



# Red Hat Enterprise Linux 9

## 管理及监控安全更新

在 Red Hat Enterprise Linux 9 中管理和监控安全更新的指南



## Red Hat Enterprise Linux 9 管理及监控安全更新

---

在 Red Hat Enterprise Linux 9 中管理和监控安全更新的指南

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

## 法律通告

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Managing\_and\_monitoring\_security\_updates.ent file |.

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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

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

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> 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<sup>®</sup> 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.

## 摘要

本文档描述了如何学习和安装安全更新，以及显示更新的附加详情。

---

## 目录

让开源更具包容性 .....	3
对红帽文档提供反馈 .....	4
<b>第 1 章 识别安全更新 .....</b>	<b>5</b>
1.1. 什么是安全公告？ .....	5
1.2. 显示主机上未安装的安全更新 .....	6
1.3. 显示在主机上安装的安全更新 .....	6
1.4. 使用 DNF 显示特定公告 .....	7
<b>第 2 章 安装安全更新 .....</b>	<b>8</b>
2.1. 安装所有可用的安全更新 .....	8
2.2. 安装特定公告提供的安全更新 .....	8
2.3. 其他资源 .....	9



## 让开源更具包容性

红帽致力于替换我们的代码、文档和 Web 属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。详情请查看 [CTO Chris Wright 的信息](#)。

## 对红帽文档提供反馈

我们感谢您对文档提供反馈信息。请让我们了解如何改进文档。

- 关于特定内容的简单评论：
  1. 请确定您使用 *Multi-page HTML* 格式查看文档。另外，确定 **Feedback** 按钮出现在文档页的右上方。
  2. 用鼠标指针高亮显示您想评论的文本部分。
  3. 点在高亮文本上弹出的 **Add Feedback**。
  4. 按照显示的步骤操作。
- 要通过 Bugzilla 提交反馈，请创建一个新的 ticket：
  1. 进入 [Bugzilla](#) 网站。
  2. 在 Component 中选择 **Documentation**。
  3. 在 **Description** 中输入您要提供的信息。包括文档相关部分的链接。
  4. 点 **Submit Bug**。



# 第 1 章 识别安全更新

为了确保企业系统不受当前和未来的安全威胁，系统需要定期进行安全更新。红帽产品安全团队为您提供安心部署和维护企业解决方案所需的指导。

## 1.1. 什么是安全公告？

红帽安全公告（Red Hat Security Advisories，简称 RHSA）记录了有关红帽产品和服务中安全漏洞的信息。

每个 RHSA 包括以下信息：

- 严重性
- 类型和状态
- 受影响的产品
- 修复问题的摘要
- 问题相关的报告链接。请注意，不是所有的报告都是公开的。
- 公共漏洞和暴露（Common Vulnerabilities and Exposures，简称 CVE）编号以及更多详情（如攻击复杂性）的链接。

红帽客户门户（Red Hat Customer Portal）提供了红帽发布的红帽安全公告列表。您可以通过访问红帽安全公告列表中的公告 ID 来显示特定公告的详情。

图 1.1. 安全公告列表

Advisory	Synopsis	Severity	Products	Publish Date
<b>RHSA-2022:1491</b>	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
<b>RHSA-2022:1488</b>	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

此外，您还可以根据特定产品、变体、版本和架构过滤结果。例如，要只显示 Red Hat Enterprise Linux 9 公告，您可以设置以下过滤器：

- 产品：Red Hat Enterprise Linux
- 变体：所有变体
- 版本：9
- （可选）选择一个次版本。

#### 其他资源

- [红帽安全公告列表](#)
- [红帽安全公告分析](#)
- [红帽客户门户网站](#)

## 1.2. 显示主机上未安装的安全更新

您可以使用 **dnf** 实用程序列出系统的所有可用安全更新。

#### 前提条件

- 附加到主机的红帽订阅。

#### 步骤

- 列出主机上尚未安装的所有可用安全更新：

```
# 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. 显示在主机上安装的安全更新

您可以使用 **dnf** 实用程序列出已安装系统的安全更新。

#### 步骤

- 列出主机上安装的所有安全更新：

```
# 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
...
```

如果安装了多个软件包更新，**dnf** 将列出该软件包的所有公告。在上例中，自系统安装以来，已安装了 **python3-libs** 软件包的两个安全更新。

## 1.4. 使用 DNF 显示特定公告

您可以使用 **dnf** 实用程序显示可用于更新的特定公告信息。

### 先决条件

- 附加到主机的红帽订阅。
- 您有一个安全公告更新 ID。请参阅[识别安全公告更新](#)。
- 公告提供的更新没有安装。

### 步骤

- 显示一个特定公告：

```
# 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: ...
```

将 *更新ID* 替换为所需的公告。例如：**# dnf updateinfo info <RHSA-2019:0997>**。

## 第 2 章 安装安全更新

### 2.1. 安装所有可用的安全更新

要保持系统的安全性，您可以使用 **dnf** 工具安装所有当前可用的安全更新。

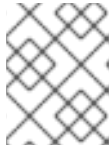
#### 前提条件

- 附加到主机的红帽订阅。

#### 步骤

1. 使用 **dnf** 工具安装安全更新：

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



#### 注意

**--security** 参数非常重要。如果没有它，**dnf update** 会安装所有更新，包括错误修复和增强。

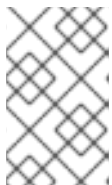
2. 按 **y** 确认并启动安装：

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

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

3. 可选：在安装更新的软件包后列出需要手动重启系统的进程：

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



#### 注意

此命令仅列出需要重启的进程，而不是服务。也就是说，您无法使用 **systemctl** 实用程序重启列出的进程。例如，当拥有此进程的用户注销时，输出中的 **bash** 进程将被终止。

### 2.2. 安装特定公告提供的的安全更新

在某些情况下，您可能只希望安装特定的更新。例如，某个特定的服务可以在不需要停机的情况下进行更新，您可以只为该服务安装安全更新，并在以后安装剩余的安全更新。

#### 先决条件

- 附加到主机的红帽订阅。

- 您有一个安全公告更新 ID。请参阅[识别安全公告更新](#)。

## 步骤

1. 安装特定的公告：

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

将 *更新 ID* 替换为所需的公告。例如：`#dnf update --advisory= <RHSA-2019:0997>`

2. 按 **y** 确认并启动安装：

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

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

3. 可选：在安装更新的软件包后列出需要手动重启系统的进程：

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



### 注意

此命令仅列出需要重启的进程，而不是服务。这意味着您无法使用 **systemctl** 工具重启所有列出的进程。例如，当拥有此进程的用户注销时，输出中的 **bash** 进程将被终止。

## 2.3. 其他资源

- 请参阅[安全固化](#)文档中保护工作站和服务器的做法。
- [Security-Enhanced Linux](#) 文档。