Red Hat Enterprise Linux 8

管理及监控安全更新

管理及监控 Red Hat Enterprise Linux 8 中的安全更新指南

Last Updated: 2021-06-07

Red Hat Enterprise Linux 8 管理及监控安全更新

管理及监控 Red Hat Enterprise Linux 8 中的安全更新指南

法律通告

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

使开源包含更多

红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。我们从这四个术语开始： master、slave、blacklist 和 whitelist。这些更改将在即将发行的几个发行本中逐渐实施。如需了解更多详细信息，请参阅 CTO Chris Wright 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。要做到这一点：

- 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。
- 要提交更复杂的反馈，请创建一个 Bugzilla 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

红帽产品安全团队为安全部署企业解决方案提供了所需的指导、稳定性和安全性。务必要识别安全更新以保持系统更新和安全。

1.1. 什么是安全公告？

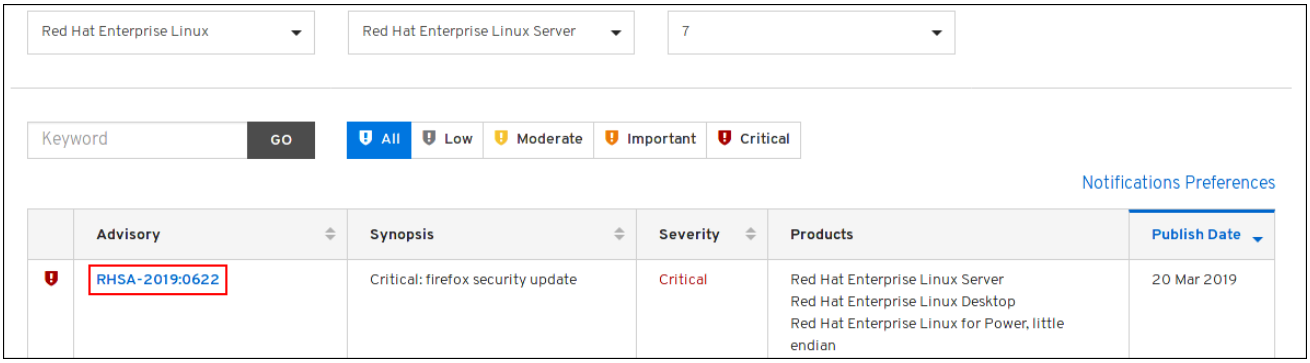
红帽安全公告(RHSA)包括了红帽产品和服务中解决的安全漏洞的信息。

每个 RHSA 都包括以下信息：

- 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。
- 常见的 Vulnerabilities and Exposures(CVE)号码,以及其它详情的链接,如攻击复杂性。

红帽客户门户网站提供红帽安全公告列表。您可以从以下图 1 中导航到公告的 ID,显示特定公告的详情。

图 1.1. 安全公告列表



另外,您还可以使用特定的产品、变体、版本和架构过滤结果。例如：仅显示 Red Hat Enterprise Linux 8 公告,您可以设置以下过滤器：

- Product: Red Hat Enterprise Linux
- Variant: All Variants
- Version: 8
- 或者，选择一个次版本，如 8.2。

其它资源

- 红帽安全公告列表
- 红帽安全公告 anatomy
- 红帽客户门户网站

1.2. 显示没有在主机上安装的安全更新

您可以使用 **yum** 实用程序列出系统可用的安全更新。

先决条件

- 附加到主机的红帽订阅。

流程

- 要列出安全更新,请执行以下操作：

```
# 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
...
```

以上命令列出所有没有在主机上安装的安全更新。

1.3. 显示在主机上安装的安全更新

您可以使用 **yum** 实用程序列出系统安装的安全更新。

流程

- 要列出安全更新,请执行：

```
# 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
...
```

以上命令列出已在主机上安装的所有可用的安全更新。

如果安装了多个软件包更新, **yum** 列出该软件包的所有公告。在上例中,自系统安装以来,已经安装了两个 **python3-libs** 软件包的安全更新。

1.4. 使用 YUM 显示具体公告

您可以使用 **yum** 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。
- 通过标识安全公告 更新来获得安全公告 **Update ID**。
- 公告提供的更新没有安装。

流程

- 显示特定公告。例如,显示 **RHSA-2019:0997** 公告详情：

```
# 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: ...
```

您可以将公告 **Update ID** 替换为任何需要的公告。

第 2 章 安装安全更新

2.1. 安装所有可用的安全更新

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

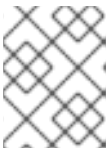
先决条件

- 附加到主机的红帽订阅。

流程

1. 执行：

```
# * yum update --security*
```



注意

--security 参数很重要,如果未引用 **yum**,则会安装所有更新,包括程序错误修复和增强。

2. 要确认并开始停机,按以下方式 **进行**:

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

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

3. 可选：列出安装更新的软件包后需要手动重启系统的进程：

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

注意

这个命令只列出需要重启的进程,而不包括服务。这意味着您无法使用 **systemctl** 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** 进程会被终止。

2.2. 安装特定公告提供的安全更新

在某些情况下，例如，如果某个特定服务可以在不需要调度停机时间的情况下更新一个特定安全更新，则系统管理员可能只想为这个服务安装这个特定的安全更新，然后在其他时间再安装其他安全更新。

先决条件

- 附加到主机的红帽订阅。

- 通过标识安全公告更新来获取 安全公告更新 ID。

流程

1. 显示特定公告。例如,显示 **RHSA-2019:0997** 公告详情：

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

将公告 **Update ID** 替换为所需公告。

2. 要确认并开始安装, 按以下 **操作**:

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

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

3. 可选：列出安装更新的软件包后需要手动重启系统的进程：

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

注意

这个命令只列出需要重启的进程,而不包括服务。这意味着您无法使用 **systemctl** 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** 进程会被终止。

第 3 章 其他参考资源

- 有关保护工作站和服务器的更多信息,请参阅 RHEL 8 安全强化文档。
- 有关 Security-Enhanced Linux 的详情,请参考 使用 SELinux 文档的 RHEL 8。