Red Hat Enterprise Linux 8

Managing and monitoring security updates

A guide to managing and monitoring security updates in Red Hat Enterprise Linux 8

Last Updated: 2020-07-03

Red Hat Enterprise Linux 8 Managing and monitoring security updates

A guide to managing and monitoring security updates in Red Hat Enterprise Linux 8

Legal Notice

Abstract

This document describes how to learn about and install security updates, as well as displaying additional details about the updates.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your input on our documentation. Please let us know how we could make it better. To do so:

- For simple comments on specific passages:
  1. Make sure you are viewing the documentation in the *Multi-page HTML* format. In addition, ensure you see the **Feedback** button in the upper right corner of the document.
  2. Use your mouse cursor to highlight the part of text that you want to comment on.
  3. Click the **Add Feedback** pop-up that appears below the highlighted text.
  4. Follow the displayed instructions.
- For submitting more complex feedback, create a Bugzilla ticket:
  1. Go to the Bugzilla website.
  2. As the Component, use **Documentation**.
  3. Fill in the **Description** field with your suggestion for improvement. Include a link to the relevant part(s) of documentation.
  4. Click **Submit Bug**.

CHAPTER 1. IDENTIFYING SECURITY UPDATES

This chapter elaborates on the *security advisories* term and describes how you can display a list of available and already installed security updates.

1.1. WHAT ARE SECURITY ADVISORIES?

Red Hat provides information about security flaws that affect Red Hat products and services in the form of security advisories.

Red Hat Security Advisories (RHSA) contain important information, such as:

- Severity
- Summary of fixed issues
- Links to the tickets about the problem. Note that not all tickets are public.
- CVE numbers and links with additional details, such as the attack complexity.

Additional resources

- List of Red Hat Security Advisories

1.2. DISPLAYING AVAILABLE SECURITY UPDATES

Use this procedure to list available security updates on your system with the **yum** utility.

Prerequisites

- A valid Red Hat subscription is assigned to the host.

Procedure

1. List the security updates available for the host which have not been installed:

```
$ sudo yum updateinfo list updates security
...
RHSA-2019:0997 Important/Sec. platform-python-3.6.8-2.el8_0.x86_64
RHSA-2019:0997 Important/Sec. python3-libs-3.6.8-2.el8_0.x86_64
RHSA-2019:0990 Moderate/Sec.  systemd-239-13.el8_0.3.x86_64
...
```

1.3. DISPLAYING SECURITY UPDATES THAT ARE INSTALLED ON A HOST

To display the list of security updates which have been installed on a Red Hat Enterprise Linux 8 host, use the **yum updateinfo list security installed** command.

Procedure

1. Display the list of security updates that have been installed on the host:

```
$ sudo yum updateinfo list security installed
...
RHSA-2019:1234 Important/Sec. libssh2-1.8.0-7.module+el8+2833+c7d6d092
RHSA-2019:4567 Important/Sec. python3-libs-3.6.7.1.el8.x86_64
RHSA-2019:8901 Important/Sec. python3-libs-3.6.8-1.el8.x86_64
...
```

If multiple updates of a single package have been installed, **yum** lists all advisories for the package. In the previous example, two security updates for the **python3-libs** package have been installed since Red Hat Enterprise Linux 8 installation.

CHAPTER 2. VIEWING SECURITY ADVISORIES

This chapter describes where you can find information about Red Hat Security Advisories (RHSA) and how to display the advisories.

2.1. DISPLAYING ADVISORIES ON THE CUSTOMER PORTAL

Red Hat publishes security advisories on the Red Hat Customer Portal. This section describes where you find the advisories, and how to filter and display them.

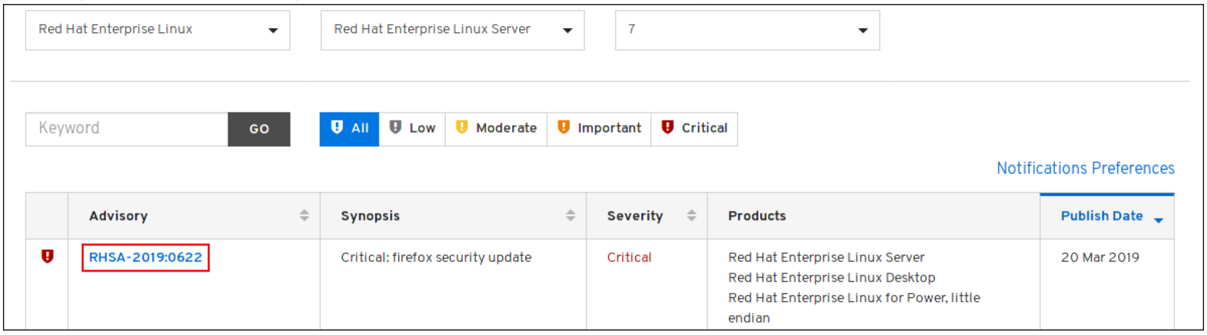
Procedure

1. Open https://access.redhat.com/security/security-updates/ in a browser.
   This page lists all security advisories Red Hat published.

2. Optionally, filter for a specific product, variant, version, and architecture. For example, to display only advisories for Red Hat Enterprise Linux 8, set the following filters:

   - Product: Red Hat Enterprise Linux
   - Variant: All Variants
   - Version: 8
     Alternatively, select a minor version, such as 8.2.

3. To display details of a specific advisory, click the advisory’s ID in the table.



	Advisory	Synopsis	Severity	Products	Publish Date
	RHSA-2019:0622	Critical: firefox security update	Critical	Red Hat Enterprise Linux Server Red Hat Enterprise Linux Desktop Red Hat Enterprise Linux for Power, little endian	20 Mar 2019

2.2. DISPLAYING A SPECIFIC ADVISORY USING YUM

If an update provided by an advisory is not already installed, use the **yum** utility to display the advisory.

Prerequisites

- A valid Red Hat subscription is assigned to the host.
- The ID of the security advisory is known. For details about displaying advisories of installed and available security updates for the host, see Chapter 1, *Identifying security updates*.
- The update provided by the advisory is not installed.

Procedure

1. Display the advisory. For example, to display the details of the **RHSA-2019:0997** advisory:

```
$ sudo yum updateinfo info RHSA-2019:0997
```

```
==========================================================================
====
  Important: python3 security update
==========================================================================
====
  Update ID: RHSA-2019:0997
       Type: security
    Updated: 2019-05-07 05:41:52
       Bugs: 1688543 - CVE-2019-9636 python: Information Disclosure due to urlsplit improper
NFKC normalization
       CVEs: CVE-2019-9636
Description: ...
```

CHAPTER 3. INSTALLING SECURITY UPDATES

This chapter describes how to install security updates on Red Hat Enterprise Linux 8.

Prerequisites

- A valid Red Hat subscription is assigned to the host.

3.1. INSTALLING ALL AVAILABLE SECURITY UPDATES

This section describes how to install all security updates available for a host.

Procedure

1. To install all security updates, enter:

   ```
   $ sudo yum update --security
   ```

   Note that without the **--security** parameter, **yum** installs updates also that include bug fixes and enhancements.

2. Press **y** to confirm, and start the installation:

   ```
   ...
   Transaction Summary
   =========================================
   Upgrade  ... Packages

   Total download size: ... M
   Is this ok [y/d/N]: y
   ```

3. Optionally, list the processes that require to be restarted manually after installing the updated packages:

   ```
   $ sudo yum needs-restarting
   ```

Additional resources

- Section 4.1, “Displaying which services require a restart after applying security updates”

3.2. INSTALLING A SECURITY UPDATE PROVIDED BY A SPECIFIC ADVISORY

In certain situations, for example, if a specific service can be updated without scheduling a downtime, administrators want to install only security updates for this service, and install all other security updates later.

This section explains how to install the updated packages provided by a specific security advisory.

Prerequisites

- A valid Red Hat subscription is assigned to the host.

- The ID of the security advisory is known. For details about displaying advisories of installed and available security updates for the host, see Chapter 1, *Identifying security updates*.

Procedure

1. Install the security updates provided by a specific security advisory. For example, to install the updates provided by the **RHSA-2019:0997** advisory, enter:

   ```
   $ sudo yum update --advisory=RHSA-2019:0997
   ```

2. Press **y** to confirm, and start the installation:

   ```
   ...
   Transaction Summary
   ============================================
   Upgrade  ... Packages

   Total download size: ... M
   Is this ok [y/d/N]: y
   ```

3. Optionally, list the processes that require to be restarted manually after installing the updated packages:

   ```
   $ sudo yum needs-restarting
   ```

Additional resources

- Section 4.1, “Displaying which services require a restart after applying security updates”

CHAPTER 4. ADDITIONAL TASKS AFTER APPLYING SECURITY UPDATES

After you have installed security updates on Red Hat Enterprise Linux 8, you may need to perform additional tasks. This section describes these tasks.

4.1. DISPLAYING WHICH SERVICES REQUIRE A RESTART AFTER APPLYING SECURITY UPDATES

When you update a package on Red Hat Enterprise Linux 8, certain processes using updated libraries and executables might need to be restarted manually. This section explains how to identify these processes.

Prerequisites

- Red Hat Enterprise Linux 8 updates have been installed. For details, see Chapter 3, *Installing security updates*.

Procedure

1. To list all processes that still use libraries or executables from the time before the update:

   ```
   $ sudo yum needs-restarting
   1107 : /usr/sbin/rsyslogd -n
   1199 : -bash
   ...
   ```

   The **yum needs-restarting** command lists only processes, not services. This means that you cannot restart all processes listed using the **systemctl** utility. For example, the **bash** process in the output will be terminated when the user that owns this process logs out.