# 开源治理服务

# 用户指南

**文档版本** 01

**发布日期** 2025-08-04

**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 登录开源治理服务控制台

**步骤1** 登录华为云官网，单击页面右上角“控制台”。

**步骤2** 在页面左上角单击，打开服务列表。

**步骤3** 搜索“开源治理服务”。

**步骤4** 单击“开源治理服务 CodeArts Governance”，进入开源治理服务控制台。

**----结束**

# 2 软件成分分析总览

软件成分分析总览页主要展示：资产信息和最近一次检测情况。

- 我的资产

  展示最近30天被扫描的软件包个数，以及有风险和未完成的软件包个数。
- 风险信息 TOP5

  展示前五项组件风险信息，可查看组件名称、组件版本、语言类型、版本时间、漏洞数、超高危漏洞数、集成风险和引用数量。
- 最近一次二进制成分分析扫描

  展示最近一次扫描详细情况，参数说明如表2-1所示。

**表 2-1** 二进制成分分析扫描参数说明

| 参数 | 说明 |
| --- | --- |
| 扫描对象 | 被扫描的软件包/固件，单击可进入本次任务的扫描详情。 |
| 文件大小 | 被扫描的文件的大小。 |
| 开始时间 | 开始扫描的时间。 |
| 扫描耗时 | 扫描耗费的时长。 |
| 任务状态 | 任务扫描状态，包括：等待中、进行中、已完成、已停止、已失败。 |
| 检测结果风险统计 | 显示各检查项的检测项目风险文件总数。 |
| 安全漏洞风险项 | 显示不同风险等级的漏洞个数，风险等级包括：超危、高危、中危、低危。 |
| 检测项目合规统计 | 显示检测项目的合规占比（合规项/总检查项）。 |
| 开源许可证 TOP6 | 显示数量排名前六的开源软件使用许可。 |
| 恶意软件扫描 | 显示各检查项的病毒扫描和恶意代码扫描风险总数。 |

# 3 开源许可证

## 操作场景

用户可以查看开源许可证的信息和自定义开源许可证的风险等级。

## 前提条件

已获取管理控制台的登录账号与密码。

## 操作步骤

**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 > 开源许可证”。

**步骤3** 在“开源许可证”页面，可看到许可证列表，内容包含许可证名称、集成风险、许可证描述和风险分析以及重置操作。

**图 3-1** 开源许可证


- 单击许可证的风险等级下拉框可以自定义对应许可证的风险等级。
- 单击许可证操作栏的“重置”可以恢复对应许可证的默认风险等级。
- 单击“全部重置”可以批量重置所有风险项。

**----结束**

# 4 源码成分分析

## 4.1 添加源码成分分析任务

提供对源码的全面分析功能，通过解压获取源码包中所有待分析源码文件，基于源码特征识别技术，获得相关被测对象的开源软件清单和潜在风险清单，并输出一份专业的分析报告。

用户只需要上传代码文件或关联代码仓库提交扫描任务，服务即可输出详尽专业的测试报告。

### 前提条件

- 已获取管理控制台的登录账号与密码。
- 已准备好待扫描的源码包。

### 操作步骤

**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 > 源码成分分析”。

**步骤3** 在“源码成分分析”页面，单击“添加任务”，弹出“添加任务”对话框，依照表4-1设置参数。

**表 4-1** 添加源码扫描任务参数说明

| 参数 | 参数说明 |
| --- | --- |
| 任务名称 | 源码成分分析任务的名称。 |
| 扫描类型 | 待扫描的源码类型，包括文件和代码仓，根据实际情况选择扫描文件或代码仓。 |

| 参数 | 参数说明 |
| --- | --- |
| 扫描对象 | • 文件扫描任务的扫描对象：待扫描的源码文件。<br>源码文件限制如下：<br>– 支持.zip、.tar.gz格式的文件。<br>– 文件大小不能超过1G。<br>– 解压后文件总大小不超过10G。<br>– 解压后文件个数不超过10万个。<br>– 单个源文件超过10M不扫描。<br>– 文件名最大长度为100字符。<br>– 任务描述最大长度为200字符。<br>• 代码仓扫描任务的扫描对象：待扫描的代码仓地址，当前只支持SSH地址。 |
| 标识类型 | 仅代码仓扫描任务涉及此参数。<br>选择待扫描的标识类型，包括代码仓分支和代码仓tag。 |
| 标识名称 | 仅代码仓扫描任务涉及此参数。<br>待扫描的分支或tag的名称。 |
| 任务描述 | 对当前源码成分分析任务的说明。 |

**步骤4** 单击“确定”，开始扫描。

**----结束**

# 4.2 管理源码成分分析任务

## 操作场景

该任务指导用户通过开源治理服务查找、删除或停止源码成分分析任务。

## 前提条件

- 已获取管理控制台的登录账号与密码。
- 已添加任务。

## 查看任务

**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 > 源码成分分析”。

**步骤3** 在“源码成分分析”页面，查看成分分析任务列表，相关参数说明如**表4-2**所示。

**表 4-2** 源码成分分析任务列表参数说明

| 参数 | 参数说明 |
| --- | --- |
| 任务名称 | 源码成分分析任务的名称。 |
| 扫描对象 | 被扫描的对象，包含文件和代码仓。 |
| 任务状态 | • “等待中”<br>导入扫描对象后开始等待扫描。<br>• “进行中”<br>任务正在进行扫描。<br>• “已完成”<br>任务已完成扫描。<br>• “已停止”<br>任务扫描中单击了操作栏的“停止”。<br>• “已失败”<br>任务扫描失败。 |
| 安全漏洞 | 成分分析扫描出的漏洞分布情况。 |
| 开始时间 | 成分分析开始的时间。 |
| 任务时长 | 成分分析扫描完成、失败或停止的所用时长。 |
| 操作 | 查看报告、停止、删除按钮。 |

**步骤4** 在下拉框 

下拉选择任务状态，可根据任务状态筛选查看任务。

**步骤5** 在输入框 

中输入任务名称关键字，可根据任务名称关键字筛选查看，可以和任务状态联合使用。

**步骤6** 单击  刷新任务列表。

**----结束**

## 删除任务

**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“源码成分分析”。

**步骤3** 在“源码成分分析”页面，可看到全部添加过的任务。

**步骤4** 单击待删除任务后操作列的“删除”。

根据系统提示执行删除操作。

**----结束**

## 停止任务

只有任务状态为进行中、等待中才可操作停止任务。

**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“源码成分分析”。

**步骤3** 在“源码成分分析”页面，可看到全部添加过的任务。

**步骤4** 单击待停止任务后操作栏的“停止”，在弹出的对话框中单击“确认”。

**----结束**

# 4.3 查看源码成分分析扫描详情

该任务指导用户通过开源治理服务查看源码成分分析扫描结果。

## 前提条件

- 已获取管理控制台的登录账号与密码。
- 已执行扫描任务。

## 操作步骤

**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 > 源码成分分析”。

**步骤3** 在“源码成分分析”页面，可看到全部添加过的任务。单击对应任务的任务名称，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4-3所示。

**表 4-3** 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：任务名称、扫描类型、文件大小、特征库版本、任务描述等基本信息。<br>• 显示目标任务的组件检测、安全漏洞、开源许可证检测概况，包括：<br>– 组件检测：展示被扫描的软件包中所有的组件数量，有漏洞和无漏洞组件的数量。<br>– 安全漏洞：展示超危、高危、中危、低危各个级别安全漏洞的数量。<br>– 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。 |

| 栏目 | 说明 |
| --- | --- |
| 软件详情 | 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。<br>● 组件名称和文件数可按升降序查看。<br>● 可按开源许可证对组件列表进行筛选查看。<br>● 单击组件名称进入组件详情页面，显示该组件包含的文件对象和已知漏洞信息。 |
| 开源许可证 | 显示开源软件的许可证检测结果，包括许可证使用的风险等级和许可证间的兼容性风险。<br>● 许可证信息：源码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。<br>● 许可证兼容性：源码文件包中各目录的许可证间兼容性风险检测。 |

**----结束**

# 5 二进制成分分析

## 5.1 添加二进制成分分析任务

提供软件包/固件全面分析功能，基于各类检测规则，获得相关被测对象的开源软件、信息泄露、安全配置、安全编译选项等存在的潜在风险。

用户只需上传产品软件包或固件文件提交扫描任务，服务即可输出详尽专业的测试报告。

### 前提条件

- 已获取管理控制台的登录账号与密码。
- 本地已准备好待扫描的二进制软件包。

### 约束与限制

- 支持检测 .zip、.rar、.tar、.tar.gz、.jar、.apk、.hap、.so、.gz、.gzip等10+种格式的文件。
- 文件名只能包含：中文、字母、数字、空格、下划线（ _ ）、中划线（ - ）或点（ . ）。
- 文件名最大长度为100字符。
- 任务描述最大长度为200字符。
- 文件大小不能超过5GB（ 免费试用任务限制300MB ）。

### 操作步骤

**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。

**表 5-1** 参数说明

| 参数 | 参数说明 |
| --- | --- |
| 扫描对象 | 待扫描的软件包/固件。 |
| 任务名称 | 扫描文件的名称。 |
| 任务描述 | 对任务信息进行说明。 |
| 是否将本次扫描升级为专业版规格 | 当计费模式不是包年/包月，且免费版有剩余次数时涉及该参数。<br>● 关闭开关，本次扫描使用免费版配额。<br>● 打开开关，可以将本次扫描升级为专业版规格。升级后，您本次扫描可享受专业版规格，包含如下额外功能：支持查看完整的扫描结果及专业扫描报告导出，单次扫描最大支持5GB文件。如果您扫描次数较为频繁，建议您购买包年专业版服务。 |

**步骤4** 单击“确定”，开始上传和扫描文件。

**步骤5** （可选）如果文件上传失败，显示“续传”按钮。

- 单击“续传”，文件从断点处进行续传。
- 单击“确定”，则重新开始上传文件，不再显示“续传”按钮。
- 显示“续传”按钮后，刷新页面则不再显示“续传”按钮，不可续传。

**----结束**

# 5.2 管理二进制成分分析任务

## 操作场景

该任务指导用户通过开源治理服务查找、删除或停止二进制成分分析任务。

## 前提条件

- 已获取管理控制台的登录账号与密码。
- 已添加任务。

## 查看任务

**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，查看成分分析任务列表，相关参数说明如表5-2所示。

**表 5-2** 二进制成分分析任务列表参数说明

| 参数 | 参数说明 |
| --- | --- |
| 任务名称 | 二进制成分分析任务的名称。 |
| 任务描述 | 自定义描述。 |
| 任务状态 | • “等待中”<br>导入扫描对象后开始等待扫描。<br>• “进行中”<br>任务正在进行扫描。<br>• “已完成”<br>任务已完成扫描。<br>• “已停止”<br>任务扫描中单击了操作栏的“停止”。<br>• “已失败”<br>任务扫描失败。 |
| 安全漏洞 | 成分分析扫描出的漏洞分布情况。 |
| 开始时间 | 成分分析开始的时间。 |
| 任务时长 | 成分分析扫描完成、失败或停止的所用时长。 |
| 操作 | 查看报告、停止、删除按钮。 |

**步骤4** 在下拉框 

下拉选择任务状态，可根据任务状态筛选查看任务。

**步骤5** 在输入框 

中输入任务名称关键字或任务描述，可根据文件名关键字或任务描述筛选查看，可以和任务状态联合使用。

**步骤6** 单击  刷新任务列表。

**步骤7** （可选）报告比对。

1. 勾选两份任务状态无异常的报告。
2. 单击“报告对比”，进入报告对比详情页面，可查看比对结果。

**----结束**

## 删除任务

**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，可看到全部添加过的任务。

**步骤4** 单击待删除任务后操作列的“删除”。

根据系统提示执行删除操作。

**----结束**

### 停止任务

只有任务状态为进行中、等待中才可操作停止任务。

**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，可看到全部添加过的任务。

**步骤4** 单击待停止任务后操作栏的“停止”，在弹出的对话框中单击“确认”。

**----结束**

## 5.3 查看二进制成分分析扫描详情

该任务指导用户通过开源治理服务查看二进制成分分析扫描结果。

### 前提条件

- 已获取管理控制台的登录账号与密码。
- 已执行扫描任务。

### 操作步骤

**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，可看到全部添加过的任务。

**步骤4** 单击对应任务的任务名称，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5-3**所示。

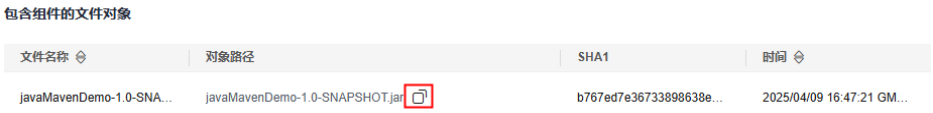
**表 5-3** 详情总览说明

| 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。<br>• 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：<br>– 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。<br>– 安全漏洞：展示超危、高危、中危、低危各个级别漏洞数量占比。<br>– 安全配置：展示通过、失败、不涉及的检测结果数量占比。<br>– 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。<br>– 密钥和信息泄露：展示信息泄露各检测项结果分布。<br>– 安全编译选项：展示安全编译各检测项结果分布。<br>– 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。<br>• 组件名称、组件版本和文件数可按升降序查看。<br>• 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。<br>• 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。<br>• 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。 |
| 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”后的  ，可以复制文件对象路径详细信息。

**图 5-1** 复制文件对象路径




  - 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”。

- 在“开源许可证”页签查看开源软件的许可证检测结果。
- 在“密钥和信息泄露”页签查看对应检测项目的检测结果。
- 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。
- 在“安全配置”页签查看凭据管理、认证问题和会话管理对应检测项目的检测结果。
- 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。

**----结束**

# 5.4 下载二进制成分分析扫描报告

## 操作场景

扫描任务成功完成后，您可以下载任务报告，报告目前支持PDF和Excel格式。

## 前提条件

已成功完成成分分析扫描任务，即任务状态为“已完成”。

## 操作步骤

**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，可看到全部添加过的任务。

**步骤4** 单击对应任务的任务名称，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。

**步骤5** 单击右上角“下载报告”，选择“生成PDF报告”或“生成Excel报告”，也可以单击“生成SBOM报告”生成国际通用的SBOM报告。

**步骤6** 扫描报告生成完成后，单击“导出PDF”或“导出Excel”，可以下载扫描报告。单击“导出SBOM报告”可以下载SBOM报告。

生成的扫描报告会在12小时后过期。过期后，若需要下载扫描报告，请再次单击生成报告，重新生成扫描报告。

**----结束**

## 二进制成分分析扫描报告模板说明

下载扫描报告后，您可以根据扫描结果，对漏洞进行修复，报告模板主要内容说明如下（以下截图中的数据仅供参考，请以实际扫描报告为准）：

- 概览
  查看目标软件包的扫描漏洞数。

**图 5-2** 查看任务概览信息

1 概览

1.1 任务综述

本次扫描检测出漏洞总数 84 个。其中超危漏洞有 9 个。

| | |
|---|---|
| 任务名称 | scrm-service-weixin.jar |
| 报告地址 | https://console /sbcScanList?recordId= |
| 开始时间 | 2022-07-25 20:48:56 |
| 结束时间 | 2022-07-25 20:51:47 |
| 扫描耗时 | 0.05小时 |
| 服务版本 | 1.1 |

- 结果概览
  统计漏洞类型及分布情况。

**图 5-3** 查看结果概览信息

2 结果概览

2.1 漏洞概览

安全漏洞等级：0.1-3.9低危；4.0-6.9中危；7.0-8.9高危；≥9.0超危

| 漏洞个数 | | | | |
|---|---|---|---|---|
| 总漏洞数 | 超危漏洞 | 高危漏洞 | 中危漏洞 | 低危漏洞 |
| 88 | 20 | 23 | 43 | 2 |

2.2 组件概览

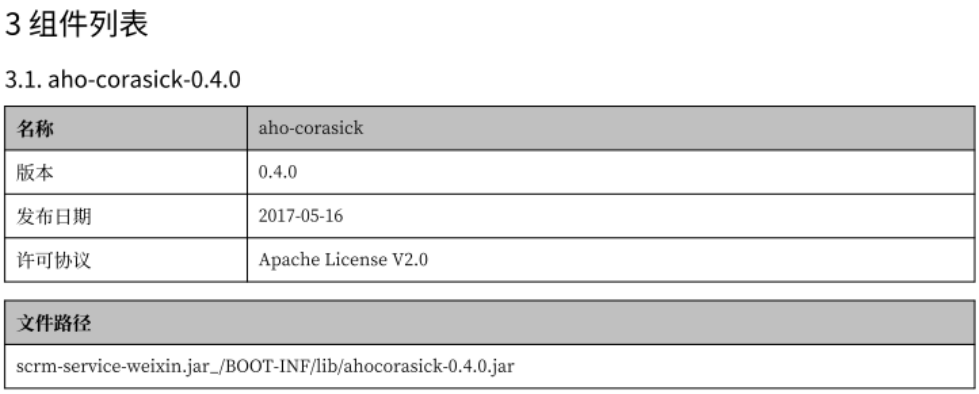
| 组件分布 | | | |
|---|---|---|---|
| 总组件数 | 风险组件 | 无漏洞组件 | 未知版本组件 |
| 55 | 6 | 34 | 15 |

2.3 许可协议概览

| 许可协议分布 | |
|---|---|
| 许可协议 | 组件数量 |
| Apache License V2.0 | 27 |
| MIT License | 2 |
| LGPL V3.0 | 2 |
| BSD 2-Clause License | 2 |
| FFmpeg License | 2 |
| BSD 3-Clause License | 1 |
| zlib/libpng License | 1 |
| OpenSSL Combined License | 1 |
| GPL V3.0 | 1 |

- 组件列表
  查看软件的所有组件信息。

  **图 5-4** 查看组件列表信息

  3 组件列表

  3.1. aho-corasick-0.4.0

  | 名称 | aho-corasick |
  | --- | --- |
  | 版本 | 0.4.0 |
  | 发布日期 | 2017-05-16 |
  | 许可协议 | Apache License V2.0 |

  | 文件路径 |
  | --- |
  | scrm-service-weixin.jar_/BOOT-INF/lib/ahocorasick-0.4.0.jar |

- 漏洞列表
  您可以参考每个组件扫描出的漏洞详细信息修复漏洞。

**图 5-5** 查看漏洞列表信息

## 4 漏洞列表

4.1.1. linux_kernel-4.4.197

4.1.1.1. CVE-2011-4917

| CVE编号 | CVE-2011-4917 |
| --- | --- |
| 漏洞描述 | Linux Kernel contains a flaw that is triggered as access to /proc/stat is world-readable and may allow disclosing mouse and keyboard activity. This may allow a local attacker to e.g. determine the length of typed passwords and in turn more easily guess a user's password. |
| 影响组件名称 | linux_kernel |
| 影响组件版本 | 4.4.197 |
| 漏洞发布时间 | 2017-07-17 00:00:00 |
| 漏洞CVSS分数 | 1.2 |
| 漏洞风险等级 | 低危 |
| 解决方案 | For details, see the reference link in the Reference Information column for vulnerability analysis and handling.[Machine Translation] |
| 漏洞修复参考 | https://lkml.org/lkml/2011/11/7/340 |

| 文件路径 |
| --- |
| rtos_sample.zip_/zImage |

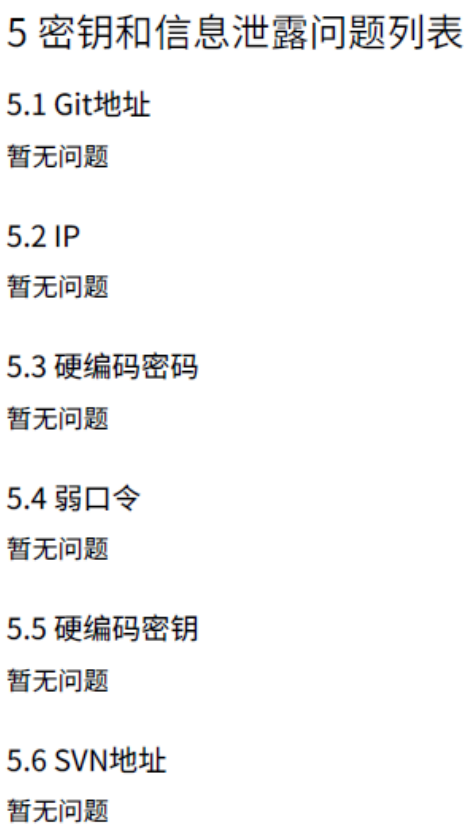
4.1.1.2. CVE-2007-3719

| CVE编号 | CVE-2007-3719 |
| --- | --- |
| 漏洞描述 | The process scheduler in the Linux kernel 2.6.16 gives preference to "interactive" processes that perform voluntary sleeps, which allows local users to cause a denial of service (CPU consumption), as described in "Secretly Monopolizing the CPU Without Superuser Privileges." |
| 影响组件名称 | linux_kernel |
| 影响组件版本 | 4.4.197 |
| 漏洞发布时间 | 2007-07-12 16:30:00 |
| 漏洞CVSS分数 | 2.1 |
| 漏洞风险等级 | 低危 |
| 解决方案 | |

- 密钥和信息泄露问题列表

**图 5-6** 查看密钥和信息泄露问题


5 密钥和信息泄露问题列表

5.1 Git地址

暂无问题

5.2 IP

暂无问题

5.3 硬编码密码

暂无问题

5.4 弱口令

暂无问题

5.5 硬编码密钥

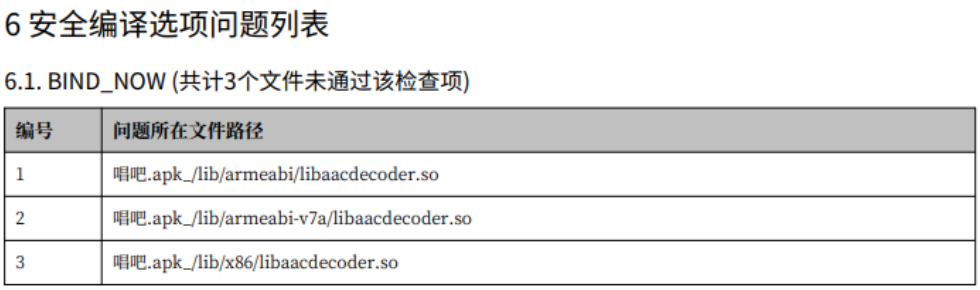
暂无问题

5.6 SVN地址

暂无问题

- 安全编译选项问题列表

**图 5-7** 查看安全编译选项问题列表


6 安全编译选项问题列表

6.1. BIND_NOW (共计3个文件未通过该检查项)

| 编号 | 问题所在文件路径 |
| --- | --- |
| 1 | 唱吧.apk_/lib/armeabi/libaacdecoder.so |
| 2 | 唱吧.apk_/lib/armeabi-v7a/libaacdecoder.so |
| 3 | 唱吧.apk_/lib/x86/libaacdecoder.so |

- 安全配置检查列表

**图 5-8** 查看安全配置检查列表

7 安全配置列表

7.1 预置账号信息检查

7.1.1

| 扫描项 | 预置账号信息检查 |
| --- | --- |
| 审视项 | 解析 /etc/passwd 和 /etc/shadow 文件，查看其配置参数是否合规 |
| 扫描结果 | 不涉及 |
| 原因 | 暂无问题 |

7.2 sudo高风险命令检查

7.2.1

| 扫描项 | sudo高风险命令检查 |
| --- | --- |
| 审视项 | 检查/etc/sudoers、/etc/sudoers.d相关配置 |
| 扫描结果 | 不涉及 |
| 原因 | 暂无问题 |

- 恶意软件扫描问题列表

**图 5-9** 查看恶意软件扫描问题

8 恶意软件扫描问题列表

8.1 病毒扫描

暂无问题

8.2 恶意代码扫描

暂无问题

# 5.5 相关术语说明

**开源(open source)**

即开放一类技术或一种产品的源代码，源数据，源资产，可以是各行业的技术或产品，其范畴涵盖文化、产业、法律、技术等多个社会维度。

**开源软件(open source software)**

允许用户直接访问源代码，通过开源许可协议将其复制、修改、再发布的权利向公众开放的计算机软件。

**开源组件(open source component)**

是开源软件系统中最小可识别且本身不再包含另外组件的、组件信息可在公共网站获取且可独立分发、开发过程中带有版本号并且可组装的软件实体。

**开源许可证(open source license)**

开源软件的版权持有人授予用户可以学习、修改开源软件，并向任何人或为任何目的分发开源软件的权利。

**软件成分分析(Software Composition Analysis)**

通过分析软件包含的一些信息和特征来实现对该软件的识别、管理、追踪的技术。

**PE(Portable Executable)**

是Windows系统下的可执行文件的标准格式。

**ELF(Executable and Linkable Format)**

是一种Unix或Linux系统下的可执行文件，目标文件，共享链接库和内核转储(core dumps)的标准文件格式。

**APK(Android application package)**

是Android操作系统使用的一种应用程序包文件格式，用于分发和安装移动应用及中间件。

**HAP(HarmonyOS application package)**

是鸿蒙操作系统使用的一种应用程序包文件格式，用于分发和安装移动应用及中间件。

**CVE(Common Vulnerabilities and Exposures)**

又称通用漏洞披露、常见漏洞与披露，是一个与信息安全有关的数据库，收集各种信息安全弱点及漏洞并给予编号以便于公众查阅。

**CVSS(Common Vulnerability Scoring System)**

通用漏洞评分系统，是一个行业公开标准，其被设计用来评测漏洞的严重程度，并帮助确定所需反应的紧急度和重要度，有CVSS 2.0、3.0、3.1标准。

**固件(firmware)**

是一种嵌入在硬件设备中的软件。

**NVD**

National Vulnerability Database国家安全漏洞库。

**CNVD**

China National Vulnerability Database国家信息安全漏洞共享平台。

**CNNVD**

China National Vulnerability Database of Information Security国家信息安全漏洞库。

**组件依赖**

保证组件正确运行所依赖的必须加载的其他组件。

# 6 查询审计日志

云审计服务是安全解决方案中专业的日志审计服务，记录了CodeArts Governance的相关操作事件，方便您日后的查询、审计和回溯。

## 支持审计日志的操作

**表 6-1** 云审计服务支持 CodeArts Governance 操作列表

| 操作名称 | 资源类型 | 事件名称 |
| --- | --- | --- |
| 创建二进制成分分析任务 | task | createScaTask |
| 删除二进制成分分析任务 | task | deleteScaTask |
| 生成二进制成分分析报告 | task | exportPdfScaTask/<br>exportExcelScaTask |
| 清理二进制成分分析资源 | resource | cleanUpScaResources |
| 创建源码成分分析任务 | task | registerTask |
| 停止源码成分分析任务 | task | cancelTask |
| 删除源码成分分析任务 | task | deleteTask |

## 查看审计日志

用户需要在云审计服务CTS的管理控制台查询CodeArts Governance服务的事件列表。详情请参考**查看审计事件**。