Red Hat Insights 2023

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

Last Updated: 2023-05-26

Red Hat Insights 2023 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

法律通告

摘要

生成漏洞服务报告，以提供 RHEL 系统中会受 CVE 安全漏洞影响的信息。 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 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. 下载摘要报告 4
2.2. 使用漏洞服务 API 下载主要报告 4

第 3 章 CVE 报告 5
3.1. 创建 CVE 的 PDF 报告 6

第 4 章 将漏洞数据导出为 JSON、CSV 或 PDF 文件 8
4.1. 从漏洞服务导出 CVE 数据 8

第 5 章 启用通知和集成 9

第 6 章 参考资料 10

对红帽文档提供反馈 11

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

能够将基础架构的安全性暴露给不同的利益相关者-DevOps 团队、安全团队、领导团队至关重要。漏洞服务可让您下载以下报告来分析离线或与其他共享：

- **参与报告。**PDF 摘要和安全漏洞概述公开您的基础架构，面向主要人员
- **CVE 报告.**PDF 报告，过滤了您的基础架构公开的 CVE，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所放入的过滤器将所选 CVE 数据导出到 JSON 或 CSV 文件

第 2 章 执行报告

您可以下载高级别报告，总结基础架构的安全风险。执行报告是两页到三页 PDF 文件，专为经理设计，并包括以下信息：

第 1 页

- 分析的 RHEL 系统数量
- 系统当前公开的独立 CVE 数量
- 基础架构中的安全规则数量

在第 2 页

- CVE 的百分比(CVSS 基本分数)范围
- 7、30 和 90 天时间框架发布的 CVE 数量
- 您的基础架构中有三个 CVE，包括安全规则和已知漏洞

在页面 3 上

- 安全规则按严重性划分
- 前 3 个安全规则，包括严重性和公开系统数

2.1. 下载摘要报告

使用以下步骤下载摘要报告：

流程

1. 进入 Red Hat Enterprise Linux > Vulnerability > Reports 选项卡，并在需要时登录。
2. 在附件 **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** 文件夹中或其他指定位置。

2.2. 使用漏洞服务 API 下载主要报告

您可以使用 漏洞服务 API 下载主要报告。

- 请求 URL ：https://console.redhat.com/api/vulnerability/v1/report/executive
- curl ：

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

第 3 章 CVE 报告

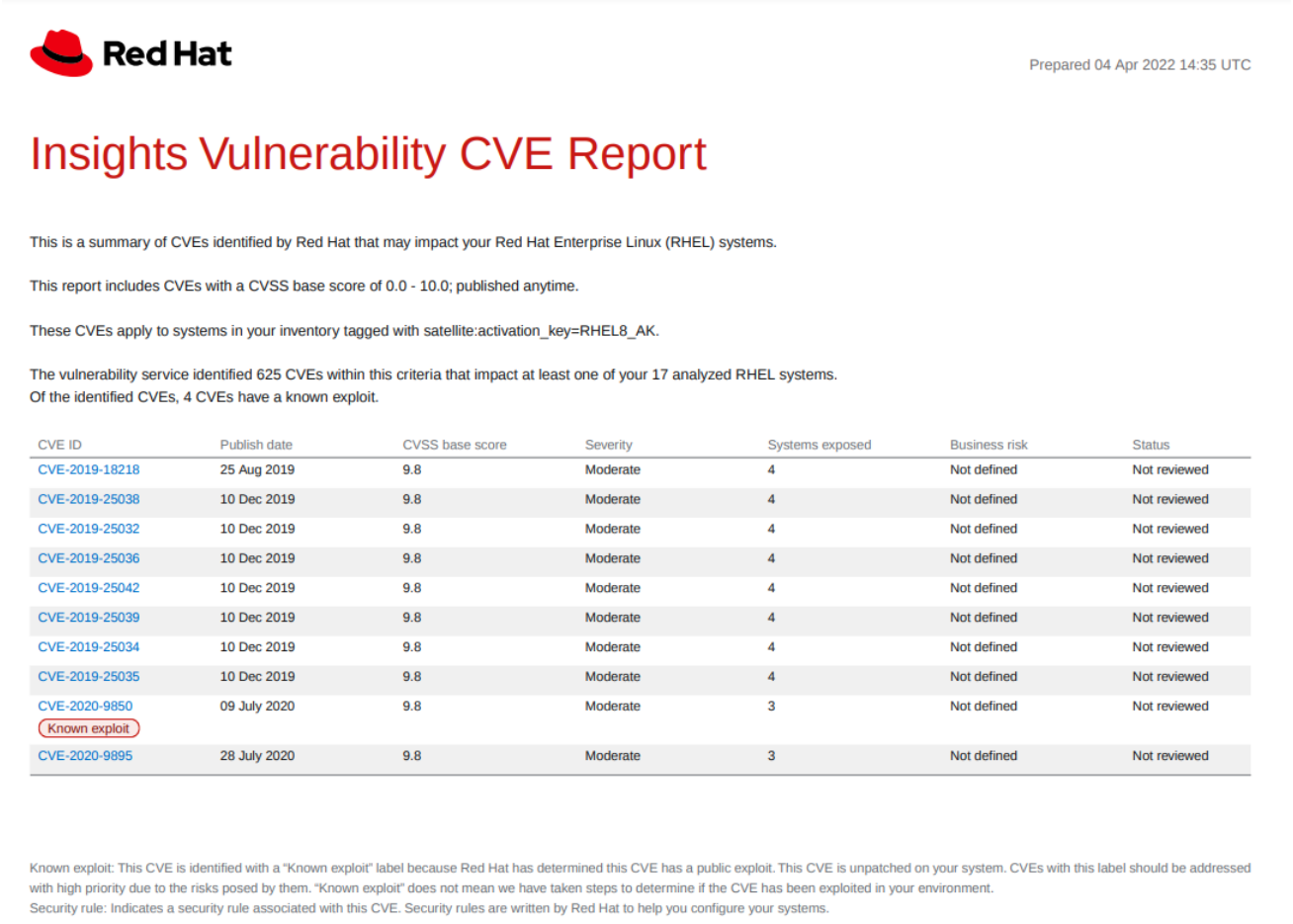
您可以创建 PDF 报告，显示系统公开的 CVE 的过滤列表。为每个报告指定相关名称、应用过滤器和添加用户备注，以向特定的利益相关者提供重点数据。

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。
- **已知的漏洞利用。**仅显示带有已知利用（knownn 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）
- **业务风险。**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 by mitigation.
- **发布日期。**从 All, Last 7 days, Last 30 days, Last 90 days, Last year, 或 More than 1 年以上选择。
- **适用于 OS。**选择要过滤和查看系统的 RHEL 次要版本。
- **标签。**选择标记的系统组。有关标签和系统组的更多信息，请参阅第 4 章系统标签和组，*评估和监控 RHEL 系统上的安全漏洞*

CVE 报告列出了 CVE，将每个 CVE 链接到 Red Hat CVE 数据库中的对应 CVE 页面，以便您可以了解更多有关它的信息。该列表主要根据 CVE 的发布日期排序，最新发布的 CVE 位于列表的顶部。

Insights 漏洞 CVE 报告示例



Red Hat

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 Known exploit	09 July 2020	9.8	Moderate	3	Not defined	Not reviewed
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

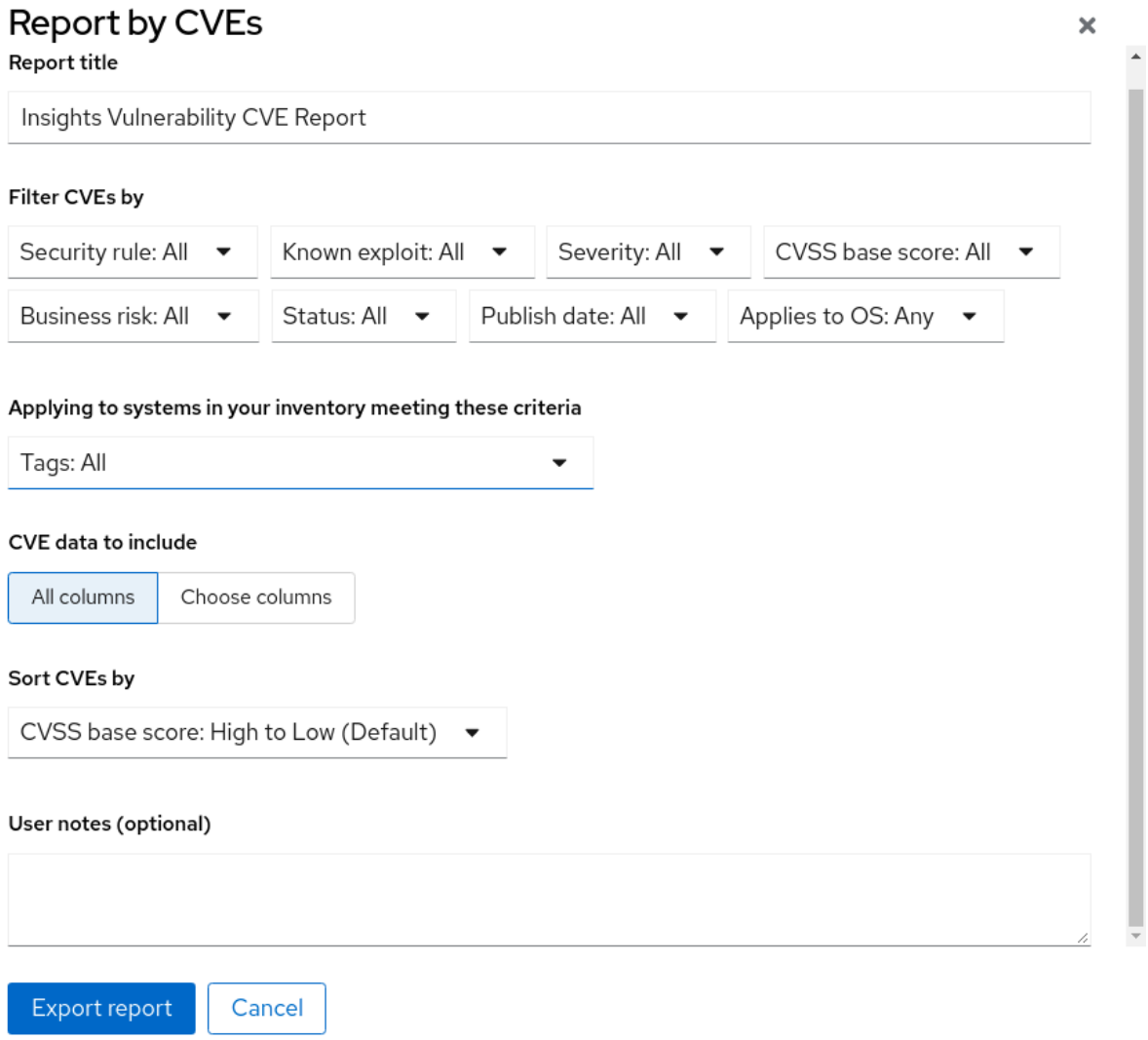
使用以下步骤创建可能会影响您的系统的 CVE 的时间点快照。

先决条件

- 您必须登录到 Red Hat Hybrid Cloud Console。

流程

1. 进入 Insights for Red Hat Enterprise Linux 应用程序的 Red Hat Enterprise Linux > Vulnerability > Reports 页面。
2. 在 **Report by CVEs** 卡上，点 **Create report**。
3. 根据需要在弹出卡中进行选择：



a. （可选）自定义报告标题。

b. 在 **按过滤 CVEs** 下，点每个过滤器下拉菜单并选择一个值。

c. 选择 **Tags** 来仅包含标记的系统组中的系统。

d. 在要包含的 CVE data 下，**选择列** 会被默认激活，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）添加备注来为预期使用者提供报告上下文。

4. 点 **Export report**，并允许应用程序一分钟来生成报告。

5. 如果您的操作系统要求，请选择打开或保存 PDF 文件，**然后单击确定**。

第 4 章 将漏洞数据导出为 JSON、CSV 或 PDF 文件

漏洞服务允许您在 RHEL 基础架构中为 CVE 导出数据。在漏洞服务中应用过滤器来查看特定的 CVE 或系统集合后，您可以根据这些标准导出数据。

这些报告可以通过 Red Hat Enterprise Linux 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的数据。

流程

1. 进入 Red Hat Enterprise Linux > 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**，或根据您的下载首选项 **导出为 PDF**。
4. 选择下载位置并点击 **Save**。

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每次安全问题影响安装时自动发送电子邮件消息，或者向每天进行的所有漏洞事件发送电子邮件摘要。使用通知服务可自由地检查 Red Hat Insights for RHEL 仪表板以了解事件触发的通知。

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 以了解事件数据
- 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，将事件通知路由到应用程序仪表板

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发送方法，以及通知是否发送到所有用户，还是只向机构管理员发送。

机构管理员创建一个带有 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，以便接收每个事件的独立电子邮件或每日事件摘要。

其他资源

- 有关如何为漏洞事件设置通知的更多信息，请参阅 Red Hat Insights 通知 。

第 6 章 参考资料

要了解更多有关漏洞服务或其他 Red Hat Enterprise Linux 服务和功能的 Red Hat Insights 的信息，可能还会考虑以下资源：

- *评估和监控 RHEL 系统上的安全漏洞*
- *使用漏洞服务和 Ansible Playbook 修复安全风险*
- Red Hat Insights for Red Hat Enterprise Linux 文档
- Red Hat Insights for Red Hat Enterprise Linux 产品支持页

对红帽文档提供反馈

我们感谢您对我们文档的反馈。要提供反馈，请突出显示文档中的文本并添加注释。

先决条件

- 已登陆到红帽客户门户网站。
- 在红帽客户门户网站中，文档采用 **Multi-page HTML** 查看格式。

流程

要提供反馈，请执行以下步骤：

1. 点击 **文档** 右上角的反馈按钮查看现有的反馈。

注意

反馈功能仅在多页 HTML 格式中启用。

2. 高亮标记您要提供反馈的文档中的部分。
3. 点在高亮文本旁弹出的 **Add Feedback**。
   文本框会出现在页面右侧的反馈部分中。
4. 在文本框中输入您的反馈，然后点 **Submit**。
   已创建一个文档问题。
5. 要查看问题，请点击反馈视图中的问题链接。