开源治理服务

最佳实践

文档版本 01

发布日期 2025-01-23

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 CodeArts Governance 最佳实践汇总.....1
2 使用 CodeArts Governance 进行二进制成分分析.....2

1 CodeArts Governance 最佳实践汇总

本文汇总了基于开源治理服务（CodeArts Governance）常见应用场景的操作实践，为每个实践提供详细的方案描述和操作指导，帮助用户了解CodeArts Governance的使用方法。

表 1-1 CodeArts Governance 最佳实践一览表

最佳实践	说明
使用CodeArts Governance进行二进制成分分析	本实践为您介绍如何使用CodeArts Governance进行二进制成分分析。

2 使用 CodeArts Governance 进行二进制成分分析

应用场景

据《2024年中国软件行业全景图谱》统计，2023年国内软件市场规模超12万亿，我国软件行业正处于成长期，市场规模增长较快，预计2029年整体行业的市场规模将超21万亿。据《2023年软件供应链状况报告》指出，过去三年针对软件供应链的攻击平均年增长高达742%。因此，开源/第三方软件引入评估面临以下问题：

- 针对采购的软件或对外交付的软件产品没有很好的安全检测手段。
- 产品需要对供应商有基础的安全性认证。
- 开源漏洞响应与修复效率低，安全风险缺乏管理。

通过二进制成分分析服务提供页面和开放API，提供风险快速评估能力。功能特性如下：

- 全方位风险检测：对软件包/固件进行全面分析，基于各类检测规则，检测相关被测对象的开源软件漏洞和许可证合规、敏感信息（弱口令、硬编码密码等）、安全配置、安全编译选项等存在的潜在风险。
- 支持各类应用：支持对桌面应用（Windows和Linux）、移动应用程序（APK、IPA、Hap等）、嵌入式系统固件等的检测。
- 专业分析指导：提供全面、直观的风险汇总信息，并针对不同的扫描告警提供专业的解决方案和修复建议。
- 恶意代码检查：提供病毒木马等恶意软件的扫描，支持开源软件中敏感信息外发、木马下载执行、反弹shell、恶意命令执行恶意行为检测。

方案架构

以下示意图为用户申请开源/第三方软件场景，该软件包含制品包，将制品包提供给二进制成分分析服务进行检测，检测项包括：已知漏洞、安全编译选项、信息泄露、安全配置、恶意代码/软件等风险项，并输出风险评估报告，待风险项完成整改后进行使用。

方案优势

- 无源码、无侵入快速检测
  只需要上传产品发布包或固件，无需构建运行环境或运行程序。
- 多语言、多文件格式、多架构平台
  支持多语言，多构建场景下的制品检测，场景覆盖不遗漏。
- 恶意代码检测，确保供应安全
  基于AI开源软件恶意代码检测能力，恶意行为早发现。
- 敏感信息检测防泄露
  支持安全配置和密码密钥等敏感信息检测，发现潜在的安全风险。

约束与限制

表 2-1 二进制成分分析使用限制说明

指标类别	指标项	限制说明
任务管理	语言类型	支持C/C++/Java/Go/JavaScript/Python/Rust/Swift/C#/PHP等语言开源软件已知漏洞检测。
	扫描包格式	支持上传的文件格式有.7z、.arj、.cpio、.phar、.rar、.tar、.xar、.zip、.jar、.apk、.war等，以及支持上传Android OTA Images、Android sparse、Intel HEX、RockChip、U-Boot等固件。
	扫描包上传大小限制	5GB。

实施步骤

步骤1 登录开源治理服务控制台。

步骤2 在左侧导航栏，单击“软件成分分析 > 二进制成分分析”。

步骤3 在“二进制成分分析”页面，单击“添加任务”，弹出“添加任务”对话框，单击“扫描对象”旁的文件框，选择本地的软件包，导入扫描对象。

步骤4 文件上传成功后，单击“确定”，等待扫描任务完成。

步骤5 单击任务名称，也可以单击任务列表操作列的“查看报告”，进入扫描报告页面。扫描报告页面说明如表2-2所示。

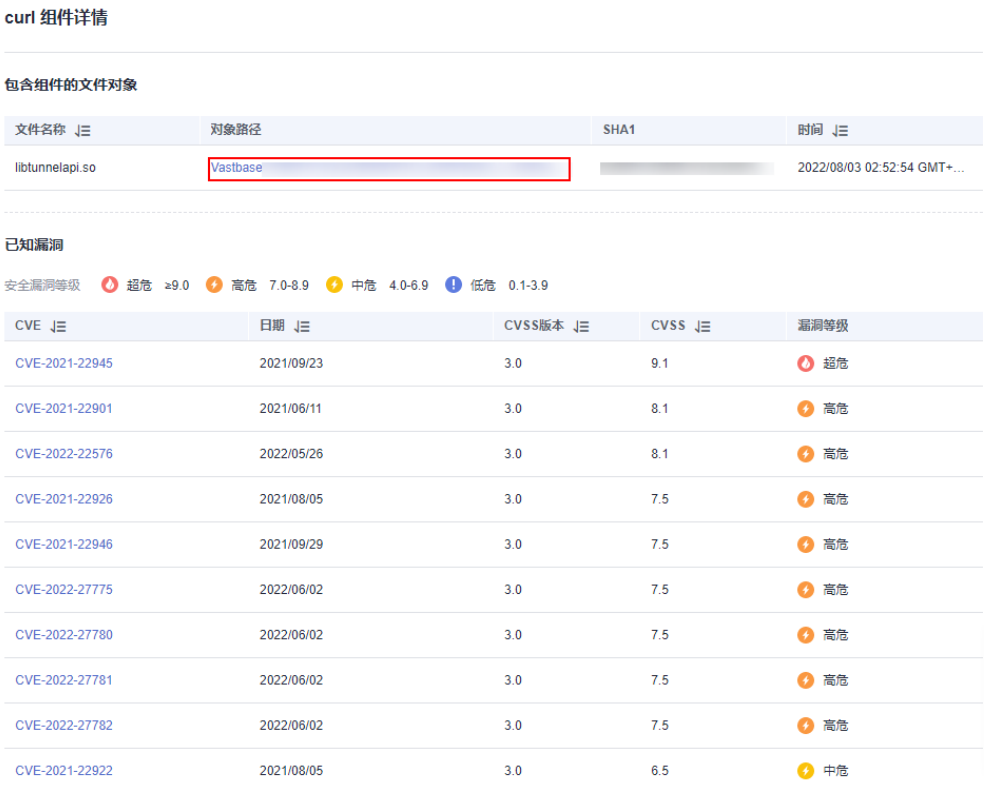
表 2-2 详情总览说明

栏目	说明
任务概况	• 显示目标任务的基本信息，包括：文件名、文件大小、特征库版本、平台版本等基本信息。 • 显示目标任务的组件检测、安全漏洞、安全配置、开源许可证、信息泄露、安全编译选项、恶意软件扫描检测概况，包括： – 组件检测：展示被扫描的软件包所有的组件数量，有漏洞、未知版本和无漏洞组件数量占比。 – 安全漏洞：展示超危、高危、中危、低危各个级别漏洞数量占比。 – 安全配置：展示通过、失败、不涉及的检测结果数量占比。 – 开源许可证：展示高风险、中风险、低风险各个级别开源许可证的统计信息。 – 密钥和信息泄露：展示信息泄露各检测项结果分布。 – 安全编译选项：展示安全编译各检测项结果分布。 – 恶意软件扫描：展示病毒和恶意代码扫描结果分布。
开源软件漏洞	显示扫描任务中每个组件的组件名称、组件版本、开源许可证、包含文件数以及存在漏洞数。 • 组件名称、组件版本和文件数可按升降序查看。 • 可按组件名称、开源许可证对组件列表进行筛选查看。
开源许可证	显示开源软件的许可证检测结果，包括许可证使用的集成风险和许可证间的兼容性风险。 • 许可证信息：二进制文件包许可证检测结果，包含许可证名称、集成风险、涉及组件和许可证描述和风险分析。 • 许可证兼容性：二进制文件包中各目录的许可证间兼容性风险检测。
密钥和信息泄露	显示Git地址、IP、硬编码密码、弱口令、硬编码密钥和SVN地址的检测结果。

栏目	说明
安全编译选项	显示BIND_NOW、NX、PIC等检测项目的描述、检测结果、不符合文件数。
安全配置	显示凭据管理、认证问题和会话管理的检测项目、安全风险等级、检测结果。
恶意软件扫描	显示病毒扫描和恶意代码扫描的结果。

- 在“开源软件漏洞”页签可查看软件包各个组件的漏洞。
  如果检测结果存在漏洞或者风险，可单击“组件名称”列，查看详细信息。
- 单击“对象路径”，可以查看文件对象路径详细信息。
- 单击“CVE”漏洞名称可以查看相应漏洞的“漏洞详情”、“漏洞简介”、“解决方案”、“漏洞修复参考”、“参考链接”。

图 2-1 开源软件漏洞检测结果



- 在“密钥和信息泄露”页签查看对应检测项目的检测结果。

图 2-2 密钥和信息泄露检测结果

检测项目	检测结果
Git地址	0
IP	0
硬编码密码	24
弱口令	0
硬编码密钥	0
SVN地址	0

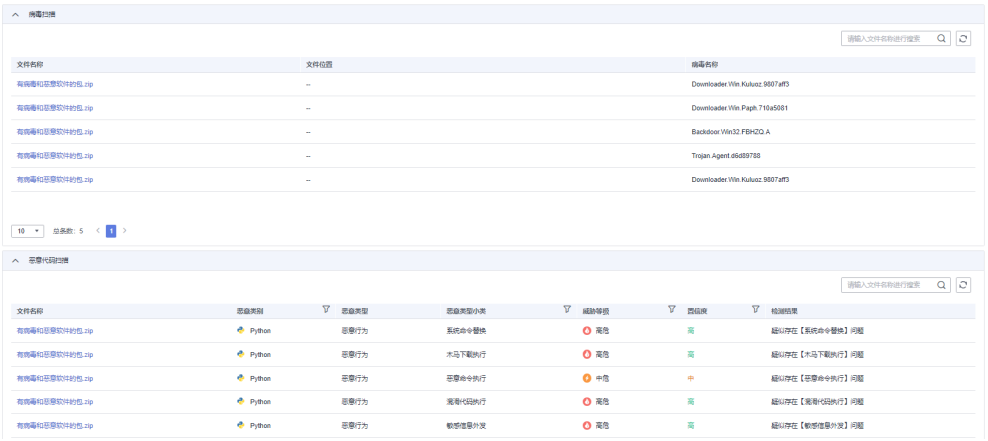
- 在“安全编译选项”页签查看编译选项对应检测项目的检测结果。

图 2-3 安全编译选项检测结果

检测项目	描述	检测结果	不符合文件数（个）
BIND_NOW	立即绑定	91.18%	3
NX	堆栈不可执行	100.00%	0
PIC	地址无关	70.97%	9
PIE	随机化	100.00%	0
RELRO	GOT表保护	91.18%	3
SP	栈保护	76.47%	8
NO Rpath/Runpath	动态库搜索路径（禁选）	100.00%	0
FS	Fortify Source	0.00%	34
Ftrapv	整数溢出检查	N/A	0
Strip	删除符号表	100.00%	0

- 在“恶意软件扫描”页签查看病毒扫描和恶意代码扫描的检测结果。

图 2-4 病毒扫描和恶意代码扫描的检测结果



----结束

