some minor convenience features of the installer mechanism have been updated, but they do not affect the installation process nor the TOE itself in any security related way

2. Para-virtualized drivers

   Para-virtualized drivers have been added to the TOE to implement block and network devices. This may affect how the TOE behaves with respect to security, as para-virtualized drivers add a new TSFI to the kernel. Therefore, the TOE is restricted to only using fully virtualized device drivers.

   Other updates regarding virtualization affect the TOE as a VM host and not a as guest. In this case, the evaluated configuration guidance disallows virtualization to be used.

3. DNS BIND server

   Red Hat added the DNS BIND server. This server is not installed in the evaluated configuration.

4. Ext4 file system added

   The ext4 file system was added to the TOE. This does not affect the security functionality of the TOE, but it is in a critical position within the TSF. This was indirectly tested during re-tests.

LVM has been added as a capability, but is not supported in the evaluated configuration.

5. System Security Services Daemon

   The System Security Services Daemon adds functionality similar to single-sign-on, which would add security features to the TOE. Therefore, for this re-certification, the SSD service is not allowed.

   The Samba update does not add any security features to the TOE.

6. Trusted Platform Module support

   The only additional security feature added is support for the Trusted Platform Module, which should not enabled or used in any way by the evaluated configuration.

IV. Conclusion

This maintenance activity covers the assessment of the evaluation impact of the changes applied to Red Hat Enterprise Linux (RHEL) 5.6 evaluated on DELL hardware compared to the baseline of RHEL 5.3 evaluated on DELL hardware.

The listed changes for RHEL 5.4, 5.5 & 5.6 show that small functional updates for SFR-supporting functions are made. No functional update to an SFR-enforcing mechanism is applied. Although these updates included changes to the underlying hardware as well as modification and recompilation of the TOE software (the kernel in particular) is modified and re-compiled, the restrictions on usage and limitations described in the ST reduce the scope of the change to a minor-level impact.

The following additional guidance is provided to emphasize which features should not be used in the evaluated configuration as the result of these changes. See the updated ST and guidance document for further details.

- Full para-virtualization support is NOT supported in the evaluated configuration

- USB keyboards and mice MAY be attached. If a USB keyboard or mouse is used, it MUST be connected before booting the operating system, and NOT added later to a running system. Other hot-pluggable hardware that depends on the dynamic loading of kernel modules MUST NOT be attached. Examples of such unsupported hardware are USB and IEEE1394/FireWire peripherals other than mice and keyboards.

- You MUST ensure that all REQUIRED services listed in the CC guide Section 3.0 are active. You MAY enable or disable services from the OPTIONAL list as suitable for your configuration. All other services MUST be deactivated.

- Device special nodes MUST NOT be added to the system

- CD/DVD devices MUST be accessed using the iso9660 filesystem type. Using an automounter is NOT permitted in the evaluated configuration.

- You MUST NOT use the -p option to useradd(8), specifying a password in that way would bypass the password quality checking mechanism