



Red Hat Insights 1-latest

使用 FedRAMP 生成安全漏洞服务报告

RHEL 系统暴露与 CVE 安全漏洞间的交流

RHEL 系统暴露与 CVE 安全漏洞间的交流

法律通告

Copyright © 2024 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.

摘要

通过 FedRAMP[®] 生成漏洞服务报告，将 RHEL 系统暴露于 CVE 安全漏洞。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、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 信息。

目录

第 1 章 INSIGHTS FOR RED HAT ENTERPRISE LINUX 漏洞服务报告概述	3
第 2 章 执行报告	4
2.1. 下载执行报告	4
2.2. 使用漏洞服务 API 下载执行报告	4
第 3 章 CVE 报告	6
3.1. 创建 CVE 的 PDF 报告	7
第 4 章 将漏洞数据导出为 JSON、CSV 或 PDF 文件	9
4.1. 从漏洞服务导出 CVE 数据	9
第 5 章 启用通知和集成	10
第 6 章 参考资料	11
对红帽文档提供反馈	12

第 1 章 INSIGHTS FOR RED HAT ENTERPRISE LINUX 漏洞服务报告概述

将基础架构安全暴露给不同的所有者(DevOps 团队、安全团队、执行团队)的能力至关重要。漏洞服务允许您下载以下报告来分析离线或与其他共享：

- **执行报告.PDF** 概述和概述您的基础架构暴露，面向执行人员
- **CVE 报告**。所选 PDF 报告，过滤过滤的 CVE，您的基础架构已公开，旨在突出显示和共享漏洞数据
- **漏洞数据导出**。根据您在执行导出时已存在的过滤器，将所选 CVE 数据导出到 JSON 或 CSV 文件

第 2 章 执行报告

您可以下载高级别的执行报告，总结基础架构的安全暴露。执行报告分为两个到三页 PDF 文件，专为执行人员设计，并包含以下信息：

第 1 页

- 分析的 RHEL 系统数量
- 系统当前公开的单独 CVE 数量
- 您的基础架构中的安全规则数量
- 带有公告的 CVE 列表

第 2 页

- 严重性为 CVE 的百分比(CVSS 基本分数)范围
- 7、30 和 90 天时间范围发布的 CVE 数量
- 您的基础架构中的前三个 CVE，包括安全规则和已知的漏洞

第 3 页

- 安全规则按严重性分类
- 前 3 个安全规则，包括公开的系统严重性和数量

2.1. 下载执行报告

使用以下步骤下载执行报告：

流程

1. 进入到 [Security > Vulnerability > Reports](#) 选项卡，并在需要时登录。
2. 在 executive 报告 卡上，单击 **Download PDF**。
3. 单击 **Save File**，再单击 **OK**。

验证

1. 验证 PDF 文件是否在您的 **Downloads** 文件夹或其他指定位置。

2.2. 使用漏洞服务 API 下载执行报告

您可以使用 [漏洞服务 API](#) 下载执行报告。

- 请求 URL：<https://console.openshiftusgov.com/api/vulnerability/v1/report/executive>
- curl：

```
curl -X GET "https://console.openshiftusgov.com/api/vulnerability/v1/report/executive" -H  
"accept: application/vnd.api+json"
```

第 3 章 CVE 报告

您可以创建 PDF 报告，显示已过滤的系统 CVE 列表。为每个报告指定相关名称、应用过滤器并添加用户备注，以向特定利益相关者呈现集中数据。

您可以在设置 PDF 报告时应用以下过滤器：

- **安全规则。** 仅显示带有安全规则标签的 CVE。
- **已知漏洞利用。** 仅显示带有已知利用 (known exploit) 标签的 CVE。
- **严重性。** 选择一个或多个值：Critical、Important、Moderate、Low 或 Unknown。
- **CVSS 基本分数。** 选择一个或多个范围：All, 0.0-3.9, 4.0-7.9, 8.0-10.0, N/A (不适用)
- **商业风险。** 选择一个或多个值：High, Medium, Low, Not defined。
- **状态。** 选择一个或多个值：Not review, In review, On-hold, Scheduled for patch, Resolved, No action - risk accepted, Resolved via mitigation.
- **发布日期。** 从 All, Last 7 days, Last 30 天, Last 90 days, Last 90 days, Last year, 或 1 年以前选择。
- **适用于操作系统。** 选择要过滤和查看的系统的 RHEL 次版本。
- **标签。** 选择标记的系统组。有关标签和系统组群的更多信息，请参阅 [系统标签和组](#)
- **公告。** 选择是否只显示相关的公告(errata)，只有 CVE 没有公告，或所有 CVE。

CVE 报告列出了 CVE，将每个链接到 Red Hat CVE 数据库中相应的 CVE 页面，以便您可以了解更多有关它的信息。该列表主要由 CVE 的发布日期排序，以及列表顶部最新发布的 CVE。

Insights 漏洞 CVE 报告示例



Prepared 04 Apr 2022 14:35 UTC

Insights Vulnerability CVE Report

This is a summary of CVEs identified by Red Hat that may impact your Red Hat Enterprise Linux (RHEL) systems.

This report includes CVEs with a CVSS base score of 0.0 - 10.0; published anytime.

These CVEs apply to systems in your inventory tagged with `satellite:activation_key=RHEL8_AK`.

The vulnerability service identified 625 CVEs within this criteria that impact at least one of your 17 analyzed RHEL systems. Of the identified CVEs, 4 CVEs have a known exploit.

CVE ID	Publish date	CVSS base score	Severity	Systems exposed	Business risk	Status
CVE-2019-18218	25 Aug 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25038	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25032	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25036	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25042	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25039	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25034	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2019-25035	10 Dec 2019	9.8	Moderate	4	Not defined	Not reviewed
CVE-2020-9850	09 July 2020	9.8	Moderate	3	Not defined	Not reviewed
Known exploit						
CVE-2020-9895	28 July 2020	9.8	Moderate	3	Not defined	Not reviewed

Known exploit: This CVE is identified with a "Known exploit" label because Red Hat has determined this CVE has a public exploit. This CVE is unpatched on your system. CVEs with this label should be addressed with high priority due to the risks posed by them. "Known exploit" does not mean we have taken steps to determine if the CVE has been exploited in your environment.

Security rule: Indicates a security rule associated with this CVE. Security rules are written by Red Hat to help you configure your systems.

3.1. 创建 CVE 的 PDF 报告

使用以下步骤创建可能影响您的系统的 CVE 的时间点快照。

先决条件

- 您必须登录 [Red Hat Hybrid Cloud Console](#)。

流程

1. 进入 Insights for Red Hat Enterprise Linux 应用程序的 [Security > Vulnerability > Reports](#) 页面。
2. 在 CVE 卡中，点 **Create report**。
3. 在弹出卡中根据需要进行选择：

Report by CVEs ×

Report title

Insights Vulnerability CVE Report

Filter CVEs by

Security rule: All ▼

Known exploit: All ▼

Severity: All ▼

CVSS base score: All ▼

Business risk: All ▼

Status: All ▼

Publish date: All ▼

Applies to OS: Any ▼

Applying to systems in your inventory meeting these criteria

Tags: All ▼

CVE data to include

All columns

Choose columns

Sort CVEs by

CVSS base score: High to Low (Default) ▼

User notes (optional)

Export report

Cancel

- a. (可选) 自定义报告标题。
 - b. 在 **Filter CVEs by** 下，单击每个过滤器下拉菜单并选择一个值。
 - c. 选择 **Tags** 只包括标记的系统组中的系统。
 - d. 在要包含的 CVE 数据下，默认激活 **Choose** 列，允许您取消选择您不想包含的列。保留对所有复选框的选择，或点 **All column** 来显示所有内容。
 - e. (可选) 添加备注，以提供预期受众的报告上下文。
4. 点 **Export report**，并允许应用程序一分钟生成报告。
 5. 选择打开或保存 PDF 文件（如果您的操作系统要求），然后单击**确定**。

第 4 章 将漏洞数据导出为 JSON、CSV 或 PDF 文件

通过这个漏洞服务，您可以在 RHEL 基础架构中的系统中导出 CVE 的数据。在漏洞服务中应用过滤器来查看一组特定的 CVE 或系统后，您可以根据这些标准导出数据。

这些报告可以通过 Red Hat Insights for Red Hat Enterprise Linux 应用程序访问，并可导出并下载为 .csv、.json 或 PDF 文件。

4.1. 从漏洞服务导出 CVE 数据

执行以下步骤从漏洞服务导出选择数据。

流程

1. 进入 [Security > Vulnerability > CVEs](#) 页面，并在需要时登录。
2. 应用过滤器并使用每个列顶部的排序功能来查找特定的 CVE。
3. 在 CVE 列表和过滤器菜单右侧，点 **Export** 图标 ，并选择 Export to JSON、Export to CSV 或 Export as PDF，根据您的下载偏好选择 **Export to JSON**、**Export to CSV** 或 **Export as PDF**。
4. 选择下载位置，然后单击**保存**。

第 5 章 启用通知和集成

您可以在 Red Hat Hybrid Cloud Console 上启用通知服务，以便在触发漏洞事件时发送通知。例如，您可以将通知服务配置为在安全问题影响您安装中的系统时自动发送电子邮件消息，或者发送每天发生的所有漏洞事件的电子邮件摘要。使用通知服务可为您持续检查 Red Hat Insights for RHEL 仪表板是否有事件触发的通知。

除了发送电子邮件信息外，您还可以将通知服务配置为以其他方式发送事件数据：

- 使用经过身份验证的客户端查询 Red Hat Insights API 获取事件数据
- 使用 Webhook 将事件发送到接受入站请求的第三方应用程序
- 将通知与 Splunk 等应用程序集成至应用程序仪表板

通知管理员为通知服务中的事件设置行为组。行为组指定每个通知的交付方法，以及通知是否发送到所有用户，还是仅向机构管理员发送。

机构管理员会创建一个具有 Notifications Administrator 角色的用户访问组，然后将帐户成员添加到组中。

从事件接收电子邮件通知的用户可能会设置其用户首选项，以便他们为每个事件接收单独的电子邮件或事件每日摘要。

其他资源

- 有关如何为漏洞事件设置通知和集成的更多信息，[请参阅使用 FedRAMP 在 Red Hat Hybrid Cloud Console 上配置通知，并将 Red Hat Hybrid Cloud Console 与第三方应用程序集成。](#)

第 6 章 参考资料

要了解更多有关漏洞服务或其他 Red Hat Insights for Red Hat Enterprise Linux 服务和功能的信息，以下资源也可能值得关注：

- [在 RHEL 系统上评估和监控安全漏洞](#)
- [Automation Toolkit > Remediations](#)
- [Red Hat Insights for Red Hat Enterprise Linux 文档](#)
- [Red Hat Insights for Red Hat Enterprise Linux 产品支持页面](#)

对红帽文档提供反馈

我们非常感谢并对我们文档的反馈进行优先排序。提供尽可能多的详细信息，以便快速解决您的请求。

先决条件

- 已登陆到红帽客户门户网站。

流程

要提供反馈，请执行以下步骤：

1. 点击以下链接：[Create Issue](#)
2. 在 **Summary** 文本框中描述问题或功能增强。
3. 在 **Description** 文本框中提供有关问题或请求的增强的详细信息。
4. 在 **Reporter** 文本框中键入您的名称。
5. 点 **Create** 按钮。

此操作会创建一个文档票据，并将其路由到适当的文档团队。感谢您花时间来提供反馈。