

Code Insight 2021 R1 Release Notes

March 2021

Introduction	2
About Code Insight	2
New Features and Enhancements.....	2
Project Inventory Review	2
Project Reporting	3
Scan Agent Plugins.....	3
Scanning and Automated Discovery.....	4
Security Vulnerability Reporting	5
REST API Enhancements.....	6
Improved Performance for Report Generation and Download.....	7
New APIs.....	7
Updates to Existing APIs	8
Resolved Issues.....	11
Known Issues in this Release.....	13
Automated Workflow for Inventory Review/Publication.....	14
Export and Import.....	14
Installation and Configuration	14
Manual Codebase Analysis	15
Performance	16
Project Administration and Management.....	16
Project Inventory	16
Project Reporting	16
REST APIs.....	17
Scan Agent Plugins.....	17
Scanning and Automated Discovery.....	18
Source Control Management (SCM) Support	20
Web UI.....	20
Legal Information	22

Introduction

These Release Notes provide the following information about the Code Insight 2021 R1 release:

- [About Code Insight](#)
- [New Features and Enhancements](#)
- [Resolved Issues](#)
- [Known Issues in this Release](#)
- [Legal Information](#)

About Code Insight

Code Insight is the next generation Open Source security and compliance management solution. It empowers organizations to take control of and manage their use of open source software (OSS) and third-party components. Code Insight helps development, legal, and security teams use automation to create a formal OSS strategy that balances business benefits and risk management.

New Features and Enhancements

The Code Insight 2021 R1 release provides new features and enhancements in the following areas:

- [Project Inventory Review](#)
- [Project Reporting](#)
- [Scan Agent Plugins](#)
- [Scanning and Automated Discovery](#)
- [Security Vulnerability Reporting](#)
- [REST API Enhancements](#)

Project Inventory Review

The following new feature is available for reviewing project inventory.

[Direct Link from Associated File to the Analysis Workbench](#)

Users with Analyst permissions for a project can click the hyperlinked path for a file associated with an inventory item in **Project Inventory** to open the file's **File Details** tab in the **Analysis Workbench**. From here, the user can view file evidence and, if necessary, add or remove files associated with the inventory.

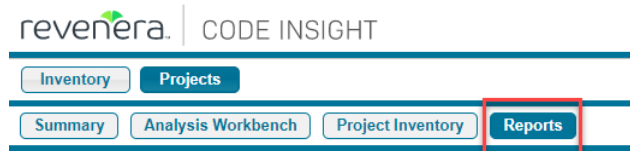
If the current user does not have Analyst permissions, the path remains in plain text in **Project Inventory**.

Project Reporting

The following new feature is available for generating and viewing project reports.

New Project Reports Tab

A new **Reports** tab is now available for generating and viewing reports for a project. (Previously, reports were generated from a reports section on the project's **Summary** tab.) This tab, available within the context of a given project, provides a quick access to all the project's most recently generated reports as well as to the UI needed to generate new reports.



From this tab, you can generate any standard or custom Code Insight report for the project and view and download the report. For those custom reports that require a second project for comparison purposes, a pop-up list is displayed to select the project. You can generate multiple *different* reports simultaneously.

Scan Agent Plugins

The following new features and enhancements are available for Code Insight scan-agent plugins.

- [License Evidence Now Reported in Code Insight](#)
- [Support for Code Insight Report Generation as Part of Jenkins Build Scan](#)

License Evidence Now Reported in Code Insight

License evidence found in files scanned by a scan-agent plugin is now reported in Code Insight Web UI. This evidence is reflected in the **Analysis Workbench** as follows:

- The **Codebase Files** and **Search File Results** panes show the green icon for those remotely scanned files that contain license evidence.
- The license instances and totals on the **Evidence Details** pane include those instances found in remotely scanned files.
- In the **Codebase Files** or **Search File Results** pane, users can now select **Show file evidence** from the right-click menu for one or more remotely scanned files (or a folder containing such files) to view the license evidence instances found in the files. (The instances are listed on the **Evidence Details** pane.)

Conversely, on the **Evidence Details** pane, if users select instances of license evidence and click **Filter to selected files**, any remotely scanned files that contain the selected evidence are listed in the **Search File Results** pane.

- Previously, the filters could locate remotely scanned files in an **Advanced File Search** included only **File Size, File Path, File Digest, Review Status, and Inventory Status**. The following additional filters can now locate these files: **Evidence status, Has license matches, Does not have license matches, and License**.

Currently, license evidence for remotely scanned files is available in the Code Insight Web UI only. The availability of license evidence in Code Insight reports and REST APIs is planned for a future release.

Migration to 2021 R1

After migrating to 2021 R1, users must rescan the remote codebases in their projects to see the codebases' license evidence in the Code Insight Web UI.

Support for Code Insight Report Generation as Part of Jenkins Build Scan

The Jenkins plugin can now be configured to generate a Code Insight report of your choice as part of the Jenkins build scan. After the plugin sends the scan results to Code Insight, the specified report is generated in Code Insight and sent back to Jenkins, where you can then view it as part of the build process. Thus, the report provides a means to view the results of the build scan within Jenkins itself without having to go to Code Insight to see the results. (The report is also available in Code Insight on the **Reports** tab for the project.)

Viewing the Code Insight report as part of the build scan requires that the Jenkins HTML Publisher extension be installed and configured in the Jenkins build environment. Complete details are found in the *Code Insight Plugins Guide*.

Scanning and Automated Discovery

This release provides the following enhancements to the Code Insight codebase scan and the Automated and Advanced Analysis techniques used in scans:

- [Rescan Options to Scan Only Changed Files](#)
- [Using Global Scan Queue to Stop Scans and Remove Scans in Queue](#)
- [Improved Detection Notes](#)

Rescan Options to Scan Only Changed Files

By default, certain Code Insight events that might have occurred since the last scan (for example, a change to Automated Analysis rules, the Code Insight version, or certain scan profile settings) can determine whether a rescan of your codebase performs a scan on all files (full rescan) or on only those codebase files that have changed since the last scan. Previously, there was no way to control this default behavior.

In this release, new options available for scan profiles enable System Administrators to override this default behavior for projects associated with a given profile. The new options can allow rescans to always skip unchanged files and scan only changed files, even if events that typically call for a full rescan have occurred. They also delineate which unchanged files are skipped: all unchanged files, only unchanged files that have been reviewed, only unchanged files that are associated with inventory, or only unchanged files that are both reviewed and associated with inventory.

Note that these new rescan options are ignored when users initiate a full forced rescan. For this type of scan, all files—changed or unchanged—are always completely rescanned.

For the latest information about rescans and the events that can result in a full rescan, see the “Rescanning Your Codebase (Server Scans Only)” in the *Code Insight User Guide*. For information about the new scan options available for scan profiles, see the *Code Insight Installation & Configuration Guide*.

Using Global Scan Queue to Stop Scans and Remove Scans in Queue

In Code Insight 2020 R4, the global Scan Queue was introduced to enable the monitoring of the scan queue and the currently running scan for any Scan Server in your Code Insight instance. In 2021 R1, this feature has been enhanced so that you can now stop the scan currently running on a selected Scan Server or remove any scans currently in queue on that server.

To stop a scan or remove a queued scan from the global Scan Queue, you must have either Project Administrator or Analyst permissions for the project associated with the scan.

Improved Detection Notes

The **Detected By** attribute in the **Detection Notes** content in both **Project Inventory** and **Analysis Workbench** indicates the automated detection technique(s) responsible for the inventory finding. The following example shows that the detection technique used to find the inventory item was Jar Analyzer.

```
Detection Notes
Notes from Automated Finding:
Vendor: oracle
As-found name: javax.ws.rs-api
Other licenses:
  License name: CDDL-1.1
  URL: http://spdx.org/licenses/CDDL-1.1.html
  License name: GPL-2.0-with-classpath-exception
  URL: http://spdx.org/licenses/GPL-2.0-with-classpath-exception.html
Detected By: Jar Analyzer
Attributes:
Source: manifest
  Bundle-Description: Java API for RESTful Web Services (JAX-RS)
Source: manifest
  Bundle-License: http://glassfish.java.net/public/CDDL+GPL_1_1.html, http://glassfish.java.net/public/CDDL+GPL_1_1.html
Source: manifest
  Implementation-Version: 2.0.1
Source: manifest
```

Security Vulnerability Reporting

This release provides the following enhancement to Code Insight’s reporting of security vulnerabilities found in open-source or third-party components.

Support for CVSS v3.1

Code Insight now supports CVSS 3.1 (along with the previously supported v3.0) when reporting security vulnerabilities associated with project inventory. A new **CVSS v3.x** replaces the previous CVSS v3 option on the **Administration > System Settings** page, enabling Code Insight to report both CVSS v3.1 and v3.0 security vulnerabilities.

Security Vulnerability Options

Select preferred Common Vulnerability Scoring System (CVSS) version for security vulnerability reporting:

CVSS v2.0

CVSS v3.x

Code Insight continues to support the option to report CVSS v2.0 vulnerabilities instead.

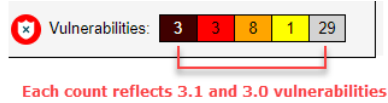
CVSS v3 Vulnerability Reporting

When reporting a CVSS v3.1 or v3.0 vulnerability, Code Insight uses the generic label **CVSS v3.x** for the vulnerability score in the Web UI and the term **CvssV3** in labels in API responses. However, the vector information for a given vulnerability (when available) will indicate the specific CVSS version—3.1 or 3.0—that was used to score the vulnerability. The following shows CVSS 3.x information for a vulnerability in the Web UI.

The following shows this same information in an API response.

```
{
  "vulnerabilityId": 1126884,
  "vulnerabilityName": "CVE-2017-1000372",
  "vulnerabilityDescription": "A flaw exists in OpenBSD's implementation of the stack guard page that allows attackers to bypass it resulting in arbitrary code execution using setuid binaries such as /usr/bin/at. This affects OpenBSD 6.1 and possibly earlier versions.",
  "vulnerabilityCvssV2Score": 7.5,
  "vulnerabilityCvssV2Severity": "HIGH",
  "vulnerabilityCvssV2Vector": "AV:N/AC:L/Au:N/C:P/I:P/A:P",
  "vulnerabilityCvssV3Score": 9.8,
  "vulnerabilityCvssV3Severity": "CRITICAL",
  "vulnerabilityCvssV3Vector": "CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H",
  "vulnerabilityURL": "https://nvd.nist.gov/vuln/detail/CVE-2017-1000372",
  "vulnerabilitySource": "NVD"
},
```

Additionally, when Code Insight uses CVSS v3x, vulnerability counts shown in the UI (see below) and the API responses reflect both 3.1 and 3.0 vulnerabilities. (A given vulnerability can have either a v3.1 or v3.0 score, not both.)



REST API Enhancements

The following tables describe the new or updated Code Insight REST APIs:

- Improved Performance for Report Generation and Download
- New APIs
- Updates to Existing APIs

Improved Performance for Report Generation and Download

The previous `project/generateReport` API both generated and downloaded a report. Memory issues occurred when reports ran in parallel or when large reports were downloaded. In this release, `project/generateReport` has been replaced with two new APIs:

```
/projects/{projectId}/reports/{reportId}/generate  
/projects/{projectId}/reports/{reportId}/download
```

Memory issues are mitigated if the new generate API is called multiple times for different reports or for different projects because reports are now placed in a queue and generated sequentially. Additionally, the new download API can process large reports with minimal memory consumption.

New APIs

The following new REST APIs were added in this release:

Table 1 - New APIs in this Release

Resource	API Endpoint	Method	Description
Project	<code>/projects/{projectId}/reports/{reportId}/download?taskId={taskId}</code>	GET	One of two new APIs replacing <code>/project/generateReport</code> (which also downloaded reports). The API requires the task ID of the generated report as parameter to download the report.
	<code>/projects/{projectId}/reports/{reportId}/generate</code>	POST	One of two new APIs replacing <code>/project/generateReport</code> . The API response is a task ID used as download the report (see the previous table row). This new API generates reports sequentially to avoid out-of-memory issues.

Updates to Existing APIs

The following updates to existing APIs have occurred in this release.

Table 2 • Updates to Existing APIs

Resource	API Endpoint	Method	Description
Component	components/search	GET	<p>Support for component search by forge. The searchBy parameter now includes a FORGE option. When this option is selected, you must select a forge for the forgeName parameter and complete the required additional parameters pertaining to the selected forge.</p> <p>Optionally, the forgeName parameter and associated required parameters can be used as additional search criteria if you selected NAME, URL, or CPE for the searchBy parameter.</p>
	components/{componentId}	GET	<p>Support for CVSS v3.1 (along with previously supported 3.0) when reporting security vulnerabilities. The response includes the following changes to address this enhancement:</p> <ul style="list-style-type: none"> • When the response is configured to show vulnerability details by component version, each vulnerability listed includes a new vulnerabilityCvssV3[V2]vector attribute. For a v3 vulnerability, this attribute specifies the version—3.1 or 3.0—used to score the given vulnerability (or shows N/A if the value is not available). • When the response is configured instead to simply summarize vulnerability counts by component version, the counts in the CvssV3 summary for each component version reflect both CVSS 3.0 and 3.1 vulnerabilities. (A given vulnerability can have either a v3.0 or v3.1 score, not both.) • Previous CVSSV3.0 labels in the summary have been changed to CvssV3. Likewise, previous CVSSV2 labels are changed to CvssV2.

Table 2 • Updates to Existing APIs


Resource	API Endpoint	Method	Description
	components/{versionId}/vulnerabilities	GET	<p>Support for CVSS v3.1 (along with previously supported 3.0) when reporting security vulnerabilities. The response includes the following changes to address this enhancement.</p> <ul style="list-style-type: none"> • A new vulnerabilityCvssV3[V2]vector attribute has been added to each security vulnerability listed. • The vulnerabilityCvssV3vector value specifies the version—3.1 or 3.0—used to score the vulnerability (or shows N/A if the value is not available).
Project	/projects/{projectId}	GET	<p>Support for CVSS v3.1 (along with previously supported 3.0) when reporting security vulnerabilities for project inventory. The response includes the following changes to address this enhancement.</p> <ul style="list-style-type: none"> • In the CvssV3 summary of vulnerability counts for each inventory item, the counts reflect both CVSS 3.0 and 3.1 vulnerabilities. (A given vulnerability can have either a v3.0 or v3.1 score, not both.) • Previous CVSSV3.0 labels in the summary have been changed to CvssV3. Likewise, previous CVSSV2 labels are changed to CvssV2.
	/projects/{projectId}/allscannedfiles	GET	<p>Additional information now returned for each file to indicate whether or not it contains evidence, has been reviewed, and is associated with inventory.</p> <ul style="list-style-type: none"> • containsEvidence (true or false) • reviewed (true or false) • inInventory (true or false) <p></p> <p>Note • The value for these new attributes returned for a legacy inventory-only project is “N/A”.</p>
	/projects/{projectId}/evidences	GET	<p>New attributes added to response to indicate whether a given file contains evidence of source-code matches or is an exact-file match:</p> <ul style="list-style-type: none"> • exactFileMatches (true or false) • sourceMatches (true or false)

Table 2 • Updates to Existing APIs

Resource	API Endpoint	Method	Description
	/projects/{projectId}/inventorySummary		<p>Support for CVSS v3.1 (along with previously supported 3.0) when reporting security vulnerabilities for project inventory. The response includes the following changes to address this enhancement. (These changes are available when vulnerabilitySummary is true.)</p> <ul style="list-style-type: none"> • In the CvssV3 summary of vulnerability counts for each inventory item, the counts reflect both CVSS 3.0 and 3.1 vulnerabilities. (A given vulnerability can have either a v3.0 or v3.1 score, not both.) • Previous CVSSV3.0 labels in the summary have been changed to CvssV3. Likewise, previous CVSSV2 labels are changed to CvssV2.
	/projects/{projectId}/users	GET	<p>New option added to the roleId parameter to retrieve the Project Administrators for the given project.</p>
	/projects/inventory/{projectId}	GET	<p>Support for CVSS v3.1 (along with previously supported 3.0) when reporting security vulnerabilities for project inventory. The response includes the following changes to address this enhancement. (These changes are available when skipVulnerabilities is false.)</p> <ul style="list-style-type: none"> • A new vulnerabilityCvssV3[V2]vector attribute has been added to each security vulnerability listed. • The vulnerabilityCvssV3vector value specifies the version—3.1 or 3.0—used to score the vulnerability (or shows N/A if the value is not available).

Table 2 • Updates to Existing APIs

Resource	API Endpoint	Method	Description
Inventory	inventories/ {inventoryId}	GET	Support for CVSS v3.1 (along with previously supported 3.0) when reporting security vulnerabilities. The response includes the following changes to address this enhancement. (These changes are available when skipVulnerabilities is false .) <ul style="list-style-type: none">• A new vulnerabilityCvssV3[V2]vector attribute has been added to each security vulnerability listed.• The vulnerabilityCvssV3vector value specifies the version—3.1 or 3.0—used to score the vulnerability (or shows N/A if the value is not available).
	inventories/ {inventoryId}/ vulnerabilities	GET	Support for CVSS v3.1 (along with previously supported 3.0) when reporting security vulnerabilities. The response includes the following changes to address this enhancement. <ul style="list-style-type: none">• A new vulnerabilityCvssV3[V2]vector attribute has been added to each security vulnerability listed.• The vulnerabilityCvssV3vector value specifies the version—3.1 or 3.0—used to score the vulnerability (or shows N/A if the value is not available).

Resolved Issues

The following issues are resolved in this release.

Table 3 • Resolved Issues

Issue	Description
SCA-12454	Variables in vulnerability notification emails now properly resolved.
SCA-26037	Selection of one or more paths (on the project Scan Settings tab) to scan within the Source Code Management (SCM) repository now properly handled.
SCA-27402	Spaces now allowed in the user password for a Source Code Management (SCM) connection.

Table 3 - Resolved Issues (cont.)

Issue	Description
SCA-28997	Out-of-memory issues when running the Project report now resolved. This issue was resolved independently of but further enforced by the REST interface enhancement described in Improved Performance for Report Generation and Download .
SCA-29452	Out-of-memory issues when generating reports now resolved. This issue was resolved with the REST interface enhancement described in Improved Performance for Report Generation and Download .
SCA-29464	Branch Project Summary page now correctly showing the Scan Server for the new branched project (instead of the Scan Server for the source project).
SCA-29488	Out-of-memory issues when running reports and scans in parallel through REST API now resolved. This issue was resolved independently of but further enforced by the REST interface enhancement described in Improved Performance for Report Generation and Download .
SCA-29652	Code Insight no longer reporting both LGPL 2.0 and LGPL 2.1 licenses for a file associated with only the LGPL 2.1 license.
SCA-29878	Special characters in component descriptions no longer getting changed.
SCA-29887	Issue with scan returning vulnerabilities that are false positives for the SplunkD component now resolved.
SCA-29930	Error message logged for an invalid password containing spaces no longer showing a part of the invalid password.
SCA-30039	Transitive dependencies now being reported for optional dependencies in a Maven POM.xml file.
SCA-30119	Improved performance in loading and searching a Projects list containing a large number of projects or projects large in size.
SCA-30486	All projects belonging to a user now visible in the Projects list when the My Projects filter is enabled. Previously, those projects for which the user had only a Project Administrator role were not visible when the filter was in effect.
SCA-30490	Out-of-memory error when generating reports in parallel through REST API now resolved. This issue was resolved with the REST interface enhancement described in Improved Performance for Report Generation and Download .
SCA-30567, SCA-30626	The detection vulnerabilities that are false positives during scan of the Spring Framework now resolved.
SCA-30700	Improved Analysis Workbench load time after a project's initial scan.
SCA-30777	Generation of an erroneous "import failure" message no longer occurring.

Table 3 - Resolved Issues (cont.)

Issue	Description
SCA-30790	Out-of-memory error when running Code Insight more than 5 days now resolved. This issue was resolved with the REST interface enhancement described in Improved Performance for Report Generation and Download .
SCA-30546	Project Contact user changed through REST API now automatically assigned to the same additional project roles that are automatically granted to a Project Contact changed through the Code Insight Web UI.
SCA-31920	The JVM maximum heap value no longer ignored when running Code Insight as a Windows service. See the <i>Code Insight Installation & Configuration Guide</i> for the new configuration steps.
SCA-32212	Issue with detection of false positive vulnerabilities in the Arc component resolved. (The issue is resolved with the latest Electronic Update.)

Known Issues in this Release

The following are current known issues in Code Insight. The issues are organized as follows:

- [Automated Workflow for Inventory Review/Publication](#)
- [Export and Import](#)
- [Installation and Configuration](#)
- [Manual Codebase Analysis](#)
- [Performance](#)
- [Project Administration and Management](#)
- [Project Inventory](#)
- [Project Reporting](#)
- [REST APIs](#)
- [Scan Agent Plugins](#)
- [Scanning and Automated Discovery](#)
- [Source Control Management \(SCM\) Support](#)
- [Web UI](#)

Automated Workflow for Inventory Review/Publication

The following are known issues with the automated workflow for inventory review and publication in Code Insight.

SCA-11193: Incorrect URL(s) in email notifications

In cases where Code Insight is running on a server that uses multiple IP addresses (for example, a server that has both a wired and wireless active network connection), the Core Server address cannot be accurately resolved. As a consequence, users can encounter an incorrect URL in the email notification received from Code Insight. This issue is most often seen if the Code Insight core server is configured as “localhost” instead of a full IP address.

Workaround: None exists.

Export and Import

The following are known issues with the Code Insight project export and import functionality.

SCA-3222: Import overrides inventory details

Importing the same inventory into a project that already contains inventory can cause some details to be overwritten or blanked out. If duplicate inventory (by associated repository item ID) is encountered during the import process, inventory details are overwritten with data from the export data file.

Recommended: Perform an export of the project prior to importing into the project in case you need to return to the original project state.

SCA-21295: Import of Detection Notes over 16 MB generates an error

When Code Insight uses a MySQL database, an error can occur during a project import if the source project’s **Detection Notes** content exceeds 16 MB. The import process generates an error message and continues processing the inventory but does not import the notes.

Workaround: Ensure that only a single network interface controller is enabled on the core server running Code Insight. As an added measure, configure the core server using a numerical IP address instead of a “localhost”.

Installation and Configuration

The following are known issues with Code Insight installation and configuration.

SCA-15952: Installer unable to install embedded JRE on some Windows 10 instances

Running the installer on some (but not all) Windows 10 systems results in an “Installation: Successful null” message and does not completely populate the <INSTALL_ROOT>\jre directory.

Workaround: Should you encounter the above error, install the JRE manually. Download JRE 8u192 [here](#). Configure the JAVA_HOME and JRE_HOME variables in catalina.* to point to the newly installed JRE.

SCA-1652 / SCA-5812: Deleted or disabled users are still visible in the Web UI

Users who are deleted from the LDAP server or disabled in LDAP still appear on the **Users** page in the Code Insight Web UI and in some selection lists, such as for projects.

Workaround: None exists. However, deleted or disabled users are blocked from logging into the application and attempting to add one of these users will result in an error.

If this workaround is not sufficient or doable, contact Revenera Support for information about executing a database SQL script that can help to complete the index process within the expected time. The script must be run *before* the Electronic Update is started. (To contact Revenera Support, access the **Get Support** menu in the Revenera Community at <https://community.revenera.com>.)

Manual Codebase Analysis

The following are known issues with manual codebase analysis in the **Analysis Workbench** in Code Insight.

SCA-27011: Advanced Search based on low confidence inventory not working

In the **Analysis Workbench**, an **Advanced Search** for files associated with inventory that has a low confidence level is returning incorrect or no results.

Workaround: None exists.

SCA-22398: Licenses not highlighted even though evidence exists

Cases can occur during a scan when a license is discovered in the scan results and listed on the **Evidence Summary** tab, but no associated license text is highlighted on the **Partial Matches** tab. The lack of highlighting occurs because the scanner is unable to calculate the offsets for license text in the file.

Workaround: None exists.

SCA-22308: "Email/URLs" evidence truncated

In some cases after running a scan, the **Email/URLs** evidence on the **Evidence Details** tab in **Analysis Workbench** is truncated.

Workaround: None exists.

SCA-10414: Associated files not displayed when user adds more than 37K files to inventory

When more than 37K files are added to an inventory item, the associated files are not displayed on the **Associated Files** tab.

Workaround: Right-click the inventory item and select **Show Inventory Files**. The content on the **File Search Results** pane in **Analysis Workbench** is filtered to the associated files for the inventory item.

Performance

The following are known issues with Code Insight performance.

Performance slower with MySQL 8 than with MySQL 7

Codebase scans and updates to the Code Insight data library are slower when Code Insight uses the MySQL 8 (5.8) database compared to when it uses MySQL 7 (5.7).

Project Administration and Management

The following are known issues with project administration in Code Insight.

SCA-20012: File filters in Chrome and Edge browsers not showing supported upload archive types correctly

When selecting a codebase archive to upload from File Upload dialog, the file filter on the browser you are using might list the supported archive types properly:

- On the Chrome browser, the file filter list incorrectly shows “Custom Files” instead of “Supported Files” and does not allow you to filter on the individual supported archive types.
- On the Edge browser, the file filter list shows unsupported archive types.

Workaround: None exists.

Project Inventory

The following are known issues with Code Insight project inventory.

SCA-11520: Policies not applied on rescan of a project

The triggering event for applying policy to project inventory is “Publish” (not scan). Policies are applied during the initial scan if the default setting **Automatically publish system-created inventory items** is enabled and not applied during a rescan because inventory is not re-published. This behavior is in place to avoid inadvertent overriding of inventory status due to a change in policy by another user.

Workaround: To apply policy, first recall all inventory and rescan with **Automatically publish system-created inventory items** enabled.

Project Reporting

The following are known issues with Code Insight reporting.

SCA-22054: Project Report not showing URLs for custom vulnerabilities

The Project report is not showing the NVD (National Vulnerability Database) URLs for custom vulnerabilities until they are updated to the Data Library.

Workaround: Use the Web UI to view all vulnerabilities associated with inventory.

SCA-11263: Project Report hyperlink on tasks worksheet for inventory does not work

Clicking on an inventory link in the Project Report takes the user to the login page even if user is currently logged in. This is a bug in Excel.

Workaround: Log into the application. Go back to the Excel report output and click on the hyperlink again. This is an issue only for inactive sessions.

REST APIs

The following are known issues with the Code Insight REST interface.

SCA-16508: Swagger page hangs when required API parameters are missing

Instead of producing an appropriate error message, a Swagger page can hang when you attempt to execute an API without providing required parameters.

Workaround: None exists.

SCA-7950: Page and size parameters are not working with some REST APIs

Limiting the result set returned by some REST APIs is not currently supported. Using the page and size parameters with the Component Lookup and Get Project Inventory APIs (and possibly others) returns the full result set.

Workaround: None exists. However, the issue will be addressed in an upcoming release.

Scan Agent Plugins

The following are known issues with Code Insight scan-agent plugins.

SCA-28141: Maven, Ant, and Gradle scan-agent rescans might fail in dynamic host environments

Rescans performed by Maven, Ant, and Gradle scan-agent plugins v2.0 (introduced in Code Insight 2020 R3) might fail in dynamic host environments. This is due to a v2.0 requirement that rescans use the same scan-agent alias and hostname used in the previous scan. This will be addressed in a future release.

Workaround: Use the Jenkins scan-agent or the scan-agent for another CI tool that supports the “host” property. This property enables you to provide a user-defined hostname that does not change between scans.

SCA-27678: Possible deadlocks with parallel agent scans on same project

Deadlocks might occur when at least one scan-agent scan and one or more other scans (agent or server) run simultaneously on the same project.

Workaround: Scans can be scheduled in sequence to avoid deadlock exceptions.

SCA-27431: Dependencies currently not reported for Maven and Gradle scan agents

Previous versions (1.x) of the Maven and Gradle scan-agent plugins scanned both the dependencies section *and* the project build directory of the Maven or Gradle application project. However, version 2 of the plugins, introduced in Code Insight 2020 R3, scans the project build directory, but not the dependencies section. Thus, dependencies are currently not reported for scans performed by the two plugins.

Workaround for Maven: Refer to the Maven documentation for instructions on how to include dependencies as a part of build directory. An example install command for including dependencies might be:

```
maven-dependency-plugin install copy-dependencies ${project.build.directory}/project-dependencies
```

Workaround for Gradle: Refer to the Gradle documentation for instructions on how to include dependencies as a part of build directory. An example install command for including dependencies might be:

```
task copyToLib(type: Copy) { into "$buildDir/output/lib" from configurations.runtime }
```

You would then use the following command to run the scan agent from the Gradle application project:

```
gradle build copyToLib code-insight-scan
```

SCA-3378: Jenkins scan-agent plugin – downgrade not supported

After a Jenkins plugin upgrade, a downgrade button option is available in the Web UI. Clicking on the option results in a 404 error.

Workaround: None exists.

Scanning and Automated Discovery

The following are known issues with Code Insight codebase scans and the detection techniques used by scans.

SCA-31486: Scan status not immediately in effect after “Stop Scan” issued

Currently, when a user forces a currently running scan to stop (for example, by clicking **Stop Scan** from the project **Summary** tab or the global **Scan Queue** dialog), the stopped status for the scan might not take effect immediately, even after a screen refresh.

Workaround: None exists.

SCA-30756: Increased scan times for some codebases when NG-bridge data update facility is enabled

In cases where the instance on which the Code Insight Scan Server is running has the NG-bridge data update facility enabled, the scan is able to identify more exact-file matches. However, increased matching can also cause the scan and rescan times to increase for certain codebases. This increased time can be a problem for some sites.

Workaround: Disable the NG-bridge data update facility. (Note that this facility is initially disabled by default.)

SCA-30423: Scans with large number of source-code matches resulting in longer scan times

When project is scanned with the Comprehensive scan profile or a custom scan profile, either of which has source-code matching enabled, the scan takes longer than usual if it encounters a large number of matches.

Workaround: None exists.

Inventory automatically published during previous scan now unpublished after rescan

To address issues, Code Insight now assigns a confidence level of **Low** to those inventory items that are identified by a file-name analyzer technique (a part of automated analysis) during a scan. If your project is configured to publish inventory with **Medium** or **High** confidence, inventory detected by this technique will now have an automatic unpublished status. This change is applicable only for new scans.

Workaround: The previously published inventory items are still available. In the **Analysis Workbench**, simply filter inventory by **Not Published** to view the unpublished inventory, and then publish inventory as needed.

SCA-26486: Conda first-level dependencies with Semantic versions not resolved

Semantic versions for Conda first-level dependencies are not being resolved.

Workaround: None exists.

SCA-7820: Some NPM version patterns are not supported

When scanning an NPM project, certain versions might not be detected through automated analysis. The following are not supported: URLs as dependencies, versions containing a hyphen (for example, "crypto-js": "3.1.9-1"), and versions of the format X.X.X (for example, "through": "X.X.X").

Workaround: None exists.

SCA-3000: Scan agent plugins might generate inventory with no selected license

In this release, using the scan agent plugin, you might end up with inventory that has no license associated with it if the scan agent is not able to identify a specific license in the scanned files. In this case, the inventory item is created using Compliance Library data. You might see the inventory item with one or more possible licenses and potentially no selected license.

Workaround: Recall the inventory item to prevent it from showing up in the published inventory items list.

Source Control Management (SCM) Support

The following are known issues with Code Insight SCM support.

SCA-30568: Significant space consumed by Perforce synchronization logs in Code Insight

When a user synchronizes a Code Insight project with a Perforce codebase by clicking **Sync Now** from any SCM instance tab, the synchronization automatically adds Perforce log data to the Tomcat logs in Code Insight. This behavior can result in large Tomcat log files.

Workaround: Synchronize Code Insight with the Perforce codebase directly through the Perforce command-line client installed on the Scan Server instance.

SCA-27751: Failure of Perforce SCM instance to synchronize Unicode files to Scan Server

Perforce SCM instances can fail to synchronize Unicode-formatted files to the Scan Server if the instance is running in Windows and configured for SSL.

Workaround: None exists.

SCA-27674: Synchronization with Team Foundation Server Failing (Linux only)

Codebase synchronization with a Team Foundation Server (TFS) instance on Linux fails when character spaces or certain special characters exist in attributes used to set up the synchronization on the **Version Control Settings** tab for a project.

The following issue has been logged with TFS:

<https://github.com/microsoft/team-explorer-everywhere/issues/321>

Workaround: None exists.

Web UI

The following are known issues with the Code Insight Web UI.

SCA-27892: Project Dashboard showing incorrect format after report generation for agent scans

If only a scan agent has performed a remote scan for a project and a report is subsequently generated for the project, the project Dashboard is showing a split **Scan Summary** pane with scan statistics for both the scan agent and the scanner (which shows statistics of 0 since it has run no scan). The **Scan Summary** should not be split; the full pane should list statistics for the remote scan only.

SCA-21917: Last Server Scan field on dashboard showing date of report generation

The **Last Server Scan** value on the **Project Dashboard** should show the date of the last scan. However, when a report is generated, this date changes to the report-generation date.

Workaround: Obtain the last scan date from the scan history link (in the **Past Server Scans** field) on the project **Summary** tab.

SCA-20683: Project details not automatically updating after scan

Project details are not automatically updating after a scan in the Web UI.

Workaround: Refresh the screen.

Legal Information

Copyright Notice

Copyright © 2021 Flexera Software

This publication contains proprietary and confidential information and creative works owned by Flexera Software and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera Software is strictly prohibited. Except where expressly provided by Flexera Software in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera Software intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera Software, must display this notice of copyright and ownership in full.

Code Insight incorporates software developed by others and redistributed according to license agreements. Copyright notices and licenses for these external libraries are provided in a supplementary document that accompanies this one.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera Software, see <https://www.revenera.com/legal/intellectual-property.html>. All other brand and product names mentioned in Flexera Software products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.