

# 嵌入式安全审计平台 常见问题



腾讯云

**【 版权声明 】**

©2013–2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

**【 商标声明 】**

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

**【 服务声明 】**

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

**【 联系我们 】**

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

# 常见问题

最近更新时间：2024-05-15 17:19:32

## 嵌入式安全审计平台的扫描对象是什么？

嵌入式安全审计平台的漏洞扫描对象为产品编译后的二进制软件包或固件：Linux 安装包、Windows 安装包、Web 部署包、安卓应用、嵌入式固件等。

## collector 是什么？其运行环境是什么？

- collector 是对目标系统的采集器，运行在本地，以无侵入的方式远程连接目标系统。
- collector 是一个可执行的二进制文件，需要使用简单命令行开启自动化检测。
- collector 运行的本地系统需为x86-64架构，对远程目标系统没有架构要求。

## 二进制 SCA 与源代码 SCA 有什么不同？

DevSecOps 中，二进制和源代码 SCA 作用互补。

- 二进制 SCA 检测对象为二进制构建产物，无需源码。
- 二进制 SCA 和源代码 SCA 检测阶段不同，源代码 SCA 在开发阶段检测，二进制 SCA 在测试阶段检测。
- 二者通常在语言支持上互补，嵌入式固件安全扫描对 C++、C、Java、Golang 等语言良好支持。
- 二者通常在检测结果上互补，嵌入式固件安全扫描可补充检测源代码规范格式外的开源软件和在构建过程中引入的开源软件。

## APK/Java SCA 分析区别是什么？

APK 与 Java jar 包由于平台，场景，编译条件不同，分析的技术路线与难点都是不一样的。

(1) 对于后台开发的 Jar 包等制品可以支持如下分析：

- native 可执行文件分析。
- jar 包编译后成分分析，主要来源是 maven 等常见开发源。

(2) 对于 APK 可以做如下分析：

- APK 本身安全问题分析。
- native 可执行文件分析。
- APK 使用的第三方 SDK 分析，主要来源是主流的 APK 开发所需要的 SDK，如地图 SDK 等。

## 如何理解符号匹配和二进制匹配模式？

符号匹配和二进制匹配通常针对内核 CVE 的匹配规则。二进制匹配和符号匹配不是单独分开的功能点。符号匹配是指在提取到内核文件的符号信息之后，将其与各个 CVE 的问题符号做对比，判断漏洞涉及的特征符号是否在当前被扫描文件中。

而二进制匹配模式功能上属于符号匹配的超集，除了基本的问题符号匹配功能以外，还能够基于专家经验总结的各种二进制规则对当前文件的数据流、控制流等静态信息与漏洞的对应信息做匹配，即二次判断当前内核文件是否有

---

相应漏洞问题，提升内核漏洞扫描的准确率。