Red Hat Enterprise Linux 9

管理及监控安全更新

更新 RHEL 9 系统安全性，以防止攻击者利用已知的漏洞

Last Updated: 2024-06-26

Red Hat Enterprise Linux 9 管理及监控安全更新

更新 RHEL 9 系统安全性，以防止攻击者利用已知的漏洞

法律通告

摘要

了解如何安装安全更新，并显示有关更新的额外详情，以保护 Red Hat Enterprise Linux 系统免受新发现的威胁和漏洞。

目录

对红帽文档提供反馈

我们感谢您对我们文档的反馈。帮助我们如何进行改进。

通过 Jira 提交反馈（需要帐户）

1. 登录到 Jira 网站。
2. 在顶部导航栏中点 **Create**
3. 在 **Summary** 字段中输入描述性标题。
4. 在 **Description** 字段中输入您的建议以改进。包括文档相关部分的链接。
5. 点对话框底部的 **Create**。

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了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？

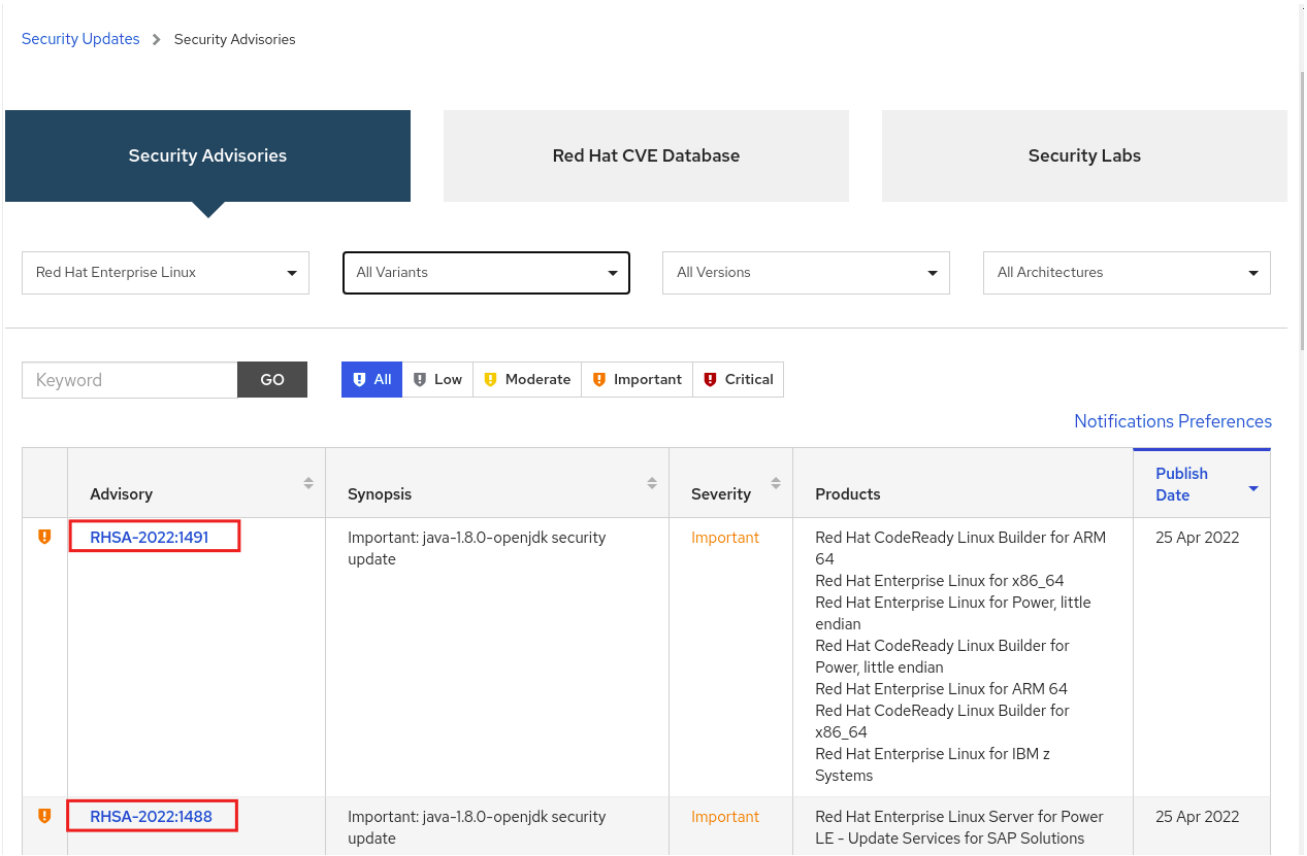
红帽安全公告（Red Hat Security Advisories，简称 RHSA）记录了有关红帽产品和服务中安全漏洞的信息。

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



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，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。

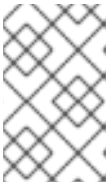
2. 按 **y** 确认并启动安装：

```
...
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。

- 您有要更新的安全公告的 ID。如需更多信息，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 *<Update_ID>* 替换为您要更新的安全公告的 ID。例如：

```
# dnf update --advisory=RHSA-2019:0997
```

重要

您可以使用 **dnf upgrade-minimal --advisory= <*Update_ID*>** 命令更新以最小版本更改来应用特定公告。

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. 自动安装安全更新

您可以配置您的系统，使其自动下载并安装所有安全更新。

先决条件

- 附加到主机的红帽订阅。
- **dnf-automatic** 软件包已安装。

步骤

1. 在 **/etc/dnf/automatic.conf** 文件中，在 **[commands]** 部分下，确保将 **upgrade_type** 选项设置为 **default** 或 **security** ：

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

2. 启用并启动 **systemd** 计时器单元：

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

验证

1. 验证计时器是否已启用：

```
# systemctl status dnf-automatic-install.timer
```

其他资源

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

2.4. 其他资源

- 请参阅安全固化文档中保护工作站和服务器安全的做法。
- Security-Enhanced Linux 文档。