

开源治理服务

# 用户指南

文档版本 01  
发布日期 2024-11-21



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI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

---

<b>1 控制台总览</b> .....	<b>1</b>
<b>2 二进制成分分析</b> .....	<b>4</b>
2.1 添加二进制成分分析任务.....	4
2.2 管理二进制成分分析任务.....	6
2.3 查看二进制成分分析扫描详情.....	7
2.4 下载二进制成分分析扫描报告.....	11
2.5 相关术语说明.....	16
<b>3 源码成分分析</b> .....	<b>18</b>
3.1 添加源码成分分析任务.....	18
3.2 管理源码成分分析任务.....	20
3.3 查看源码成分分析扫描详情.....	22
<b>4 开源知识库</b> .....	<b>24</b>
<b>5 开源许可证</b> .....	<b>27</b>
<b>6 查询审计日志</b> .....	<b>28</b>

# 1 控制台总览

开源治理服务（CodeArts Governance）是覆盖软件研发阶段的安全、合规检测产品集合，提供一站式的原子化的安全服务和专家咨询服务的入口，满足企业客户、检测机构针对于研发阶段安全和漏洞检测的需求。


本节为您介绍开源治理服务控制台登录方式及菜单页。

## 登录开源治理服务控制台

1. 登录华为云官网，单击页面右上角“控制台”，如图1-1所示。

图 1-1 华为云官网



2. 将鼠标移至页面左上角，在滑出的服务列表中选择“开源治理服务”，即可进入开源治理服务控制台。

## 控制台简介

控制台包含：开源知识库、开源许可证、软件成分分析和专家咨询服务。

其中，软件成分分析包含总览、源码成分分析和二进制成分分析。专家咨询服务包括研发安全SDL培训。

表 1-1 单服务页面列表

服务名称	说明
开源知识库	开源知识库提供开源软件统一管理能力，通过对开源软件元数据、开源软件制品及源码的统一管理，提供可信的开源软件来源。
开源许可证	根据企业开源软件使用要求，管理和设置开源许可证的风险等级。

服务名称	说明
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， <a href="#">了解更多</a> 。
源码成分分析	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。
二进制成分分析	提供对产品二进制包的快速逆向分析，如：开源软件已知漏洞、密钥和信息泄露、安全编译选项、安全配置检测，并提供汇总的分析报告， <a href="#">了解更多</a> 。
专家咨询服务	<p>研发安全SDL培训</p> <p>SDL ( Security Development Lifecycle, 安全开发生命周期 ) 是为了应对愈发严峻的网络安全挑战而建立、发展的一系列方法论与最佳实践。华为SDL更是与IPD紧密结合，从公司政策、组织、流程、供应链、服务等方面建立和完善可持续、可信赖的覆盖产品研发全流程的安全保障体系。华为研发安全SDL实践高研班已上线云商店，面向研发高管，提供华为研发安全SDL概述、R&amp;D安全保障体系、网络安全技术能力建设等培训课程。</p>

## 软件成分分析总览页

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、高危漏洞数、许可证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，如所示，参数说明如所示。

图 1-2 最近一次二进制成分分析扫描



表 1-2 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。

# 2 二进制成分分析

## 2.1 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。

### 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。

图 2-1 添加任务

### 添加任务 温馨提示：免费版配额剩余3次 ?

✕

**\* 扫描对象**



点击选择文件或者将文件拖到此处

1. 支持 .zip、.rar、.tar、.tar.gz、.jar、.apk、.hap、.so、.gz、.gzip 等10+格式的文件
2. 文件名只能包含：中文、字母、数字、空格、下划线 ( \_ )、破折号 ( - ) 或点 ( . )
3. 文件名最大长度为100字符
4. 文件大小不能超过5GB(免费试用任务限制100MB)

任务名称

任务描述

是否将本次扫描升级为正式版规格 ?

**⚠ 二进制成分分析 免费版功能特点**

1. 每个用户有5次免费体验额度
2. 扫描文件大小不能超过100M
3. 仅支持开源软件漏洞扫描
4. 不支持报告下载

注：本次任务扫描将从您的免费扫描次数中扣除一次扫描配额！扫描失败不扣除！

数据资产严格保密

1. 服务将对您上传的文件及测试报告等严格保密；
2. 只有您 (相应华为云账号) 有权访问和处理以上数据资产；
3. 服务对您上传的文件扫描分析后会立即删除；

#### 📖 说明

- 支持上传 .7z、.arj、.cpio、.phar、.rar、.tar、.xar、.zip、.jar、.apk、.war 等格式文件，及 Android OTA Images、Android sparse、Intel HEX、RockChip、U-Boot 等固件。
- 当前仅提供正式版按需套餐扫描计费模式。

**步骤4** (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。

**步骤5** 文件上传成功后，单击“确定”，开始扫描。

----结束



## 2.2 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

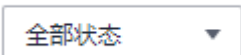
**步骤1** 登录开源治理服务控制台。


**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2-1所示。

表 2-1 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	<ul style="list-style-type: none"><li>• “等待中” 导入扫描对象后开始等待扫描。</li><li>• “进行中” 任务正在进行扫描。</li><li>• “已完成” 任务已完成扫描。</li><li>• “已停止” 任务扫描中单击了操作栏的“停止”。</li><li>• “已失败” 任务扫描失败。</li></ul>
创建人	此任务的创建者。
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。

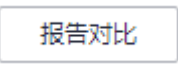
**步骤4** 在下拉框  下拉选择任务状态，可根据任务状态筛选查看任务。

**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  ，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

**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”。

### 说明

只有任务状态为进行中、等待中才可操作停止任务。

----结束

## 2.3 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2-2所示。

表 2-2 详情总览说明

栏目	说明
任务概况	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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： <ul style="list-style-type: none"> <li>- 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。</li> <li>- 安全漏洞：展示超危、高危、中危、低危各个级别漏洞数量占比。</li> <li>- 安全配置：展示通过、失败、不涉及的检测结果数量占比。</li> <li>- 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。</li> <li>- 信息泄露：展示信息泄露各检测项结果分布。</li> <li>- 安全编译选项：展示安全编译各检测项结果分布。</li> <li>- 恶意软件扫描：展示病毒和恶意代码扫描结果分布。</li> </ul> </li> </ul>
开源软件漏洞	<p>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。</p> <ul style="list-style-type: none"> <li>• 组件名称、组件版本和文件数可按升降序查看。</li> <li>• 可按组件名称、开源许可证对组件列表进行筛选查看。</li> </ul>
开源许可证	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
密钥和信息泄露	<p>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。</p>
安全编译选项	<p>显示BIND_NOW、NX、PIC等检测项目的描述、检测结果、不符合文件数。</p>

栏目	说明
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。

## 📖 说明

当扫描任务成功完成后，单击右上角的“下载报告”，选择“生成PDF报告”或“生成Excel报告”，生成扫描报告后，单击右上角的“导出PDF”或“导出Excel”，可以下载报告。

- 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”。

### curl 组件详情

#### 包含组件的文件对象

文件名称	对象路径	SHA1	时间
libtunnelapi.so	vastbase		2022/08/03 02:52:54 GMT+...

#### 已知漏洞

安全漏洞等级 🔴 超危 ≥9.0 🟡 高危 7.0-8.9 🟠 中危 4.0-6.9 🟡 低危 0.1-3.9

CVE	日期	CVSS版本	CVSS	漏洞等级
CVE-2021-22945	2021/09/23	3.0	9.1	超危
CVE-2021-22901	2021/06/11	3.0	8.1	高危
CVE-2022-22576	2022/05/26	3.0	8.1	高危
CVE-2021-22926	2021/08/05	3.0	7.5	高危
CVE-2021-22946	2021/09/29	3.0	7.5	高危
CVE-2022-27775	2022/06/02	3.0	7.5	高危
CVE-2022-27780	2022/06/02	3.0	7.5	高危
CVE-2022-27781	2022/06/02	3.0	7.5	高危
CVE-2022-27782	2022/06/02	3.0	7.5	高危
CVE-2021-22922	2021/08/05	3.0	6.5	中危

- 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“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。

图 2-4 安全配置检查结果

凭据管理		
检测项目	安全风险等级	检测结果
部署中等危险位置	低危	NA
sudo高危命令检查	低危	NA
组成及消息检查	低危	NA
UID为0的libroot库检查	低危	NA
库依赖高度检测	低危	NA
硬编码口令检查	低危	NA
历史口令重复使用检查	中危	NA
认证问题和会话管理		
检测项目	安全风险等级	检测结果
SSH authorized_keys文件检查	低危	NA
硬编码SSH主机密钥	低危	NA
SSH 配置检查	高危	NA
硬编码SSH私钥	低危	NA
开机启动服务检查	低危	NA
防暴力破解机制检查	低危	NA

- 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。

文件名称	文件位置	病毒名称
有病毒和恶意软件的文件.zip	--	Downloader.Win.Kulucz.8807a1f3
有病毒和恶意软件的文件.zip	--	Downloader.Win.Paph.710a5081
有病毒和恶意软件的文件.zip	--	Backdoor.Win32.FBIHQ.A
有病毒和恶意软件的文件.zip	--	Trojan.Agent.d5d69708
有病毒和恶意软件的文件.zip	--	Downloader.Win.Kulucz.8807a1f3

文件名称	病毒类别	病毒类型	病毒类型子类	威胁等级	所在位置	检测详情
有病毒和恶意软件的文件.zip	Python	恶意行为	系统命令替换	高危	高	疑似存在【系统命令替换】问题
有病毒和恶意软件的文件.zip	Python	恶意行为	木马下载执行	高危	高	疑似存在【木马下载执行】问题
有病毒和恶意软件的文件.zip	Python	恶意行为	恶意命令执行	中危	中	疑似存在【恶意命令执行】问题
有病毒和恶意软件的文件.zip	Python	恶意行为	高敏感码执行	高危	高	疑似存在【高敏感码执行】问题
有病毒和恶意软件的文件.zip	Python	恶意行为	敏感信息外发	高危	高	疑似存在【敏感信息外发】问题

---结束

## 2.4 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 单击右上角的“生成PDF报告”或“生成Excel报告”。

图 2-5 生成扫描报告



- 步骤6 扫描报告生成完成后，单击右上角的“导出PDF”或“导出Excel”，可以下载扫描报告。

图 2-6 下载扫描报告



### 说明

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PDF报告”或“生成Excel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 2-7 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[redacted]sbcScanList?recordId=[redacted]
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 2-8 查看结果概览信息

## 2 结果概览

### 2.1 漏洞概览

漏洞个数				
总漏洞数	超危漏洞	高危漏洞	中危漏洞	低危漏洞
927	24	344	523	36

### 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
19	8	0	1

### 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	8
MIT License	2
LGPL V2.1	2
Mozilla Public License (MPL) V1.1	1
GPL V2.0	1
OpenSSL Combined License	1
GPL V3.0	1

### 2.4 信息泄露概览

问题分布	
检查项	问题数量
弱口令	0
硬编码密码	4
硬编码密钥	14
IP	26
Git地址	30
SVN地址	1

- 组件列表  
查看软件的所有组件信息。

图 2-9 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 2-10 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	<a href="https://lkml.org/lkml/2011/11/7/340">https://lkml.org/lkml/2011/11/7/340</a>

文件路径	
	rtds_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 2-11 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 2-12 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 2-13 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 2-14 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

## 2.5 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。

# 3 源码成分分析

## 3.1 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，可根据实际情况选择扫描文件或代码仓。

- 文件扫描

图 3-1 添加文件扫描任务

×

### 添加任务

\* 任务名称

\* 扫描类型  文件  代码仓

\* 扫描对象 

  
点击选择文件或者将文件拖到此处

1. 支持 .zip、.tar.gz 格式的文件
2. 文件大小不能超过 1G
3. 解压后文件总大小不超过 10G
4. 解压后文件个数不超过 10 万个
5. 单个源文件超过 10M 不扫描
6. 文件名最大长度为 100 字符
7. 任务描述最大长度为 200 字符

任务描述

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。
扫描对象	待扫描的源码文件。
任务描述	对当前源码成分分析任务的说明。

- 代码仓扫描

图 3-2 添加代码仓扫描任务

×

### 添加任务

\* 任务名称

\* 扫描类型  文件  代码仓

\* 扫描对象

\* 标识类型  分支  tag

\* 标识名称

任务描述

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。
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	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	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

## 3.2 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。

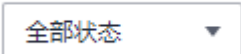
**步骤2** 在左侧导航栏，单击“软件成分分析 > 源码成分分析”。


**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3-1所示。

表 3-1 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。

参数	参数说明
任务状态	<ul style="list-style-type: none"><li>“等待中” 导入扫描对象后开始等待扫描。</li><li>“进行中” 任务正在进行扫描。</li><li>“已完成” 任务已完成扫描。</li><li>“已停止” 任务扫描中单击了操作栏的“停止”。</li><li>“已失败” 任务扫描失败。</li></ul>
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

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”。

#### 📖 说明

只有任务状态为进行中、等待中才可操作停止任务。

---结束

## 3.3 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3-2所示。

表 3-2 详情总览说明

栏目	说明
任务概况	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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： <ul style="list-style-type: none"> <li>- 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。</li> <li>- 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。</li> <li>- 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。</li> </ul> </li> </ul>
软件详情	<p>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。</p> <ul style="list-style-type: none"> <li>• 组件名称和文件数可按升降序查看。</li> <li>• 可按开源许可证对组件列表进行筛选查看。</li> <li>• 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。</li> </ul>

栏目	说明
开源许可证	<p>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。</p> <ul style="list-style-type: none"><li>• 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。</li><li>• 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。</li></ul>

----结束

# 4 开源知识库

开源知识库提供已治理的开源软件数据资产信息，包含元数据信息、漏洞信息、依赖信息等内容。

## 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“开源知识库”。
- 步骤3** 单击“开源知识库”页面搜索框左侧，在下拉框中选择“软件”或“组件”，在搜索框中输入对应名称，支持模糊搜索，单击“查询”，显示查询到的所有软件或组件信息，页面右侧显示当前库中软件和组件的统计图表，相关参数说明如表4-1所示。

图 4-1 开源知识库总览

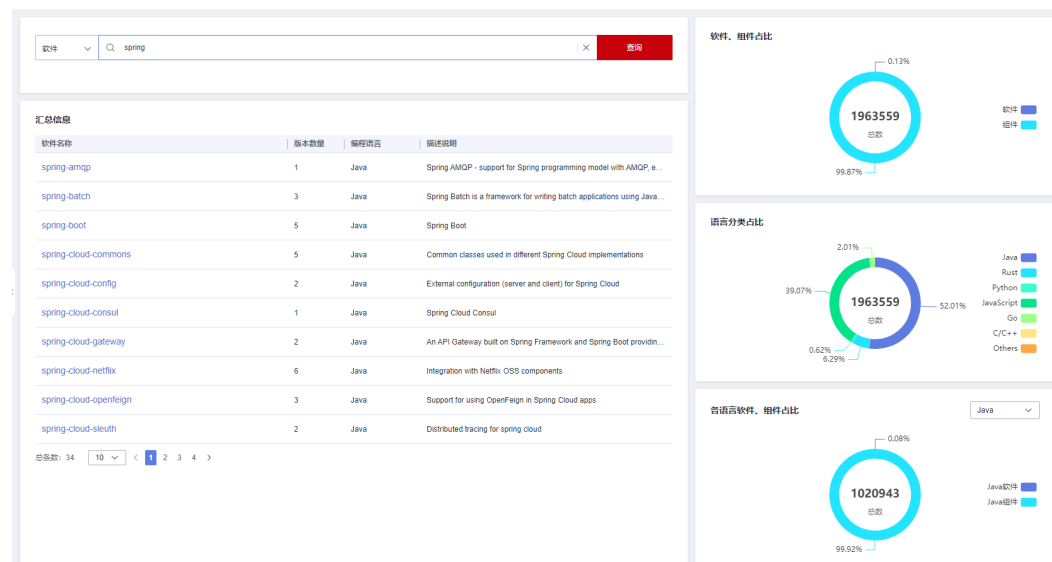


表 4-1 汇总信息参数说明

参数	参数说明
软件/组件名称	开源软件或组件的完整名称。
版本数量	该开源软件或组件在库中的版本数量。
编程语言	该开源软件或组件的主要编码语言。
描述说明	该开源软件或组件的描述。

**步骤4** 单击软件或组件名称，进入版本列表，显示所选择的软件或组件的所有版本信息，相关参数说明如表4-2所示。

图 4-2 所有版本信息列表

版本	漏洞数	发布时间	许可协议
3.0.9	1 3 9 0	2023/05/30 21:26:19 GMT+08:00	Apache-2.0

表 4-2 版本信息参数说明

参数	参数说明
版本	该开源软件或组件的版本号。
漏洞数	该版本下的具体漏洞数量，从左到右依次是超危、高危、中危、低危。
发布时间	该版本的发布时间。
开源许可证	该版本的开源许可证信息。

**步骤5** 单击软件或组件版本号，进入版本详情，显示版本的详细信息。

图 4-3 版本信息

基本信息	
软件名称	openssl
开发商	OpenSSL
版本描述	TLS/SSL and crypto library
版本	openssl-3.0.14
主语言	C/C++
参考信息	
官网地址	https://www.openssl.org
社区源码托管地址	https://github.com/openssl/openssl

**步骤6** 单击“漏洞信息”页签，查看漏洞列表，相关参数说明如表4-3所示。

图 4-4 漏洞信息

CVE	发布时间	CVSS版本	CVSS	漏洞等级
<a href="#">CVE-2023-2975</a>	2023/07/14 00:00:00 GMT+08:00	3.1	5.3	中危
<a href="#">CVE-2023-3446</a>	2023/07/19 00:00:00 GMT+08:00	3.1	5.3	中危
<a href="#">CVE-2023-3817</a>	2023/08/01 00:00:00 GMT+08:00	3.1	5.3	中危
<a href="#">CVE-2023-4807</a>	2023/09/08 00:00:00 GMT+08:00	3.1	7.8	高危
<a href="#">CVE-2023-5363</a>	2023/10/26 00:00:00 GMT+08:00	3.1	7.5	高危
<a href="#">CVE-2023-5678</a>	2023/11/07 00:00:00 GMT+08:00	3.1	5.3	中危
<a href="#">CVE-2023-6129</a>	2024/01/10 00:00:00 GMT+08:00	3.1	6.5	中危
<a href="#">CVE-2023-6237</a>	2024/01/15 00:00:00 GMT+08:00	3.1	5.9	中危
<a href="#">CVE-2024-0727</a>	2024/01/26 00:00:00 GMT+08:00	3.1	5.5	中危

总条数: 9  < 1 >

表 4-3 漏洞信息参数说明

参数	参数说明
CVE	漏洞的CVE名称。
发布时间	该漏洞的发布时间。
CVSS版本	该漏洞的分数版本。
CVSS	该漏洞的分数。
漏洞等级	该漏洞分数对应的漏洞等级。

步骤7 单击“CVE”字段，查看漏洞的详细信息。

图 4-5 漏洞详细信息

开源软件中心 / 版本历史 / 版本详情 软件 openssl 3.0.9

版本信息 漏洞信息

CVE	发布时间	CVSS版本
<a href="#">CVE-2023-2975</a>	2023/07/14 00:00:00 GMT+08:00	3.1
<a href="#">CVE-2023-3446</a>	2023/07/19 00:00:00 GMT+08:00	3.1
<a href="#">CVE-2023-3817</a>	2023/08/01 00:00:00 GMT+08:00	3.1
<a href="#">CVE-2023-4807</a>	2023/09/08 00:00:00 GMT+08:00	3.1
<a href="#">CVE-2023-5363</a>	2023/10/26 00:00:00 GMT+08:00	3.1
<a href="#">CVE-2023-5678</a>	2023/11/07 00:00:00 GMT+08:00	3.1
<a href="#">CVE-2023-6129</a>	2024/01/10 00:00:00 GMT+08:00	3.1
<a href="#">CVE-2023-6237</a>	2024/01/15 00:00:00 GMT+08:00	3.1
<a href="#">CVE-2024-0727</a>	2024/01/26 00:00:00 GMT+08:00	3.1

总条数: 9  < 1 >

**CVE-2023-2975 漏洞详情**

**漏洞详情**

漏洞ID CVE-2023-2975

发布时间 2023/07/14

修改时间 2024/02/04

CVSS分数 5.3

CVSS版本 3.1

CVSS矢量 --

---

**漏洞简介**

--

---

**解决方案**

--

---

**漏洞修复参考**

--

---

**参考链接**

<https://nvd.nist.gov/vuln/detail/CVE-2023-2975>

----结束

# 5 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“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 5-1 开源许可证

许可证名称	集成风险	许可证描述和风险分析	操作
AGPL V3.0	高	在分发或通过网络向用户提供软件时，无论是否修改，该软件本身都必须开源。2. 允许各种链接，但与其链接的所有代码必须开源。	重置
Apache 2.0 License with Export Control Warning	低	风险来自于美国出口管制制度的遵循。必须使用在产品中。建议向贵公司贸易合规办公室。	重置
Apache License V2.0	低	1. 允许以源代码和目标码形式复制、分发、分发作品或衍生作品。（注：衍生作品是指任何基于或衍生自该软件中的源代码或目标码形式的作品。为本许可证目的，衍生作品不包括...	重置
Apache Software License V1.1	低	允许以源代码和目标码形式修改或不停使用 and 分发。无限制代码开源义务。需要履行使用声明义务。需要在分发时附带版权声明。许可证声明	重置
BSD 2-Clause License	低	1. 允许以源代码和目标码形式修改或不停使用和分发。2. 声明要求 所使用软件中的版权声明+许可证文本+不担保声明	重置
BSD 3-Clause License	低	1. 允许以源代码和目标码形式修改或不停使用和分发。2. 声明要求 所使用软件中的版权声明+许可证文本+不担保声明	重置
BSD 3-Clause Open MPI variant	低	1. 允许以源代码和目标码形式修改或不停使用和分发。2. 声明要求 所使用软件中的版权声明+许可证文本+不担保声明	重置
BSD 3-Clause-LBNL	低	无开源风险。在分发时需附上版权声明及免责声明。不允许未经授权使用加州大学、Lawrence Berkeley 国家实验室、美国能源部的名字进行产品宣传。	重置
Common Development and Distribution License (CDDL)	中	Common Development and Distribution License: 2005年，SUN公司宣布将开放源代码Solaris的源代码，并推出CDDL作为其开放Open Solaris的许可证。许可证义务：可以复制...	重置
Common Development and Distribution License (CDDL)	中	许可证义务：可以复制和分发 CDDL 许可证软件的源码。不能删除或更改软件中所包含的任何版权、专利或商标声明。如果以可执行文件形式分发，需要包含和获取源码的链接方式。...	重置

- 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

# 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/ 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](#)。