

**CodeArts Governance**

# **Best Practices**

<b>Issue</b>	01
<b>Date</b>	2025-06-05



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

## **Huawei Cloud Computing Technologies Co., Ltd.**

Address: Huawei Cloud Data Center Jiaoxinggong Road  
Qianzhong Avenue  
Gui'an New District  
Gui Zhou 550029  
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

---

# Contents

1 CodeArts Governance Best Practices.....1

2 Performing Binary Software Composition Analysis (SCA)..... 2

# 1 CodeArts Governance Best Practices

---

This document summarizes operations practices of CodeArts Governance in each scenario, including the solution description, operation guide, and usage guide.

**Table 1-1** CodeArts Governance best practices

Best Practice	Description
<b>Performing Binary Software Composition Analysis (SCA)</b>	Performing binary software composition analysis (SCA) in CodeArts Governance

# 2 Performing Binary Software Composition Analysis (SCA)

---

## Scenario

According to the *2024 China Software Industry Outlook*, the software market in China exceeded CNY12 trillion in 2023. The software industry in China is developing rapidly. It is estimated that the overall market scale will exceed CNY21 trillion by 2029. According to the 2023 Software Supply Chain Status Report, from 2019 to 2022, the average YoY increase in open source software (OSS) supply chain attacks is 742%. Assessing open-source and third-party software faces the following challenges:

- There are no effective security detection methods for purchased or delivered software.
- Suppliers need to have basic security certifications.
- Open-source vulnerability response and fixing are inefficient. Security risks are not well managed.

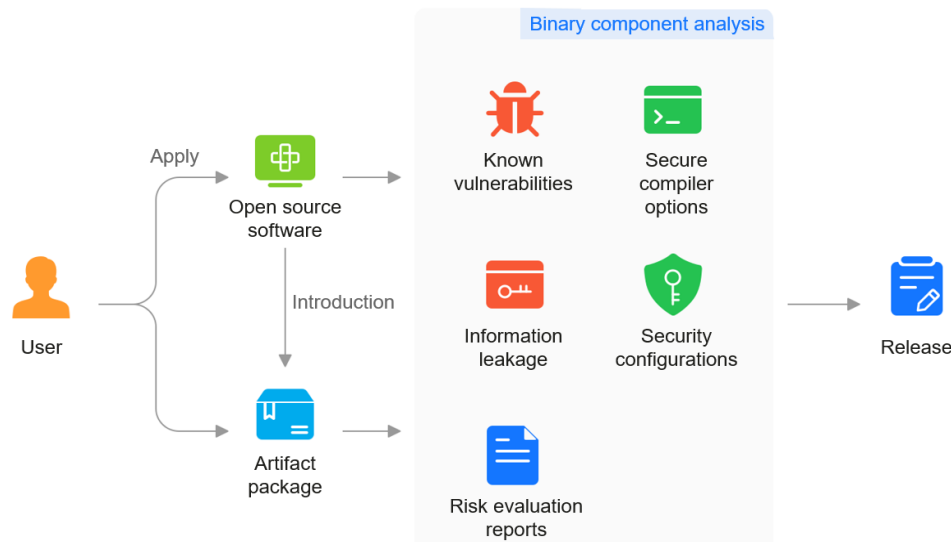
With CodeArts Governance, you can efficiently assess risks using APIs or on the web pages before you introduce software. The following features are provided.

- Comprehensive risk detection: CodeArts Governance analyzes software and firmware packages to identify software vulnerabilities against security rules. It also evaluates license compliance, password strength (including weak or hard-coded passwords), security configurations, and secure compiler options.
- Various applications supported: CodeArts Governance can scan desktop applications that run on Windows and Linux, mobile applications that run on Android Application Package (APK), iOS App Store Package (IPA), and HarmonyOS Ability Package (HAP), as well as embedded system firmware.
- Professional analysis and guidance: Risk information is presented based on thorough analysis from different perspectives, along with relevant troubleshooting suggestions.

## Solution Architecture

The following figure shows an example of how CodeArts Governance works. A user applies for open-source software (same process as third-party software) and

provides the artifact package to CodeArts Governance. The service then checks for known vulnerabilities, secure compiler options, information leakage, and security configurations, and provides a risk assessment report. The user fixes the detected vulnerabilities before using the software.



## Advantages

- Source code-free and harmless detection  
You only need to upload the product release package or firmware, without the need to build the running environment or run programs.
- Supporting multiple languages, file formats, and architectures  
Artifacts built using different languages or architectures can all be scanned.
- Prevention of sensitive data breach  
Potential risks in security configurations, passwords, and secret keys can all be identified.

## Constraints

**Table 2-1** Restrictions of the binary component analysis function

Category	Item	Description
Job management	Language	C, C++, Java, Go, JavaScript, Python, Rust, Swift, C#, and PHP
	Package format	Files in .7z, .arj, .cpio, .phar, .rar, .tar, .xar, .zip, .jar, .apk, .war, .rpm, and .deb formats and firmware such as Android OTA Images, Android sparse, Intel HEX, RockChip, and U-Boot can be uploaded.
	Package size	<ul style="list-style-type: none"><li>• Professional edition: 5 GB</li><li>• Free edition: 300 MB</li></ul>

## Procedure

- Step 1** Log in to the CodeArts Governance console.
- Step 2** In the navigation pane on the left, choose **SCA > Binary SCA**.
- Step 3** Click **Create Job**. In the displayed dialog box, click **Scan File**, select the software package to be scanned, and import it.

**Table 2-2** Parameters

Parameter	Description
Scan File	The software package and firmware to be scanned
Job	Name of the file to be scanned
Description	Description of the job
Upgrade this scan to Professional.	<p>This is shown when your free package has remaining scanning quota and yearly/monthly billing is not used.</p> <ul style="list-style-type: none"><li>• Disabled: The Free edition will be used for this scan job.</li><li>• Enabled: The Professional edition will be used for this scan job. After the upgrade, you can check complete scan results, export the report, and upload a file up to 5 GB. For frequent scans, yearly/monthly packages are recommended.</li></ul>

- Step 4** After the file is uploaded, click **OK** to start scanning.
- Step 5** Click a job name to check its report. Alternatively, click **View Report** in the **Operation** column of the job. [Table 2-3](#) lists items on the details page.


**Table 2-3** Items on the details page

Item	Description
Job Info	<ul style="list-style-type: none"><li>• <b>Basic Info:</b> The file name, file size, feature library version, and platform version are shown.</li><li>• Here presents the results of all scan items in a general way.<ul style="list-style-type: none"><li>– <b>Component Analysis:</b> the total number of components in the software package and the proportions of components with vulnerabilities, unknown versions, and no vulnerabilities</li><li>– <b>Vulnerability Severity:</b> the total number of vulnerabilities and the proportions of critical, high-risk, medium-risk, and low-risk vulnerabilities</li><li>– <b>Security Configurations:</b> the total number of check items and the proportions of passed, failed, and not-involved check items</li><li>– <b>Open-Source Software Licenses:</b> the statistics of licenses with high, medium, and low risks</li><li>– <b>Key and Info Leakage:</b> the total number of data leakage issues and their distribution</li><li>– <b>Secure Complier Options:</b> the total number of secure complier option issues and their distribution</li></ul></li></ul>
Open-Source Software Vulnerabilities	<p>The name, version, license, number of files, and number of vulnerabilities of each component in the scanning job</p> <ul style="list-style-type: none"><li>• You can filter the list by alphabetical order, component version, or the number of files.</li><li>• You can filter the component list by component name or open-source license.</li></ul>
Open-Source Software Licenses	<p>The license risks of different severity, including the integration and compatibility risks.</p> <ul style="list-style-type: none"><li>• <b>Licenses:</b> The license check result of binary file packages. The license name, integration risk, components involved, license description, and risk analysis are displayed.</li><li>• <b>Compatibility:</b> The check result of license compatibility risks in each directory of the binary file package.</li></ul>
Key and Info Leakage	<p>The check results of the Git addresses, IPs, hard-coded passwords, weak passwords, hard-coded keys, and SVN addresses.</p>
Secure Complier Options	<p>The description and result of BIND_NOW, NX, PIC check items, and number of files that do not meet the requirements.</p>
Security Configurations	<p>The check items, issue severity, and results related to credential management, authentication questions, and session management.</p>






- On the **Open Source Software Vulnerabilities** tab, check the vulnerabilities of each component.

You can click a component name to check vulnerability details.

- Click  next to object path to copy it.

**Figure 2-1** Copying an object path

Files with This Component

File 	Object Path	SHA1	Time 
javaMavenDemo-1.0-SNA...	javaMavenDemo-1.0-SNAPSHOT.jar 	b767ed7e36733898638e...	Apr 09, 2025 16:47:21 G...

- Click the CVE vulnerability name to check its details, description, fixing solution, reference, and reference links.
- On the **Key and Info Leakage** tab, check the result of each check item.
- On the **Secure Compiler Options** tab, check the result of each check item.

----End