



Red Hat Enterprise Linux 9

Managing and monitoring security updates

Update RHEL 9 system security to prevent attackers from exploiting known flaws

Red Hat Enterprise Linux 9 Managing and monitoring security updates

Update RHEL 9 system security to prevent attackers from exploiting known flaws

Legal Notice

Copyright © 2023 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

Learn how to install security updates and display additional details about the updates to keep your Red Hat Enterprise Linux systems secured against newly discovered threats and vulnerabilities.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE	3
PROVIDING FEEDBACK ON RED HAT DOCUMENTATION	4
CHAPTER 1. IDENTIFYING SECURITY UPDATES	5
1.1. WHAT ARE SECURITY ADVISORIES?	5
1.2. DISPLAYING SECURITY UPDATES THAT ARE NOT INSTALLED ON A HOST	6
1.3. DISPLAYING SECURITY UPDATES THAT ARE INSTALLED ON A HOST	6
1.4. DISPLAYING A SPECIFIC ADVISORY USING DNF	7
CHAPTER 2. INSTALLING SECURITY UPDATES	8
2.1. INSTALLING ALL AVAILABLE SECURITY UPDATES	8
2.2. INSTALLING A SECURITY UPDATE PROVIDED BY A SPECIFIC ADVISORY	8
2.3. INSTALLING SECURITY UPDATES AUTOMATICALLY	9
2.4. ADDITIONAL RESOURCES	10

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see [our CTO Chris Wright's message](#).

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our documentation. Let us know how we can improve it.

Submitting comments on specific passages

1. View the documentation in the **Multi-page HTML** format and ensure that you see the **Feedback** button in the upper right corner after the page fully loads.
2. Use your cursor to highlight the part of the text that you want to comment on.
3. Click the **Add Feedback** button that appears near the highlighted text.
4. Add your feedback and click **Submit**.

Submitting feedback through Jira (account required)

1. Log in to the [Jira](#) website.
2. Click **Create** in the top navigation bar
3. Enter a descriptive title in the **Summary** field.
4. Enter your suggestion for improvement in the **Description** field. Include links to the relevant parts of the documentation.
5. Click **Create** at the bottom of the dialogue.

CHAPTER 1. IDENTIFYING SECURITY UPDATES

Keeping enterprise systems secure from current and future threats requires regular security updates. Red Hat Product Security provides the guidance you need to confidently deploy and maintain enterprise solutions.

1.1. WHAT ARE SECURITY ADVISORIES?

Red Hat Security Advisories (RHSA) document the information about security flaws being fixed in Red Hat products and services.

Each RHSA includes the following information:

- Severity
- Type and status
- Affected products
- Summary of fixed issues
- Links to the tickets about the problem. Note that not all tickets are public.
- Common Vulnerabilities and Exposures (CVE) numbers and links with additional details, such as attack complexity.

Red Hat Customer Portal provides a list of Red Hat Security Advisories published by Red Hat. You can display details of a specific advisory by navigating to the advisory's ID from the list of Red Hat Security Advisories.

Figure 1.1. List of security advisories

The screenshot shows the 'Security Advisories' page in the Red Hat Customer Portal. The page has a navigation bar with 'Security Updates' and 'Security Advisories'. Below the navigation bar are three main sections: 'Security Advisories' (active), 'Red Hat CVE Database', and 'Security Labs'. There are four filters: 'Red Hat Enterprise Linux', 'All Variants', 'All Versions', and 'All Architectures'. Below the filters is a search bar with a 'GO' button and a severity filter bar with options: 'All', 'Low', 'Moderate', 'Important', and 'Critical'. The 'Important' filter is selected. There are links for 'Notifications' and 'Preferences'. The main table lists the following advisories:

Advisory	Synopsis	Severity	Products	Publish Date
RHSA-2022:1491	Important: java-1.8.0-openjdk security update	Important	Red Hat CodeReady Linux Builder for ARM 64 Red Hat Enterprise Linux for x86_64 Red Hat Enterprise Linux for Power, little endian Red Hat CodeReady Linux Builder for Power, little endian Red Hat Enterprise Linux for ARM 64 Red Hat CodeReady Linux Builder for x86_64 Red Hat Enterprise Linux for IBM z Systems	25 Apr 2022
RHSA-2022:1488	Important: java-1.8.0-openjdk security update	Important	Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions	25 Apr 2022

Optionally, you can also filter the results by specific product, variant, version, and architecture. For example, to display only advisories for Red Hat Enterprise Linux 9, you can set the following filters:

- Product: Red Hat Enterprise Linux
- Variant: All Variants
- Version: 9
- Optionally, select a minor version.

Additional resources

- [List of Red Hat Security Advisories](#)
- [Anatomy of a Red Hat Security Advisory](#)
- [Red Hat Customer Portal](#)

1.2. DISPLAYING SECURITY UPDATES THAT ARE NOT INSTALLED ON A HOST

You can list all available security updates for your system by using the **dnf** utility.

Prerequisite

- A Red Hat subscription attached to the host.

Procedure

- List all available security updates which have not been installed on the host:

```
# dnf 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

You can list installed security updates for your system by using the **dnf** utility.

Procedure

- List all security updates which are installed on the host:

```
# dnf 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 are installed, **dnf** lists all advisories for the package. In the previous example, two security updates for the **python3-libs** package have been installed since the system installation.

1.4. DISPLAYING A SPECIFIC ADVISORY USING DNF

You can use the **dnf** utility to display a specific advisory information that is available for an update.

Prerequisites

- A Red Hat subscription attached to the host.
- You have a security advisory **Update ID**. See [identifying the security advisory updates](#).
- The update provided by the advisory is not installed.

Procedure

- Display a specific advisory:

```
# dnf updateinfo info <Update ID>
=====
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: ...
```

Replace the *Update ID* with the required advisory. For example, **# dnf updateinfo info <RHSA-2019:0997>**.

CHAPTER 2. INSTALLING SECURITY UPDATES

2.1. INSTALLING ALL AVAILABLE SECURITY UPDATES

To keep the security of your system up to date, you can install all currently available security updates using the **dnf** utility.

Prerequisite

- A Red Hat subscription attached to the host.

Procedure

1. Install security updates using **dnf** utility:

```
# dnf update --security
```



NOTE

The **--security** parameter is important. Without it, **dnf update** installs all updates, including bug fixes and enhancements.

2. Confirm and start the installation by pressing **y**:

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

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

3. Optional: list processes that require a manual restart of the system after installing the updated packages:

```
# dnf needs-restarting
1107 : /usr/sbin/rsyslogd -n
1199 : -bash
```



NOTE

This command lists only processes that require a restart, and not services. That is, you cannot restart processes listed using the **systemctl** utility. For example, the **bash** process in the output is terminated when the user that owns this process logs out.

2.2. INSTALLING A SECURITY UPDATE PROVIDED BY A SPECIFIC ADVISORY

In certain situations, you might want to install only specific updates. For example, if a specific service can be updated without scheduling a downtime, you can install security updates for only this service, and install the remaining security updates later.

Prerequisites

- A Red Hat subscription attached to the host.
- You have a security advisory Update ID. See [identifying the security advisory updates](#).

Procedure

1. Install a specific advisory:

```
# dnf update --advisory=<Update ID>
```

Replace the *Update ID* with the required advisory. For example, **#dnf update --advisory=<RHSA-2019:0997>**

2. Confirm and start the installation by pressing **y**:

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

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

3. Optional: List the processes that require a manual restart of the system after installing the updated packages:

```
# dnf needs-restarting
1107 : /usr/sbin/rsyslogd -n
1199 : -bash
```



NOTE

This command lists only processes that require a restart, and not services. This means that you cannot restart all processes listed by using the **systemctl** utility. For example, the **bash** process in the output is terminated when the user that owns this process logs out.

2.3. INSTALLING SECURITY UPDATES AUTOMATICALLY

Use the following procedure to update your system automatically with security updates.

Prerequisites

- A Red Hat subscription attached to the host.

Procedure

1. Install `dnf-automatic` using `dnf`

```
# dnf install dnf-automatic
```

2. Confirm and start the installation by pressing `y`:

```
...
Transaction Summary
=====
Upgrade ... Packages
Total download size: ... M
Is this ok [y/d/N]: y
```

3. Open the `/etc/dnf/automatic.conf` file in a text editor of your choice, for example:

```
# vi /etc/dnf/automatic.conf
```

4. Configure the `upgrade_type = security` option in the `[commands]` section:

```
[commands]
# What kind of upgrade to perform:
# default                = all available upgrades
# security                = only the security upgrades
upgrade_type = security
```

5. Enable the **systemd timer unit**

```
# systemctl enable --now dnf-automatic-install.timer
```

Additional resources

- **`dnf-automatic(8)`** man page

2.4. ADDITIONAL RESOURCES

- See practices of securing workstations and servers in [Security Hardening](#) document.
- [Security-Enhanced Linux](#) documentation.