Red Hat Trusted Profile Analyzer 1

参考指南

Red Hat Trusted Profile Analyzer 的其他参考信息

Last Updated: 2024-06-11

Red Hat Trusted Profile Analyzer 1 参考指南

Red Hat Trusted Profile Analyzer 的其他参考信息

法律通告

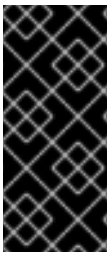
摘要

本参考指南为用户提供有关红帽受信任的配置文件分析器服务的附加信息。 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

欢迎使用红帽受信任的配置文件分析器参考指南！



重要

Red Hat Trusted Profile Analyzer 是一个技术预览版本。服务预览版本有早期开发中的功能。

要提供反馈或告知我们的工程团队与受信任的配置文件分析器相关的技术问题，请发送电子邮件至 rhtc-support@redhat.com。

第 1 章 常见问题解答

您是否对受信任的配置文件分析器有疑问？以下是一系列常见问题及其答案，可帮助您了解更多有关红帽的受信任的配置文件分析器服务的信息。

问： 红帽的受信任的配置文件分析器服务是什么？

答： 红帽的受信任的配置文件分析器服务是一个主动服务，可帮助您评估在应用程序堆栈中使用开源软件(OSS)软件包和依赖项的安全性和漏洞风险。

问： 如何使用红帽的受信任的配置文件分析器服务？

答： 您可以通过两种方式使用红帽的受信任的配置文件分析器服务。首先，通过将依赖分析扩展用于集成开发环境(IDE)平台，如 Microsoft 的 Visual Studio Code 或 Jet Brains 的 IntelliJ IDEA。使用依赖分析可在编写应用程序时为您提供对漏洞的在线指导。其次，通过搜索 红帽混合云控制台 上的红帽产品的软件 Bill of Materials (SBOM)和漏洞扩展 eXchange (VEX)信息。

问： 受信任的配置文件分析器服务将提供什么类型的内容？

答： 您可以访问 Java、NodeJS、Python、Go 和 Red Hat Enterprise Linux 软件包的应用程序库。有关开源软件包的漏洞信息直接来自红帽内部资源、红帽的生态系统，如 Snyk 和开源社区数据源。

问： Trusted Profile Analyzer Service Preview 发行版将提供什么内容？

答： 以下内容将可用于服务预览：

Quarkus Java Framework for Java Archive (JAR)文件与关联的 SBOM 文件。

Red Hat Enterprise Linux Universal Base Image (UBI)版本 8 和 9 以及关联的 SBOM 文件。

有关开源 Java 软件包的漏洞信息。

问： Trusted Profile Analyzer SBOM 如何帮助我？

答： 受信任的配置文件分析器软件 Bill of Materials (SBOM)可以帮助您了解应用程序堆栈中的软件组件，以及这些软件组件可以获得的任何相关漏洞。SBOM 通过组件的成熟、许可证信息以及测试其构建方式，提高软件供应链中开源代码的可见性和透明度。

问： 谁正在使用红帽的受信任的配置文件分析器服务？

答： 红帽受信任的配置文件分析器服务的主要受众是 Quarkus Java 开发人员，云原生容器镜像构建器则使用 Red Hat Enterprise Linux UBI。

问： 要使用红帽的受信任的配置文件分析器服务，我需要了解任何新的配置文件，或更改我的开发工作流和流程？

答： No.

问： **我不是 Quarkus Java 开发人员，我仍然可以从红帽的受信任的配置文件分析器服务中获取任何价值？**

答： 是。Trusted Profile Analyzer 服务仍提供有关当前未包含在受信任的配置文件分析器存储库中的开源软件包的安全风险信息。

第 2 章 术语表

红帽受信任的配置文件分析器服务的常见术语和定义。

Exhort

Trusted Profile Analyzer （包括所有 API 请求被发送）的后端端点，以检索要分析所需的数据，包括软件包依赖项和漏洞。红帽依赖分析(RHDA)集成开发环境(IDE)插件使用此端点在 IDE 框架内生成漏洞报告。

软件 Bill of Materials

也称为 cronym、SBOM。特定应用所需的依赖软件包的清单。

单一 Glas 的 Panes

也称为 SPOG 的缩写。Trusted Profile Analyzer Web 仪表板和通知的 RESTful 应用程序编程接口(API)。

漏洞利用 eXchange

也称为 cronym, VEX。由软件供应商为产品内特定漏洞发布的安全公告。

常见漏洞暴露

也称为缩写(cronym) CVE。CVE 表示通过给出一个分数 1-10 影响产品的攻击和恶意活动的风险，其中 1 是最低风险级别，10 是最高风险级别。

通用漏洞分数系统

也称为缩写 CVSS。当试图计算各种产品和网络中的 CVE 时，CVSS 根据特定公式计算 CVE 分数。

第 3 章 创建资料清单文件的软件清单

Red Hat Trusted Profile Analyzer 可以使用 JSON 文件格式分析 CycloneDX 和软件软件包数据交换 (SPDX) SBOM 格式。许多开源工具可用于从容器镜像或您的应用程序创建软件 Bill of Materials (SBOM) 清单文件。对于此过程，我们将使用 Syft 工具。

重要

目前，Trusted Profile Analyzer 只支持 CycloneDX 版本 1.3 和 SPDX 版本 2.2。

先决条件

- 为您的工作站平台安装 Syft ：
  - Red Hat Ecosystem Catalog
  - GitHub

流程

1. 使用容器镜像创建 SBOM。
   CycloneDX 格式：

   语法

   ```
   syft IMAGE_PATH -o cyclonedx-json
   ```

   Example

   ```
   $ syft registry:example.io/hello-world:latest -o cyclonedx-json
   ```

   SPDX 格式：

   语法

   ```
   syft IMAGE_PATH -o spdx-json
   ```

   Example

   ```
   $ syft registry:example.io/hello-world:latest -o spdx-json
   ```

   注意

   Syft 支持许多类型的容器镜像源。请参阅 Syft 的 GitHub 站点上的官方支持的源列表。

2. 通过扫描本地文件系统来创建 SBOM。
   CycloneDX 格式：

   语法

```
syft dir: DIRECTORY_PATH -o cyclonedx-json
syft file: FILE_PATH -o cyclonedx-json
```

Example

```
$ syft dir:. -o cyclonedx-json
$ syft file:/example-binary -o cyclonedx-json
```

SPDX 格式：

语法

```
syft dir: DIRECTORY_PATH -o spdx-json
syft file: FILE_PATH -o spdx-json
```

示例

```
$ syft dir:. -o spdx-json
$ syft file:/example-binary -o spdx-json
```

其他资源

- 使用红帽受信任的配置文件分析器托管服务扫描 SBOM 清单文件。
- 国家电信和信息管理(NTIA) 如何生成 SBOM 的指南。