嵌入式安全审计平台

产品简介

腾讯云

【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。

文档目录

产品简介

产品概述

最近更新时间：2024-05-15 17:19:31

什么是嵌入式安全审计平台

嵌入式安全审计平台（Embedded System Security Audit Studio）是一款聚焦于嵌入式系统软件成分分析和基线检查的平台。支持系统级基线审计、漏洞扫描、开源许可证审计、攻击链捕获、敏感信息等安全威胁检测，旨在为用户提供威胁处理平台，打造安全竞争能力。

产品功能

二进制文件解析

嵌入式固件安全扫描，良好支持自动化解析各类二进制构建产物。

支持 CPU 架构

x86/x64	ARM/ARM64	MIPS	PowerPC
ARM7、9、11	SuperH	TriCore	其他

支持操作系统

Linux	Android	Windows	QNX	MacOS
Proprietary	RTOS	NetBSD	FreeBSD	其他

支持文件格式

类型	文件格式
安装包格式	Redhat RPM (.rpm)、Debian package (.deb)、Mac installers (.dmg, .pkg)、Windows installers 7z, zip, rar self extracting .exe、Windows installers MSI Installer、Windows installers CAB Installer等
文件系统/磁盘镜像	支持 ext2、ext4、squashfs、vfat、ubifs、ubi、romfs、sparse (simg2img) 等文件系统，gpt、dos、PMBR、mac 等多种分区，vhd Windows 磁盘镜像
压缩文件格式	gzip(.gz)、bzip2(.bz2)、lzma(.lz)、lz4(.lz4)、compress(.Z)、xz(.xz)、pack200(.jar)、upx(.exe)、Zip(.zip, .jar, .apk and a number of others

	derivates)、Xar (.xar)、zip (.7z)、ARJ (.arj)、ar (.tar)、VM Tar (.tar)、cpio (.cpio)、RAR (.rar)、LZH (.lzh)
编程语言/编程类型	支持以下不同编程语言、不同编译器及编译选项、不同平台架构、不同 OS 系统的二进制软件包的检测： • C/C++、Java/Kotlin、ArkTS、Go、Rust 等二进制软件包 • GCC、VisualStudio、Clang、intel C++编译器及不同编译优化选项、不同安全编译选项生成的二进制软件包 • x86、arm、mips、ppc、risc-v 的32位或64位 CPU 指令的二进制软件包 • Windows 的 PE 格式(.dll/.exe/.ocx/.sys/.com/.lib/.obj) • Linux 的 elf 格式(.so/.exe/.o/.a) • 内核 images 格式 • 跨平台语言 Java(.jar/.apk/.aar)的二进制软件包
固件格式	支持以下不同固件格式的检测：Intel HEX、SREC、uBoot、Juniper firmwares、cramfs、fit（flattened image tree）、jffs2、Android OTA、dmg (macos .dmg)、uImage/zImage、android boot image 等
其他未知格式	可以采用遍历穷举方式识别出可识别的数据片段，进行部分解包还原（具体以产品实际可识别格式范围为准）
源码 SCA-分析能力	• 支持通过锁文件分析、文件 hash 分析、代码片段分析等技术手段识别以下各类第三方组件 • 支持十种以上依赖包管理器如：Maven、Npm、Yarn、Pnpm、GoMod、Nuget、Cargo、RubyGems、Bundler、Composer、CocoaPods、Poetry、Pip、Setuptools、Conan、Hex、Conda、Dart、Gradle • 能够识别主流开发语言的开源组件识别，包括：C/C++、Java、ArkTS、Kotlin、JavaScript、TypeScript、Python、Go、C#、Ruby、PHP、Swift、Rust、Pub

产品优势

最近更新时间：2024-05-15 17:19:31

已知漏洞检测

嵌入式固件安全扫描，支持公开漏洞检测，并提供漏洞暴露位置、漏洞详细信息、解决建议等实用信息。

开源软件检测

嵌入式固件安全扫描，支持检测构建产物使用的开源软件，并提供软件需遵循的开源协议详细信息和声明要求，协助合规性检查。

敏感信息检测

支持检测文件敏感信息，定位敏感信息位置，减少信息泄漏及被非法利用的风险。

二进制分析

具备二进制 SCA 能力，与依赖扫描结合，分析二进制制品安全问题。

漏洞扫描

腾讯安全专家持续维护追踪漏洞，使用数据流、控制流、污点分析等技术，从常见攻击面出发，提炼漏洞的二进制特征，使得版本匹配更精准，漏洞匹配更准确。

内核漏洞概率输出

支持多种规则 CVE 漏洞检测，通过安全专家经验，给出漏洞规则匹配概率，提升内核漏洞判断准确性，降低漏洞核实成本。

丰富强大的开源协议库

覆盖市面常见各类开源组件，支持针对开源软件的许可证信息、许可证冲突、许可证风险、版权信息、敏感信息泄露、安全配置等各类安全问题检测，协助合规性检查。

敏感成分分析

支持密钥敏感信息、设备敏感信息、商业敏感数据、通用敏感信息检查，输出详细敏感信息成分，定位信息泄漏位置。

文件格式支持

支持20+文件格式，包括常见固件、镜像、文件系统、压缩文件等。支持 Linux、Android、QNX 等常见系统，支持 x86/x64、MIPS、ARM/ARM64、PowerPC 等主流 CPU 架构。

报告易读

支持一键上传固件包、软件包等文件，即可分析，获取完整安全成分分析报告。

应用场景

最近更新时间：2024-05-15 17:19:31

风险识别

识别使用的开源软件信息，有助于遵守许可证协议；展示文件包含的相关开源敏感信息，避免敏感信息泄露。

物联网安全

为智能家居、工控设备、医疗设备、智能穿戴、出行交通等行业的设备制造商、应用开发商，提供自动化软件安全成分分析。

供应链安全

利用二进制 SCA 分析，将不同供应商的系统、自研应用集成之后进行统一的系统安全测试，识别第三方库的开源许可证信息，有助于发布包遵守许可证协议；展示文件包含的敏感信息，避免敏感信息泄露。

持续集成/持续部署

持续集成/持续部署(CI/CD)融入软件生命周期（SDLC）管理，在安全开发流程，实现安全左移。在发布前对发布包进行安全检测，检查软件发布合规性与安全性，降低安全风险。

汽车行业信息安全法规监管

适配汽车行业的《车载信息交互系统信息安全技术要求》、《汽车网关信息安全技术要求及试验方法》、UN_Regulation_No.155，156等标准中安全检测相关要求。