Red Hat Trusted Profile Analyzer 1

快速入门指南

在 Red Hat Hybrid Cloud Console 上使用 Red Hat Trusted Profile Analyzer 托管服务

Last Updated: 2024-06-11

Red Hat Trusted Profile Analyzer 1 快速入门指南

在 Red Hat Hybrid Cloud Console 上使用 Red Hat Trusted Profile Analyzer 托管服务

法律通告

摘要

此快速入门指南为用户提供了在 Red Hat Hybrid Cloud Console 上使用 Red Hat Trusted Profile Analyzer 托管服务的重要信息。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

前言

欢迎使用红帽的受信任的配置文件分析器(RHTPA)快速入门指南！这是有关如何在红帽混合云控制台上使用 RHTPA 管理的服务的快速指南。

第 1 章 搜索漏洞信息

您可以使用受信任的配置文件分析器服务查找现有软件 Bill of Materials (SBOM)、漏洞扩展性 eXchange (VEX)文档以及红帽产品和软件包的通用漏洞和暴露(CVE)信息。

重要

在这个技术预览版本中，Trusted Profile Analyzer 只提供以下红帽产品的信息：

- Red Hat Enterprise Linux Universal Base Image (UBI)版本 8 和 9。
- Java Quarkus 库。

先决条件

- 用于访问 Red Hat Hybrid Cloud Console 的红帽用户帐户。

流程

1. 打开 Web 浏览器。
2. 进入 Hybrid Cloud Console 上的 **Application and Data Services** 主页。
3. 如有提示，使用您的凭证登录到 Hybrid Cloud Console。
4. 在导航菜单中点 **Trusted Profile Analyzer**。
5. 在 Trusted Profile Analyzer 主页上，单击 **Subscribe and launch** 按钮。Trusted Profile Analyzer 控制台主页将打开一个新的 Web 浏览器窗口。

注意

通过订阅，注册的电子邮件地址将进入产品邮件列表中，因此您可以接收有关新产品开发的信息。

6. 在 **Home** 页面中，在搜索字段中输入您的搜索条件，然后点 **搜索**。
7. 在搜索结果页中，您可以过滤红帽产品的结果，下载 SBOM 文件，查看软件包漏洞信息，并查看任何可能的补救方法。

注意

Advisories 选项卡中显示的数量是您的搜索条件匹配的次数。在 **Products 和 containers** 选项卡中，**产品公告** 列中的数字显示该特定产品的公告数。

第 2 章 扫描资料文件的软件清单

您可以扫描自定义软件材料清单(SBOM)清单文件，以便红帽进行分析。

重要

红帽不会保留扫描的 SBOM 文件的副本。

先决条件

- 用于访问 Red Hat Hybrid Cloud Console 的红帽用户帐户。
- 现有的 CycloneDX 1.3 或软件软件包数据交换(SPDX) 2.2 清单文件。

流程

1. 打开 Web 浏览器。
2. 进入 Hybrid Cloud Console 上的 **Application and Data Services** 主页。
3. 如有提示，使用您的凭证登录到 Hybrid Cloud Console。
4. 在导航菜单中点 **Trusted Profile Analyzer**。
5. 在 Trusted Profile Analyzer 主页上，单击 **Subscribe and launch** 按钮。Trusted Profile Analyzer 控制台主页将打开一个新的 Web 浏览器窗口。

注意

通过订阅，注册的电子邮件地址将进入产品邮件列表中，以便您可以接收有关新产品开发的信息。

6. 从导航菜单中点 **Scan SBOM**。
7. 您可以将 SBOM 清单文件拖放到页面中，或者点击 **Load an SBOM**。
8. 扫描 SBOM 文件后，您可以获得 SBOM 文件中包含的软件包的分析概述和特定的漏洞信息。

其他资源

- 要了解如何创建材料文件软件清单，请参阅受信任的配置文件分析器 参考指南。

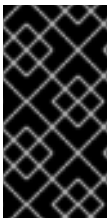
第 3 章 配置 VISUAL STUDIO CODE 以使用依赖分析

您可以使用 Microsoft 的 Visual Studio Code (VS Code)编辑器应用程序的依赖分析扩展，获取红帽受信任的配置文件分析器服务。通过这个扩展，您可以访问最新的开源漏洞信息，并深入了解应用程序依赖的软件包。Red Hat Dependency Analytics 扩展为可用的最新漏洞信息使用以下数据源：

- ONGuard 服务，集成 开源漏洞(OSV) 和 国家漏洞数据库(NVD) 数据源。当为 ONGuard 服务指定一组软件包时，对 OSV 的查询会检索相关的漏洞信息，然后查询 NVD 以了解公共漏洞和暴露(CVE)信息。

依赖项分析支持以下编程语言：

- Maven
- 节点
- Python
- Go



重要

默认情况下，Vis Studio Code 直接在系统 **PATH** 环境中的终端中执行二进制文件。您可以将 Visual Studio Code 配置为查找其他位置以运行必要的二进制文件。您可以通过访问 扩展设置 来配置。点 **Workspace** 选项卡，搜索单词 *executable*，并指定您要用于 Maven、Node、Python 或 Go 的二进制文件的绝对路径。

注意

Dependency Analytics 扩展是由红帽维护的在线服务。依赖项分析只访问清单文件，以便在显示结果前分析应用程序依赖项。

先决条件

- 在工作站上安装 Visual Studio Code。
- 对于 Maven 项目，分析 **pom.xml** 文件，您必须在系统的 **PATH** 环境中具有 **mvn** 二进制文件。
- 对于 Node 项目，分析 **package.json** 文件，您必须在系统的 **PATH** 环境中具有 **npm** 二进制文件。
- 对于 Go 项目，分析 **go.mod** 文件，您必须在系统的 **PATH** 环境中具有 **go** 二进制文件。
- 对于 Python 项目，分析 **requirements.txt** 文件，您必须在系统的 **PATH** 环境中具有 **python3/pip3** 或 **python/pip** 二进制文件。此外，Python 应用需要位于 VS Code 的解释器路径中。

流程

1. 打开 Visual Studio Code 应用。
2. 从文件菜单中，单击 **View**，然后单击 **Extensions**。
3. 搜索 **Marketplace** for *Red Hat Dependency Analytics*。
4. 点 **Install** 按钮安装扩展。等待安装完成。

5. 要启动扫描应用程序以了解安全漏洞，并查看漏洞报告，您可以执行以下操作之一：

    - 打开清单文件，将鼠标悬停在由内联组件分析标记的依赖项上，在依赖项名称下由 wavy-red 行指示，点 **Quick Fix**，然后点 Detailsed **Vulnerability Report**。
    - 打开清单文件，然后点 **pie chart** 图标。
    - 在 **Explorer** 视图中点清单文件右键，点 **Red Hat Dependency Analytics Report...**。
    - 在漏洞弹出警报消息中，点 **Open detailed vulnerability report**。

其他资源

- 红帽依赖分析 Visual Studio 市场 页面.
- GitHub 项目.

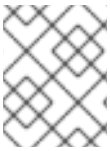
第 4 章 将 INTELLIJ 配置为使用依赖分析

您可以使用 Jet Brains 的 IntelliJ IDEA 应用程序的依赖分析插件获取红帽受信任的配置文件分析器服务的访问权限。使用这个插件，您可以访问最新的安全漏洞信息，并深入了解应用程序依赖的软件包。Red Hat Dependency Analytics 插件为可用的最新漏洞信息使用以下数据源：

- ONGuard 服务，集成 开源漏洞(OSV) 和 国家漏洞数据库(NVD) 数据源。当为 ONGuard 服务指定一组软件包时，对 OSV 的查询会检索相关的漏洞信息，然后查询 NVD 以了解公共漏洞和暴露(CVE)信息。

依赖项分析支持以下编程语言：

- Maven
- 节点
- Python
- Go



注意

Dependency Analytics 扩展是由红帽维护的在线服务。依赖项分析只访问清单文件，以便在显示结果前分析应用程序依赖项。

先决条件

- 在您的工作站上安装 IntelliJ IDEA。
- 对于 Maven 项目，分析 **pom.xml** 文件，您必须在系统的 **PATH** 环境中具有 **mvn** 二进制文件。
- 对于 Node 项目，分析 **package.json** 文件，您必须在系统的 **PATH** 环境中具有 **npm** 二进制文件。
- 对于 Go 项目，分析 **go.mod** 文件，您必须在系统的 **PATH** 环境中具有 **go** 二进制文件。
- 对于 Python 项目，分析 **requirements.txt** 文件，您必须在系统的 **PATH** 环境中具有 **python3/pip3** 或 **python/pip** 二进制文件。

流程

1. 打开 IntelliJ 应用程序。
2. 在文件菜单中，单击 **Settings**，然后单击 **Plugins**。
3. 搜索 **Marketplace** for *Red Hat Dependency Analytics*。
4. 单击 **INSTALL** 按钮，以安装插件。
5. 要启动扫描应用程序以了解安全漏洞，并查看漏洞报告，您可以执行以下操作之一：
   - 打开清单文件，将鼠标悬停在由内联组件分析标记的依赖项上，由依赖项下的 wavy-red 行指示，然后单击 **详细漏洞报告**。
   - 在项目窗口中单击清单文件右键，然后单击 **依赖分析报告**。

其他资源

- 红帽的依赖分析 Jet Brains 市场 页面.
- GitHub 项目.