Red Hat Enterprise Linux 8.6
Common Criteria Guidance

Version 3.4
December 2023

Table of Contents

1 Introduction

This guide provides instructions to configure and operate Red Hat Enterprise Linux (RHEL) 8.6 Extended Update Support (EUS) in the Common Criteria evaluated configuration running on one of the following models:

Vendor	Model	CPU
Dell Inc.	PowerEdge R440	Xeon Silver 42xx
Dell Inc.	PowerEdge R540	Xeon Silver 42xx
Dell Inc.	PowerEdge R640	Xeon Silver 42xx
Dell Inc.	PowerEdge R740	Xeon Silver 42xx
Dell Inc.	PowerEdge R740XD	Xeon Silver 42xx
Dell Inc.	PowerEdge 840	Xeon Silver 42xx
Dell Inc.	PowerEdge 940	Xeon Silver 42xx
Dell Inc.	PowerEdge 940sa	Xeon Silver 42xx
IBM	z15 8561-T01	IBM z15
IBM	z15 8562-T02	IBM z15
IBM	z15 8561-LT1	IBM z15
IBM	z15 8562-LT2	IBM z15

The Target of Evaluation (TOE) consists of the Red Hat Enterprise Linux 8.6 EUS operating system and the applications installed by the kickstart file.

1.1 Getting Started

Ensure the environment is consistent with the following assumptions:

- The RHEL hardware platform is physically protected and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be enough to protect the device and the data it contains.
- The Security Administrator(s) for the device are trusted and act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have enough strength and entropy and to lack malicious intent when administering the device. The device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

- The device firmware and software are updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The administrator's credentials (private key) used to access the device are protected by the platform on which they reside.
- The administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords etc.) when the equipment is discarded or removed from its operational environment.

RHEL also supports secure connectivity with several other IT environment devices as described below:

Component	Required	Usage/Purpose Description for RHEL performance
HW Platform	Yes	x86_64 platform to run RHEL on. The platform must protect RHEL from hardware vulnerabilities, support UEFI Secure Boot, and provide network connectivity.
Workstation with SSH Client	No	This includes any IT Environment Management workstation with an SSH client installed that is used by RHEL users (including administrators) to remotely connect to RHEL through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Audit Server	No	The audit server is used for remote storage of audit records that have been generated by and transmitted from RHEL.
Update Server	Yes	Provides the ability to check for updates to RHEL as well as providing signed updates.

RHEL also has the ability to connect to remote SSHv2 and TLSv1.2 servers, acting as a client for both of these connections.

1.2 Disclaimers

OpenSSL was the only tested cryptographic engine. Other cryptographic engines were not evaluated nor tested, so they should not be used.

The evaluation was limited to verify secure communications using SSH or TLS. Other protocols such as TELNET are not secure and should not be used.

The following security functionality is included in RHEL but was not evaluated:

- SELinux provided access controls

RHEL has two modes of operation:

1. Normal: Once installation has been completed, as described in Section 2 below, RHEL is in a secure mode of operation. The behavior of RHEL can further be configured as specified in Section 3 below.
2. Error: RHEL (with the support of the underlying hardware) verifies the integrity of the bootloader and kernel prior to execution. If a bootloader or kernel integrity error is detected,

RHEL enters an error mode and does not boot. This indicates that an unknown integrity error has occurred. To safely boot RHEL, a specialist must correct the error and determine if any other modifications (accidental or malicious) have been made to RHEL. Additional recover options can be found at: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html-single/performing_a_standard_rhel_installation/index#using-rescue-mode_troubleshooting-after-installation

2 Installation

To install the TOE, you will need to fulfill 4 separate system roles:

1. A personal computer for accessing https://access.redhat.com/ and downloading the installation image.
2. A system running RHEL-8.6 with the Extended Update Support (EUS) subscription, for extracting additional files from the **cc-config** RPM package.
3. The TOE hardware.
4. An HTTP/FTP server for hosting files required for the TOE installation.

Depending on your company infrastructure, roles (1), (2) and (4) may be satisfied by just one or two systems.

2.1 Downloading Required Software

From https://access.redhat.com/, you will need to download:

1. A RHEL installation image (ISO)
2. The cc-config RPM package with additional installation files
3. Additional select RPM packages, updated versions of the ones bundled on the ISO

2.2 The installation Image (ISO)

Use the personal computer to:

1. Log in to https://access.redhat.com/
2. Click on 'Downloads' in the top left corner
3. Click on the 'Red Hat Enterprise Linux' link under Product
    a. For installation on Dell PowerEdge, select 'Red Hat Enterprise Linux for x86_64' as a Product Variant and '8.6' as the version.
    b. For installation on IBM Z LPAR, search for the ‘Red Hat Enterprise Linux for IBM z Systems’ as a Product Variant and ‘8.6’ as the version.
4. Below, under 'Product Software' you should see a section called 'Full installation image' and a line with 'Red Hat Enterprise Linux 8.6 Binary DVD'
5. Click 'Download Now' on the right side of that line

You may further need to follow additional instructions to either burn the DVD to a physical disc, write it to a bootable USB drive or otherwise make it available to the TOE hardware.

See the related RHEL documentation for more:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/performing_a_standard_rhel_8_installation/assembly_creating-a-bootable-installation-medium_installing-rhel

2.3 The cc-config RPM package

The cc-config RPM package is Red Hat's way of shipping additional installation files to customers through trusted channels, requiring a RHEL Extended Update Support (EUS) subscription to access.

To download it, you can use the following:

1. Log in to https://access.redhat.com/
2. Click on 'Downloads' in the top left corner
3. Click on the 'Red Hat Enterprise Linux' link under Product
4. Select 'Red Hat Enterprise Linux for x86_64 - Extended Update Support' as a Product Variant and '8.6' as the version
5. Click on the 'Packages' tab.
6. In the 'Search' field, enter cc-config without a version or release.
7. In the list of filtered results, click on the cc-config item (not 'Download Latest').
8. Select the 8.6 in the 'Version' tab.
9. In the download RPM section at the bottom, click on the 'Download Now' button beside the package name.

After transferring the downloaded file to a RHEL-8.6 system, you can install it:

rpm -ivh cc-config-8.6-*.rpm

Alternatively, instead of downloading it from https://access.redhat.com/, you can install it directly on a RHEL-8.6 system with an EUS subscription:

dnf install cc-config-8.6

In either case, you should find the additional installation files in:

/usr/share/cc-config

One of these files is an Anaconda Kickstart, an automated script for Anaconda, the RHEL installer, a file named **ospp.ks**. This "kickstart" is required for the next steps.

Note that the cc-config RPM package itself is NOT used by or installed on the TOE. It is just to supply the additional installation files. You can omit it from the steps below.

2.4 Additional RPM packages

Open the kickstart **ospp.ks** file in a text editor and find a section called **sanity_check_nvrs** which contains a list of RPM packages described in several columns:

Source RPM	Name	Version	Release	Architectures

To download these, use the personal computer, following the same procedure as for downloading **cc-config** (previous section), using the **Name** for the initial search, and concatenating **Version** and **Release** with a dash (-), selecting it in the Version dropdown on the website.

Alternatively, from the RHEL 8.6 EUS subscribed system, use **dnf download** to download each package individually:

dnf download Name-Version-Release.Architecture.rpm

Note that a package may have **noarch** as an architecture, in which case it is installable on any hardware architecture.

2.5 Preparing the installation files

During the TOE installation, the installer needs some way of reaching the kickstart (**ospp.ks**) and the additional RPM packages downloaded in previous steps. This is what the required HTTP/FTP server is for.

However, before the files are transferred to it, you need to:

1. Create a YUM (DNF) repository with the downloaded RPM packages
2. Modify ospp.ks to tell the installer where this repository will be hosted

2.6 Creating a YUM repository

On the RHEL-8.6 system, put all the downloaded RPM packages in a directory, and run the **createrepo** command on this directory.

```
mkdir   cc-custom
mv  *.rpm   cc-custom/
dnf install createrepo
createrepo cc-custom
```

You can now upload the **cc-custom** directory to the HTTP/FTP server.

2.7 Modifying the kickstart

Open **ospp.ks** in a text editor and search for a line beginning with

#repo --name=cc-custom

uncomment it (remove the leading hash symbol),
and replace **http://server.with.repositories/path/to/custom/repository/** with a valid URL to the **cc-custom** directory uploaded in the previous step.

Additionally, find and uncomment a line beginning with

#cdrom

a few lines above the cc-custom URL.

Further, at the bottom of the **ospp.ks** file, replace

content-url = http://server/path/to/ssg-rhel8-ds.xml

with a full URL to the RHEL8 SCAP datastream, one of the additional files downloaded in the previous steps, and uploaded to the **cc-custom** directory on the HTTP/FTP server. This is required because the OpenSCAP software cannot interact with the YUM/DNF repository directly, and needs its own URL.

Feel free to make further sensible modifications to the kickstart, namely:

- changing the network details (static vs DHCP) and hostname
- changing the root password
- changing the admin user and its password
- changing the bootloader password
- altering disk partition sizes and adding optional extra partitions
- customizing the Pre-login banner

You can now save and upload this modified **ospp.ks** to the HTTP/FTP server. It doesn't need to be located inside the **cc-custom** directory.

2.8 Setting up the TOE hardware

The Dell PowerEdge systems need to be configured to use UEFI boot, with Secure Boot signature checking enabled. This needs to be performed prior to the installation of the operating system.

1. Boot the hardware into a system setup (BIOS) configuration software, using iDRAC Virtual Console or by pressing F2 during early boot.
2. Navigate to System BIOS
3. Under Boot Settings, set Boot Mode to **UEFI**
4. Under System Security, set
    a. Secure Boot to **Enabled**
    b. Secure Boot Policy to **Standard**
    c. Secure Boot Mode to **Deployed**

Then press the Esc key several times and, when asked, save the modified settings and reboot.

2.9 Installing the TOE

Before proceeding, make sure there is no valuable data stored on the TOE hardware. These installation steps **may erase any data on any connected drives** (including possible USB drives, excluding the USB drive containing the ISO image used for installation).

Installing on Dell PowerEdge

Boot the TOE hardware using the RHEL installation image (ISO). Early in this boot process, you should see the Grub2 boot loader, a black-and-white text interface with three lines, the middle line being selected:

Install Red Hat Enterprise Linux 8.6
Test this media & install Red Hat Enterprise Linux 8.6
Troubleshooting -->

Press the ‘e’ key to edit the selected middle entry, navigate the cursor (using arrow keys) to the line beginning with **linuxefi**, and append the following to it:

inst.ks=http://server-hostname/path/to/ospp.ks

where **http://server-hostname/path/to/ospp.ks** is a valid reachable URL of the HTTP/FTP server and the path to **ospp.ks** on that server.

The entire line should then look similar to

linuxefi /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=RHEL-8.6.0-BaseOS-x86_64 rd.live.check quiet inst.ks=http://download.yourcompany.tld/ospp.ks

If your HTTP/FTP server doesn't have a DNS hostname, you can use an IP address instead. If it further runs on a non-standard port, you can specify that too, ie.

inst.ks=http://192.168.1.1:8080/ospp.ks

You might want to add further options to the kernel command line, ie. if your system uses static IP addresses instead of DHCP, add an **ip=** option with the correct arguments, as described by the dracut.cmdline(7) manpage or the RHEL documentation:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/performing_an_advanced_rhel_8_installation/kickstart-and-advanced-boot-options_installing-rhel-as-an-experienced-user#network-boot-options_kickstart-and-advanced-boot-options

After you perform this modification, press **Ctrl-x** to begin the installation.

The installation should now finish automatically.

Installing on IBM Z LPAR

For installations on IBM Z, the standard RHEL documentation applies:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html-single/performing_a_standard_rhel_8_installation/index#booting-the-installation_installing-RHEL

Instead of the images/genericdvd.prm, a customized .prm file with **inst.ks=http://server-hostname/path/to/ospp.ks**
line should be used and referenced from the generic.ins file, where **http://server-hostname/path/to/ospp.ks** is a valid reachable URL of the HTTP/FTP server and the path to ospp.ks on that server.

Installation then gets started using the **Load from Removable Media or Server** task in the Hardware Management Console (HMC).

After installation finishes, Secure Boot should get enabled with the **Enable Secure Boot for Linux** checkbox in the **Load** task screen in the HMC.

2.10 Post-installation steps

If you want the installed system to receive updates from the Extended Update Support channel, you need to register it with Red Hat.

Log in as the 'admin' user, and gain root by issuing 'su -'.
Then execute:

subscription-manager register --auto-attach
subscription-manager release --set=8.6

subscription-manager repos --disable=rhel-8-for-$(uname -m)-baseos-rpms --disable=rhel-8-for-$(uname -m)-appstream-rpms

subscription-manager repos --enable=rhel-8-for-$(uname -m)-baseos-eus-rpms --enable=rhel-8-for-$(uname -m)-appstream-eus-rpms

You will be prompted for login credentials during the **register** step.

The system must be used in FIPS mode. To see if your system is in FIPS mode, run the following:

fips-mode-setup --check

If it is not in FIPS mode, run the following commands to put it in FIPS mode:

update-crypto-policies --set FIPS:OSPP
reboot

After the system comes back up, it will be configured to the OSPP subpolicy of FIPS.

You **must** use the **oscap** tool, from the OpenSCAP project, to verify that the TOE is compliant with the OSPP profile. To do so, follow the steps in the SCAP section to verify and remediate the system if needed.

3 System Configuration

3.1 Firewall

Please see Chapter 7 of the Red Hat Enterprise Linux 8 Securing Networks for instructions for configuring the firewall found here:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/securing_networks/using-and-configuring-firewalld_securing-networks

3.2 Warning Banner

Edit the file /etc/issue to configure the warning banner that will be displayed prior to authentication attempts (local as well as remote SSH). The contents of the file will be displayed to the user.

3.3 SSH

3.3.1 Changing SSH policies

RHEL 8.6 includes a utility, update-crypto-policies, that is used to set the policies for the various cryptographic back-ends such as OpenSSH. The administrator can make any changes to the files located in /etc/crypto-policies/. Both the server and the client application inherit the cipher preferences, the key exchange algorithms as well as the GSSAPI key exchange algorithms. To opt-out from the policy for clients, override the global ssh_config with a user-specific configuration in ~/.ssh/config. To opt-out from the policy for the server, uncomment the line containing **CRYPTO_POLICY=** in /etc/sysconfig/sshd.

The following command is used to apply the new settings.

update-crypto-policies --set FIPS:OSPP
reboot

After the system comes back up, it will be configured to the OSPP subpolicy of FIPS.

3.3.2 Changing the ECDSA Curve

RHEL supports using P-256 and P-384 curves when using an ECDSA hostkey. By default, RHEL generates a P-256 ECDSA hostkey. To change the curve, the administrator runs "**sudo ssh-keygen -t ecdsa -b 256|384 -f /etc/ssh/ssh_host_ecdsa_key**". Do not set a password for this key.

- 256 generates a P-256 key
- 384 generates a P-384 key

Once the key has been generated, restart sshd by running "**sudo systemctl restart sshd.service**".

3.3.3 SSH Public key based authentication

A user can generate an ssh public/private keypair by running "**ssh-keygen -t [rsa|ecdsa] -b [2048|3072|256|384|521]".** 2048 and 3072 are only valid with rsa. 256, 384, and 521 are only valid with ecdsa.

By default, all files created by ssh-keygen are placed in the .ssh directory of their **home directory**. To share the key with a remote system, the user would run:

ssh-copy-id remoteuser@remoteserver

Next , enter the user's password. The public key is shared with the remote server, and the user can log in without a password.

3.3.4 SSH Password based authentication

The administrator can enable or disable SSH password-based authentication to the SSH server by configuring **PasswordAuthentication** in /etc/ssh/sshd_config. "**PasswordAuthentication yes**" enables password-based authentication while "**PasswordAuthentication no**" disables password-based authentication.

When connecting to a remote SSH server, the SSH client supports password-based authentication without configuration. If the remote SSH server supports password-based authentication and other authentication methods (e.g. public key) are not supported or fail, the ssh utility will prompt the user for a password.

3.3.5 Ensure openssh is strongly seeded

RHEL is configured to seed the openssh client and server with 32 bytes. This can be verified by:

- openssh client: verify /etc/profile.d/cc-ssh-strong-rng.sh contains "export SSH_USE_STRONG_RNG=32"
- openssh server: verify /etc/sysconfig/sshd contains "SSH_USE_STRONG_RNG=32"

3.4 Failed Authentication Timeout

The administrator can configure the timeout between failed authentication attempts by editing the /etc/pam.d/system-auth file. Edit the line:

```
auth    required    pam_faildelay.so    delay=<microseconds>
```

3.5 Inactivity Timeout

The administrator can change the local inactivity timeout by changing the idle variable setting in /etc/tmux.conf. The default value is 840 seconds.

The administrator can change the remote (i.e. SSH) inactivity timeout in /etc/ssh/sshd_config by changing the value of **ClientAliveInterval**. This option is specified as "**ClientAliveInterval <time in seconds>**". For example, if the administrator wants to set the timeout to 10 minutes, it would look like "**ClientAliveInterval 600**". A value of "0" disables the remote inactivity timeout. The default value setup by the kickstart is 600.

3.6 NTP

The administrator can configure the name/address of the NTP server(s) by editing /etc/chrony.conf.

Within this file each NTP server is specified on a separate line using the syntax:

"**server <FQDN/IP address> iburst**".

3.7 System Updates

Updates to RHEL are distributed using the RPM format. All updates are signed using a Red Hat controlled RSA 4096 key, so the administrator can be assured of the authenticity of the updates.

The administrator uses the "dnf" program to check for updates and install updates. The command "dnf check-update" is used for checking whether any updates are available. The command "dnf update" is used to install available updates. dnf automatically verifies signatures when checking for and installing updates. dnf does not install an update if the signature check fails.

dnf check-update returns an exit value of:

- 100 if there are packages available for an update and prints a list of the packages to be updated.
- 0 if no packages are available for update.
- 1 if an error occurred (including invalid signatures).

dnf update prints messages indicating which packages were updated and any failures in the update process (including invalid signatures).

3.7.1 Configure Automatic Software Updates

By default, the kickstart script and SCAP content installs RHEL 8.6 with automatic software updates enabled. The system checks for updates daily.

Run the following commands as an administrator to disable automatic software updates:

sudo systemctl disable dnf-automatic.timer
sudo systemctl stop dnf-automatic.timer

To enable automatic software updates, run the following commands as an administrator:

sudo vi /etc/dnf/automatic.conf
a) change upgrade_type to security
b) change apply_updates to yes
sudo systemctl enable --now dnf-automatic.timer

If all you want all updates to be automatically applied, don't do step "a" above. By default, all updates are applied.

3.8 Audit

3.8.1 Configure Audit Storage

The administrator configures the local audit storage by editing /etc/audit/auditd.conf. The amount of local audit storage is determined by a combination of the num_logs and max_log_file settings:

num_logs = <0-999>
: indicates the number of log files to rotate. When set to 0 or 1, a single log file is saved

max_log_file = <number>
: This keyword specifies the maximum file size in megabytes. When this limit is reached, it will trigger a configurable action. The value given must be numeric.

max_log_file_action = <value>
: This parameter tells the system what action to take when the system has detected that the max file size limit has been reached. Valid values are *ignore, syslog, suspend, rotate,* and *keep_logs*. If set to ignore, the audit daemon does nothing. syslog means that it will issue a warning to syslog. suspend will cause the audit daemon to stop writing records to the disk. The daemon will still be alive. The rotate option will cause the audit daemon to rotate the logs. It should be noted that logs with higher numbers are older than logs with lower numbers. This is the same convention used by the logrotate utility. The keep_logs option is similar to rotate except it does not use the num_logs setting. This prevents audit logs from being overwritten.

The amount of local storage used for audit logs is num_logs multiplied by max_log_file unless keep_logs is specified. All free space on the partition storing logs may be used when keep_logs is specified.

3.8.2 Configure Audit Rules

The auditctl command allows you to control the basic functionality of the Audit system and to define rules that decide which Audit events are logged. Persistent audit rules are kept in files at /etc/audit/rules.d/.

Note: All commands which interact with the Audit service and the Audit log files require root privileges. Ensure you execute these commands as the root user. Additionally, CAP_AUDIT_CONTROL is required to configure the audit services and CAP_AUDIT_WRITE is required to log user originating messages.

The TOE is preconfigured by the SCAP content to enable all auditing suggested by the OSPP Configuration Annex except *successful file access*. This is because this is normal system behavior rather than an exception to the access policy. And more importantly, it will fill up the logs making it harder to find policy violations. If you really need to enable auditing successful file access, as the root user do the following:

cp /usr/share/audit/sample-rules/30-ospp-v42-3-access-success.rules /etc/audit/rules.d/
restorecon /etc/audit/rules.d/*
service auditd restart

Please see Section 10.6 of the Red Hat Enterprise Linux 8 Security Hardening for additional details.

3.9 Software Restriction Policies (fapolicyd)

Fapolicyd is a daemon that determines whether or not access to files or execution of programs is allowed based on the software's reputation and sha256 hash. By default, all applications that are packaged by rpm are automatically trusted.

To enable fapolicyd integrity checks using SHA-256 hashes open the /etc/fapolicyd/fapolicyd.conf file in a text editor of your choice, for example:

sudo vi /etc/fapolicyd/fapolicyd.conf

Change the value of the integrity option from **none** to **sha256**, save the file, and exit the editor:

integrity = sha256

Restart the fapolicyd service:

sudo systemctl restart fapolicyd

Please see Section 14.5 of the Red Hat Enterprise Linux 8 Security Hardening for additional details.

The rules that ship with the daemon are set up to only audit denied access requests. It is possible to audit successful access by changing any rule in /etc/fapolicyd/fapolicyd.rules from **deny_audit** to **allow_audit**. Restarting the daemon makes the rule take effect. It is not configured to audit successful access by default because it will result in a large quantity of audit events making it hard to find policy violations.

3.10 Extra Kernel Security Command line parameters

The RHEL 8 TOE is configured with extra kernel security command line parameters for system boot. These are in effort to mitigate certain vulnerabilities in the kernel. These are not required by OSPP nor evaluated. The extra command line parameters are:

slub_debug=P - this option enables slub/slab allocator free poisoning. This is in effort to prevent use after free vulnerabilities from being successful.

page_poison=1 - this option enables buddy allocator free poisoning. This is in effort to prevent use after free vulnerabilities from being successful.

vsyscall=none - this removes vsyscall to avoid it being a fixed-position ROP target. Normally this is needed for compatibility with RHEL6 and earlier software. If you know that you will not need that compatibility, it's recommended to add this.

To add these option to the boot prompt, as root run the following command:

grubby --update-kernel=ALL --args="vsyscall=none page_poison=1 slub_debug=P"

To remove these options, as root run the following command:

grubby --update-kernel=ALL --remove-args="vsyscall=none page_poison=1 slub_debug=P"

This will rebuild the boot menu for UEFI systems.

4 Administration

4.1 User/Administrator Accounts

4.1.1 Creating User Accounts

The administrator can create user accounts using the "**useradd <username>**" command. The user account will be locked and password-less.

Once a user account has been created, the administrator can make this account an administrator by adding it to the wheel group by running "**usermod -aG wheel <username>**".

The most basic tasks to manage user accounts and groups, and the appropriate command-line tools, include:

- Displaying user and group IDs:

  id

- Creating a new user account:

  useradd [options] ***user_name***

- Assigning a new password to a user account belonging to *username*:

  passwd ***user_name***

- Adding a user to a group:

  usermod -a -G ***group_name user_name***

Once an account is created and added to the wheel group, it can be used to administer RHEL from the local console or through a remote SSH connection.

4.1.2 Configure Password Policy

The password policy is enforced by the pam_pwquality PAM module. See the pwquality.conf(5) man page for details. The default policy that is set up by the kickstart guarantees a minimum length of 12 characters.

4.1.3 Change Passwords

A user can change their password using the "passwd" command. The user will be prompted to enter their current password as well as their new password.

4.2 SCAP

SCAP (Secure Content Automation Protocol) is a distinguishing feature of RHEL security. It is a standard created by NIST to allow content migration between certified security vendors to check or remediate the security posture of their system.

4.2.1 Viewing the OSPP configuration profile

The RHEL installation as previously described includes a package named scap-security-guide. In it, there is a datastream file for RHEL 8, ssg-rhel8-ds.xml. Within it is the OSPP profile which contains the evaluated configuration. A document that describes the evaluated configuration can be viewed by running the following command:

```
oscap xccdf generate guide --profile ospp /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml \
--output checklist.html
```

The checklist for the evaluated configuration is a full lockdown that not only meets the requirements for OSPP, but exceeds them.

4.2.2 Checking the system configuration

The details of the evaluated configuration can be viewed with any web browser after generating the checklist. An administrator can verify the configuration of the system at any time.

The following command will show the profile name (ospp) in the file:

```
oscap info /usr/share/xml/scap/ssg/content/ssg-rhel8-xccdf.xml
```

To verify the status of the profile being applied to the system, an administrator must use:

```
oscap xccdf eval --profile ospp /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

This verification can also generate a HTML report via the **--report** option:

```
oscap xccdf eval --profile ospp --report report.html \
        /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

4.2.3 System Remediation

If the system is found to be out of the evaluated configuration, it may be put back into configuration by performing an online remediation. Online remediation means that it remediates the system at the time of scanning. To restore the system to the evaluated configuration, run the following command as root:

```
oscap xccdf eval --remediate --profile ospp --results scan-xccdf-results.xml \
 /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

The results of the command are stored into the scan results XML file. The output consists of two sections. The first section is a TestResult element in an XCCDF file which contains the results of the scan prior to the remediation. The second section contains f*ixed* and *error* results. The *fixed* result indicates that the scan passed after the remediation. The *error* result indicates that even after applying the remediation, the evaluation still does not pass.

4.2.4 Tailoring the OSPP profile

Sometimes you need to customize SCAP content to match local policy and needs. For example, suppose you need to enable user namespaces for container applications. First edit the ospp sysctl file /etc/sysctl.d/70-cc-security.conf. Enable user namespace by changing the value of user.max_user_namespaces from 0 to any positive number such as 25. Save the file. Because of this

change, the SCAP content will now complain about user namespaces being enabled. To stop this complaint, you would tailor the SCAP content to allow it. The way that you would do this is to use a RHEL workstation with scap-workbench installed. Ensure that the SCAP content matching the OSPP evaluated configuration is also installed on the workstation. Follow these steps to create a tailoring file:

1) Open scap-workbench.
2) Select RHEL 8 content, click on "**Load Content**."
3) Select "**Protection Profile for General Purpose Operating System**".
4) Click on the "**Customize**" button to create a new copy. Use the default name - click "**OK**."
5) In the search box, type "**user_namespaces**". Click the "**Search**" button.
6) If the search was successful, it will highlight the associated SCAP rule. In this case it is checked. Click on the **checkmark** to deselect this rule. Click "**OK**".
7) To save this change, click on the "**File**" menu item and then select "**Save Customization Only**".
8) In the dialog box give it the name "tailoring-file.xml" and click on "**Save**". This saves just the changes and not a whole profile.
9) The tailoring file can now be copied to a server in the OSPP configuration and used as follows (adjusting for the actual path to the tailoring file):

```
oscap xccdf eval --tailoring-file tailoring-file.xml  \
        --profile ospp /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

You can find more information about tailoring here:
https://www.open-scap.org/resources/documentation/customizing-scap-security-guide-for-your-use-case/

4.2.5 Changing to a new profile

One of the advantages of using SCAP for system configuration is that it makes it easy to move in and out of the evaluated configuration. If one day you were asked to reconfigure the system to meet the DISA STIG, then you would list the available profiles as mentioned here and then choose the STIG ID.

To see if your system conforms to the STIG, run the following command as root:

```
oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_stig \
/usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

To then switch to the STID, you would remediate as mentioned in a previous section

```
oscap xccdf eval --remediate --profile xccdf_org.ssgproject.content_profile_stig \        --
results scan-xccdf-results.xml  /usr/share/xml/scap/ssg/content/ssg-rhel8-ds.xml
```

4.2.6 More information

More information can be found here: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/pdf/system_design_guide/Red_Hat_Enterprise_Linux-8-System_Design_Guide-en-US.pdf

4.3 SWID Tag

RHEL 8 ships with a Software Identification (SWID) tag to enable ISO/IEC 19770-2:2015 based software identification. This helps with software inventory management and application of rules based on the platform's identity. It is loosely associated with SCAP and has been adopted by NIST. The tag's location is /usr/lib/swidtag/redhat.com/com.redhat.RHEL-8-<architecture>.swidtag with the symlink /etc/swid/swidtags.d/redhat.com pointing to the directory containing original file.

There will be two tags in the directory. The first is a primary tag that has no version. This tag has all of the mandatory fields populated describing the product. There will be another tag that has a version in its name, in this case 8.6. The second tag is a supplemental which identifies which version of RHEL 8 is installed. Together they describe the product and release.

4.4 TLS Usage

RHEL provides a TLS client for secure communication with remote systems. The TLS client is invoked using:

openssl s_client -connect [host]:[port] -x509_strict -verify_return_error -CAfile [ca certificate] \ -crl_check_all -tls1_2 [-verify_hostname [hostname]|-verify_ip [IP address]] -rand /dev/random

The options are described as follows:

-connect [host]:[port]
: specifies the FQDN or IP address and port of the remote system.

-x509_strict
: checks that all certificates, including issuing CAs, are compliant to x509 standards.

-verify_return_error
: terminates the connection if an error is found.

-CAfile [ca certificate]
: points to the Root CA used to validate the presented server certificate.

-crl_check_all
: checks revocation on the entire chain of certificates

-tls1_2
: force to use TLSv1.2 only.

-verify_hostname [hostname]
: Configures the hostname that the TOE will convert into a DNS-ID and CN reference identifier. The left-most component in the presented certificate may be a wildcard (i.e. "*").

-verify_ip [IP address]
: Configures the IP address that the TOE will convert into an IP address SAN reference identifier.

OpenSSL supports the following ciphersuites when configured with the ospp crypto policy:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

RHEL also presents the following curves in the Supported Groups Extension without any configuration:

- secp256r1
- secp384r1
- secp521r1

4.4.1 RFC6125 Identifier

RHEL 8 verifies that the presented identifier matches the reference identifier according to RFC 6125 as follows. The TOE establishes the reference identifier by parsing the DNS Name or IP address for the configured TLS server. The reference identifier is matched against the SAN, if present. If the SAN is not present, the referenced identifier is matched against the CN for DNS. For IP addresses, the TOE matches the identifier against the SAN only. The TOE supports wildcards in the DNS name of the server certificate. The TOE does not support URI reference identifiers, SRV reference identifiers, or certificate pinning.

4.5 Storage of Sensitive Data

RHEL follows standard conventions for storing sensitive data. Applications must store their sensitive data in the /etc directory with restrictive access permissions. Access to sensitive data should be restricted to root and/or the application storing the sensitive data. Sensitive data consists of keys and passwords.

RHEL also provides the ability to encrypt/decrypt sensitive files using OpenSSL. The command to use is the following:

**openssl enc [-d] -aes-128-cbc|-aes-256-cbc -in <file> -out <file> **
-pass file:<file_with_password> -pbkdf2

The -d option is used for decryption instead of encryption.

4.6 Secure Erase

The TOE has a utility, shred, that can assist in the secure erasure of files and partitions within the limitations expressed in the next section. The utility by default writes 3 patterns to files or disk devices to make retrieval of data more difficult. To securely erase an external drive with default options, as root, use the following (adjusting for the actual drive):

shred /dev/sde1

See the man page for additional information.

4.7 Non-volatile drives and keys

All instances of keys in non-volatile storage might not be deleted if the physical drive has replaced a sector containing a key with a spare sector. To minimize this risk, the physical drive should be end-of-life before a significant amount of damage to the drive's health can occur.

5 Using the System Safely

This section has additional guidance to help workaround potential issues that are residual in the TOE.

5.1 Video Frame Buffer Access

The administrator should not add the "video" group to user accounts to mitigate CVE-2021-33655.

5.2 Tar program usage

Only untar files that you trust to avoid triggering CVE-2022-48303.

5.3 Slip kernel module

The TOE does not have the kernel-modules-extra rpm installed. If it has to be installed, the slip kernel module must be blacklisted. The slip kernel module provides support for the Serial Line Internet Protocol. It has largely been replaced by the PPP protocol for serial communication. To ensure that you are protected against CVE-2022-41858 if the kernel-modules-extra rpm has to be installed, create a file as follows

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install slip /bin/false

blacklist slip

Save and exit. This will prevent the module from loading.

5.4 Quick Fair Queueing (QFQ) scheduler kernel module

The TOE does not have the kernel-modules-extra rpm installed. If it has to be installed, the QFQ kernel module must be blacklisted. The QFQ kernel module provides support for the Quick Fair Queuing network packet scheduler algorithm. To ensure that you are protected against CVE-2023-31436 and CVE-2023-3611 if the kernel-modules-extra rpm has to be installed, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install sch_qfq /bin/false

blacklist sch_qfq

Save and exit. This will prevent the module from loading.

5.5 Car Area Network (CAN) kernel module

The CAN kernel module provides support for the Car Area Network protocol. To ensure that you are protected against CVE-2023-2166, create a file as follows

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install can /bin/false

blacklist can

Save and exit. This will prevent the module from loading.

5.6 TIPC kernel module

The TIPC kernel module provides support for the Transparent Inter Process Communication network protocol which is designed for intra-cluster communication. To ensure that you are protected against CVE-2023-1382, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install tipc /bin/false

blacklist tipc

Save and exit. This will prevent the module from loading.

5.7 ISCSI_TCP kernel module

The ISCSI_TCP kernel module provides support for the iSCSI protocol to transport SCSI requests and responses over a TCP/IP network. To ensure that you are protected against CVE-2023-2162, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install iscsi_tcp /bin/false

blacklist iscsi_tcp

Save and exit. This will prevent the module from loading.

5.8 Asus HID kernel module

On the Dell system only, the asus-hid kernel module provides support for an Asus Keyboard. The TOE does not come with one but a malicious device could be plugged in the USB connector. To ensure that you are protected against CVE-2023-1079, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install hid-asus /bin/false

blacklist hid-asus

Save and exit. This will prevent the module from loading.

5.9 Intel's iSMT SMBus kernel module

To ensure that you are protected against CVE-2022-2873, create a file as follows

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install i2c-ismt /bin/false

blacklist i2c-ismt

Save and exit. This will prevent the module from loading.

5.10 IEEE 802.15.4 kernel module

To ensure that you are protected against CVE-2021-3659, create a file as follows

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install mac802154 /bin/false

blacklist mac802154

Save and exit. This will prevent the module from loading.

5.11 SDMC DM1105 kernel module

To ensure that you are protected against CVE-2023-35824, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install dm1105 /bin/false

blacklist dm1105

Save and exit. This will prevent the module from loading.

5.12 Ricoh R5C592 kernel module

To ensure that you are protected against CVE-2023-3141, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install r592 /bin/false

blacklist r592

Save and exit. This will prevent the module from loading.

5.13 GFS2 kernel module

To ensure that you are protected against CVE-2023-3212, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install gfs2 /bin/false

blacklist gfs2

Save and exit. This will prevent the module from loading.

5.14 Integrated Sensor Hub (ISH) kernel module

To ensure that you are protected against CVE-2023-3358, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install intel-ishtp /bin/false

blacklist intel-ishtp

Save and exit. This will prevent the module from loading.

5.15 Sun RPC kernel module

To ensure that you are protected against CVE-2022-28893, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install sunrpc /bin/false

blacklist sunrpc

Save and exit. This will prevent the module from loading.

5.16 Universal 32bit comparisons w/ hashing (U32) kernel module

To ensure that you are protected against CVE-2022-29581, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install cls_u32 /bin/false

blacklist cls_u32

Save and exit. This will prevent the module from loading.

5.17 Netfilter NFQUEUE kernel module

To ensure that you are protected against CVE-2022-36946, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install nfnetlink_queue /bin/false

blacklist nfnetlink_queue

Save and exit. This will prevent the module from loading.

5.18 CIFS kernel module

To ensure that you are protected against CVE-2023-1195 and CVE-2023-1192, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install cifs /bin/false

blacklist cifs

Save and exit. This will prevent the module from loading.

5.19 FBCON kernel module

To ensure that you are protected against CVE-2023-3161 and CVE-2023-38409, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install fbcon /bin/false

blacklist fbcon

Save and exit. This will prevent the module from loading.

5.20 NVME kernel module

To ensure that you are protected against CVE-2023-5178, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install nvme_tcp /bin/false

blacklist nvme_tcp

Save and exit. This will prevent the module from loading.

5.21 SCH HFSC kernel module

To ensure that you are protected against CVE-2023-4623, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install sch_hfsc /bin/false

blacklist sch_hfsc

Save and exit. This will prevent the module from loading.

5.22 Disable Transparent Huge Pages

To ensure that you are protected against CVE-2023-4732, disable the Transparent Huge Pages by running the following command:

grub2-editenv - list | grep kernelopts

kernelopts=root=/dev/mapper/rhel-root ro resume=/dev/mapper/rhel-swap rd.lvm.lv [rd.lvm.lv]=rhel/root rd.lvm.lv [rd.lvm.lv]=rhel/swap

grub2-editenv - set "kernelopts=root=/dev/mapper/rhel-root ro resume=/dev/mapper/rhel-swap rd.lvm.lv [rd.lvm.lv]=rhel/root rd.lvm.lv [rd.lvm.lv]=rhel/swap transparent_hugepage=never"

For further information please see https://access.redhat.com/solutions/3799821

5.23 smsusb kernel module

To ensure that you are protected against CVE-2023-4132, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install smsusb /bin/false

blacklist smsusb

Save and exit. This will prevent the module from loading.

5.24 cls_rsvp kernel module

To ensure that you are protected against CVE-2023-42755, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install cls_rsvp /bin/false

blacklist cls_rsvp

Save and exit. This will prevent the module from loading.

5.25 nftables kernel module

To ensure that you are protected against CVE-2023-4569, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install nftables /bin/false

blacklist nftables

Save and exit. This will prevent the module from loading.

5.26 tun kernel module

To ensure that you are protected against CVE-2023-3812, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install tun /bin/false

blacklist tun

Save and exit. This will prevent the module from loading.

5.27 tap kernel module

To ensure that you are protected against CVE-2023-3812, create a file as follows:

vi /etc/modprobe.d/cve-workarounds.conf

add the following text:

install tap /bin/false

blacklist tap

Save and exit. This will prevent the module from loading.

6 Application Developers

Application developers can use the included `gcc` compiler and linker to create applications that run on RHEL. When invoking `gcc`, developers should follow best practices for secure development:

Include the following compiler flags to enable stack smashing protections:

-fstack-protector-strong --param=ssp-buffer-size=4

Include the following compiler and linker flags to enable more ASLR:

-fpie -Wl,-pie

6.1 Developer Security Workarounds

6.1.1 CVE-2019-17543

Application developers using LZ4 compression should use the LZ4 library APIs according to the documentation to avoid triggering CVE-2019-17543.

6.1.2 CVE-2023-2513

The vulnerability can be exploited by a regular user, but the filesystem should be mounted with debug_want_extra_isize=128 and the user must have write access to the filesystem. It's also important to emphasize that debug_want_extra_isize is a debug mount option and should never be used in production.

6.1.3 OpenSSL

OpenSSL has 3 vulnerabilities, CVE-2023-0464, CVE-2023-0465, and CVE-2023-0466, that should be worked around if your application uses TLS certificate policies (look for the function X509_VERIFY_PARAM_add0_policy). It should be noted that certificate policy checking is disabled by default and rarely used. If your application uses certificate policies, you will need to switch to using X509_VERIFY_PARAM_set1_policies() or explicitly enable the policy check by calling X509_VERIFY_PARAM_set_flags() with the X509_V_FLAG_POLICY_CHECK flag argument. All three vulnerabilities are fixed by using this function.

6.1.4 CVE-2022-43552

Do not tunnel SMB or Telnet to an HTTP proxy server. Or do not use the - -proxy option to curl to avoid triggering CVE-2022-43552.

6.1.5 CVE-2023-28772

Avoid using the debug tool tracefs to avoid triggering CVE-2023-28772.. Mounting tracefs requires administrator privileges and admins are expected to be well behaved.

6.2 Additional Security Compile Flags

The vulnerability can be exploited by a regular user, but the filesystem should be mounted with debug_want_extra_isize=128 and the user must have write access to the filesystem. It's also important to emphasize that debug_want_extra_isize is a debug mount option and should never be used in production.

-Werror=format-security

-Wp,-D_FORTIFY_SOURCE=2

-fstack-clash-protection

-fcf-protection

See the gcc man page for more details.

If you build your software using rpmbuild and open source tooling, you can install the redhat-rpm-config package and these additional hardening flags will be automatically applied.

6.3 Use of /dev/random and /dev/urandom

Application developers **must** use the getrandom system call to gather entropy or key material required for applications. The use of /dev/random and /dev/urandom were not evaluated and are not guaranteed to be sufficiently seeded before reading. The system **must** be operated in the **fips mode** as directed in the SCAP content. Any draw from getrandom that requires entropy **must** use the GRND_RANDOM flag to getrandom.

7 Enabling the use of containers

Linux containers are technologies that allow packaging and isolating applications with all of the files necessary to run. This makes it easy to move the contained application between environments (dev, test, production, etc.) while retaining full functionality. Containers are also an important part of IT security. By building security into the container pipeline and defending your infrastructure, you can make sure your containers are reliable, scalable, and trusted.

7.1 Enabling user namespace

The user namespace in the TOE is configured by the installation scripts to be turned off. This is in effort to reduce the attack surface. However, if you know that you want to run container workloads, then you will need to re-enable user namespaces. To do this, edit the file /etc/sysctl.d/70-cc-security.conf. Find the line with user.max_user_namespaces. Change the value on the right hand side of the equal sign to some positive number for how many of them you think you'll need. For example, you could set it to 100. Save the file and run:

sysctl --system

Alternatively, you can tailor the SCAP profile that you are using and remediate the system with SCAP. This is probably a better way so that you do not have future findings when scanning.

7.2 More information

More information about containers and how to manage them can be found here:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html-single/building_running_and_managing_containers/index

8 Audit Event Reference

All the audits are found in /var/log/audit/audit.log. The ausearch utility is intended to be the way to see the events. The Audit event format is as follows:

node=ospp type=<type> msg=audit(<timestamp>: <serial_number>): pid=<pid> uid=<uid> auid=<auid> ses=<session> <message> <source> res=<res>

<type>
SERVICE_STAR, SERVICE_STOP, USER_AUTH, SYSCALL, USER_START, USER_CMD, ADD_GROUP, PROCTITLE, CWD, SOFTWARE_UPDATE, SYSTEM_BOOT, SYSTEM_SHUTDOWN, PATH, CWD, or EXECVE

<timestamp>
Epoch time (seconds since January 1, 1970 12:00:00 AM) to the millisecond

<serial_number>
unique numerical event identifier appended to the timestamp. Repeats across multiple records that are related to the same event

<uid>
user ID of the process at the time the audit event was generated

<auid>
user ID of the user authenticated by the system (regardless if the user has changed his real and / or effective user ID afterwards)

<pid>
Process ID of the subject that caused the event

<session>
session ID – used to disambiguating actions when a single user has multiple active sessions

<message>
Information about the intended operation

<source>
hostname=<host>, addr=<IP_address>, and/or terminal=<terminal> – identifies how the subject is connected to RHEL

<res>
success or failure – indicates whether the action succeeded or failed

RHEL generates audit logs for the following events (note: some information has been edited, such as IP addresses and DNS names):

- Start-up of the audit function
  node=ospp type=SERVICE_START msg=audit(1575382890.662:89388): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=auditd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'

- Shut-down of the audit function
  node=ospp type=SERVICE_STOP msg=audit(1575382790.412:89043): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=auditd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'

- Software Restriction Policies
  node=localhost.localdomain type=PROCTITLE msg=audit(08/05/2020 05:57:33.980:354084) : proctitle=-bash
  node=localhost.localdomain type=PATH msg=audit(08/05/2020 05:57:33.980:354084) : item=0 name=./hex-val.sh inode=160 dev=fd:07 mode=file,750 ouid=admin ogid=admin rdev=00:00 obj=unconfined_u:object_r:user_home_t:s0 nametype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
  node=localhost.localdomain type=CWD msg=audit(08/05/2020 05:57:33.980:354084) : cwd=/home/admin
  node=localhost.localdomain type=SYSCALL msg=audit(08/05/2020 05:57:33.980:354084) : arch=x86_64 syscall=openat success=no exit=EPERM(Operation not permitted) a0=0xffffff9c

a1=0x5625fd081300 a2=O_RDONLY a3=0x0 items=1 ppid=53526 pid=53583 auid=admin uid=admin gid=admin euid=admin suid=admin fsuid=admin egid=admin sgid=admin fsgid=admin tty=pts8 ses=126 comm=bash exe=/usr/bin/bash subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=unsuccessful-access node=localhost.localdomain type=FANOTIFY msg=audit(08/05/2020 05:57:33.980:354084) : resp=deny

- Authentication Events
  node=ospp type=USER_AUTH msg=audit(02/17/2020 07:13:09.773:5805) : pid=42586 uid=root auid=unset ses=unset subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=success acct=admin exe=/usr/sbin/sshd hostname=? addr=? terminal=ssh res=success'

  node=ospp type=USER_AUTH msg=audit(02/17/2020 07:16:36.927:6494) : pid=42655 uid=root auid=unset ses=unset subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=? acct=admin exe=/usr/sbin/sshd hostname=? addr=? terminal=ssh res=failed'

- Use of privileged/special rights
  node=ospp type=SYSCALL msg=audit(1573571951.064:66845): arch=c000003e syscall=2 success=yes exit=3 a0=7f85317c74e4 a1=80000 a2=1 a3=7f85319cd4f8 items=1 ppid=25815 pid=25890 auid=1000 uid=1000 gid=1000 euid=0 suid=0 fsuid=0 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=348 comm="sudo" exe="/usr/bin/sudo" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="successful-access"

- Role escalation events
  node=ospp type=USER_START msg=audit(02/21/2020 08:27:59.746:2208) : pid=16861 uid=root auid=admin ses=195 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_keyinit,pam_limits,pam_systemd,pam_unix acct=root exe=/usr/bin/sudo hostname=? addr=? terminal=/dev/pts/1 res=success'

  node=ospp type=USER_CMD msg=audit(02/17/2020 07:32:48.902:9813) : pid=42912 uid=tester auid=tester ses=582 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd=/home/tester cmd=vi /etc/rsyslog.conf terminal=pts/1 res=failed'

- File and object events (Successful and unsuccessful attempts to create, access, delete, modify file, modify permissions)
  node=ospp type=SYSCALL msg=audit(1573571943.611:66844): arch=c000003e syscall=2 success=no exit=-13 a0=7ffcae0b175f a1=0 a2=0 a3=7ffcae0afb60 items=1 ppid=25815 pid=25889 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=348 comm="tail" exe="/usr/bin/tail"

- User and Group management events (Successful and unsuccessful add, delete, modify, disable, enable, and credential change)

node=ospp type=ADD_GROUP msg=audit(1575391931.170:89985): pid=49353 uid=0 auid=1000 ses=884 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=add-group acct="user " exe="/usr/sbin/useradd" hostname=ospp addr=? terminal=pts/0 res=success'4050

- Audit and log data access events (Success/Failure)
  Success:
  node=ospp type=PROCTITLE msg=audit(01/21/2020 07:48:10.775:1235) : proctitle=ls --color=auto -al /var/log/
  node=ospp type=PATH msg=audit(01/21/2020 07:48:10.775:1235) : item=0 name=/var/log/audit inode=64 dev=fd:03 mode=dir,700 ouid=root ogid=root rdev=00:00 obj=system_u:object_r:auditd_log_t:s0 objtype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
  node=ospp type=CWD msg=audit(01/21/2020 07:48:10.775:1235) : cwd=/root
  node=ospp type=SYSCALL msg=audit(01/21/2020 07:48:10.775:1235) : arch=x86_64 syscall=lgetxattr success=yes exit=34 a0=0x7ffc989bbca0 a1=0x7f94d0e52eaa a2=0x1107480 a3=0xff items=1 ppid=10022 pid=10062 auid=admin uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=1 comm=ls exe=/usr/bin/ls subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=access-audit-trail

  Failure:
  node=ospp type=PROCTITLE msg=audit(01/21/2020 07:48:10.775:1237) : proctitle=ls --color=auto -al /var/log/
  node=ospp type=PATH msg=audit(01/21/2020 07:48:10.775:1237) : item=0 name=/var/log/audit inode=64 dev=fd:03 mode=dir,700 ouid=root ogid=root rdev=00:00 obj=system_u:object_r:auditd_log_t:s0 objtype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
  node=ospp type=CWD msg=audit(01/21/2020 07:48:10.775:1237) : cwd=/root
  node=ospp type=SYSCALL msg=audit(01/21/2020 07:48:10.775:1237) : arch=x86_64 syscall=getxattr success=no exit=ENODATA(No data available) a0=0x7ffc989bbca0 a1=0x7f94d0a2ddb0 a2=0x0 a3=0x0 items=1 ppid=10022 pid=10062 auid=admin uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=1 comm=ls exe=/usr/bin/ls subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=access-audit-trail

- Cryptographic verification of software (Success/Failure)
  Success:
  node=ospp type=SOFTWARE_UPDATE msg=audit(12/18/2019 07:50:26.337:61554) : pid=25065 uid=root auid=admin ses=347 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='sw=dnf-cron-3.4.3-161.el7.noarch sw_type=rpm key_enforce=0 gpg_res=1 root_dir=/ comm=dnf exe=/usr/bin/python2.7 hostname=ospp addr=? terminal=pts/0 res=success'

  Failure:

node=ospp type=SOFTWARE_UPDATE msg=audit(08/27/2019 11:21:51.198:3625) : pid=19723 uid=root auid=admin ses=254 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='sw=kernel-3.10.0-1062.el7.x86_64 sw_type=rpm key_enforce=0 gpg_res=1 root_dir=/ comm=dnf exe=/usr/bin/python2.7 hostname=ospp addr=? terminal=pts/0 res=failed'

- System reboot, restart, and shutdown events (Success/Failure)
  Success:
  type=SYSTEM_BOOT msg=audit(09/20/2016 01:10:32.392:7) : pid=657 uid=root auid=unset ses=unset subj=system_u:system_r:init_t:s0 msg=' comm=systemd-update-utmp exe=/usr/lib/systemd/systemd-update-utmp hostname=? addr=? terminal=? res=success'

  Failure: N/A

  System Shutdown:
  node=ospp type=SYSTEM_SHUTDOWN msg=audit(04/23/2020 05:15:54.157:379) : pid=9432 uid=root auid=unset ses=unset subj=system_u:system_r:init_t:s0 msg=' comm=systemd-update-utmp exe=/usr/lib/systemd/systemd-update-utmp hostname=? addr=? terminal=? res=success'

- Kernel module loading and unloading events (Success/Failure)
  Success:
  Jul 30 18:16:19 hostname dracut[22908]: *** Including module: drm *
  Failure:
  Jul 30 18:16:18 hostname dracut[22908]: dracut module 'nfs' will not be installed, because command 'mount.nfs4' could not be found!

- Administrator or root-level access events (Success/Failure)

  Success:
  time->Fri Oct 11 10:29:29 2019
  node=ospp type=USER_START msg=audit(1570804169.135:2217): pid=11088 uid=0 auid=1000 ses=93 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'

  Failure:
  node=ospp type=PATH msg=audit(02/17/2020 07:32:15.005:9264) : item=0 name=/bin/passwd inode=805792770 dev=fd:00 mode=file,suid,755 ouid=root ogid=root rdev=00:00 obj=system_u:object_r:passwd_exec_t:s0 objtype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
  node=ospp type=CWD msg=audit(02/17/2020 07:32:15.005:9264) : cwd=/root
  node=ospp type=EXECVE msg=audit(02/17/2020 07:32:15.005:9264) : argc=2 a0=passwd a1=tester

node=ospp type=SYSCALL msg=audit(02/17/2020 07:32:15.005:9264) : arch=x86_64 syscall=execve success=yes exit=0 a0=0x17099d0 a1=0x17098b0 a2=0x17007a0 a3=0x7ffcbd833ce0 items=2 ppid=42728 pid=42883 auid=admin uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=579 comm=passwd exe=/usr/bin/passwd subj=unconfined_u:unconfined_r:passwd_t:s0-s0:c0.c1023 key=special-config-changes

9 References

- Red Hat Enterprise Linux 8.6 Security Target, v3.0
- Kickstart file, v0.6.2
- Red Hat Enterprise Linux 8 Security Hardening, Updated 2021-01-14