

Code Insight 2023 R2 SP1 Release Notes

June 2023

Introduction	2
About Code Insight	2
Revenera Resources	2
Changes in Code Insight 2023 R2 SP1	3
New Features and Enhancements	3
Advanced Inventory Searches	3
Application Life Cycle Management (ALM) Support	4
Components and Licenses	5
Data Library and Electronic Updates	6
Jobs Queue	7
Project Management	7
Project Reporting	9
Scan Agent Plugins	9
Scanning and Automated Discovery	10
Source Code Management (SCM) Support	12
User Experience	13
REST API Enhancements	13
New APIs	14
Updates to Existing APIs	15
Resolved Issues	19
Issues Resolved in 2023 R2 SP1	20
Issues Resolved in 2023 R2	20
Known Issues	22
All-Project Inventory View	22
Automated Workflow for Inventory Review/Publication	23
Data Library and Electronic Updates	23
Export and Import	25
Installation, Upgrades, and Configuration	25
Inventory History	26
Manual Codebase Analysis	26
Performance	28
Project Inventory	28
Project Management	29
Project Reporting	30
REST APIs	30

Scan Agent Plugins.....	30
Scanning and Automated Discovery.....	34
Source Code Management (SCM) Support	36
Vulnerability Suppression/Unsuppression	38
Web UI.....	39
Legal Information	40

Introduction

These Release Notes provide the following information about the Code Insight 2023 R2 release and subsequent service packs:

- [About Code Insight](#)
- [Reverera Resources](#)
- [Changes in Code Insight 2023 R2 SP1](#)
- [New Features and Enhancements](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [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.

Reverera Resources

The following resources can help you stay up to date with Code Insight news and product knowledge:

- In addition to providing case management, the [Reverera Community](#) site can help you quickly find answers to your questions by searching content from other customers, product experts, and thought leaders. You can also post questions on discussion forums for experts to answer. For each of Reverera's product solutions, you can access forums, blog posts, and knowledge base articles.
- You can find documentation for Code Insight and all other Reverera products on the [Reverera Product Documentation](#) site.
- The [Reverera Learning Center](#) offers free, self-guided online videos to help you quickly get the most out of your Reverera products. You can find a complete list of these training videos in the Learning Center.

- For customers who have purchased a maintenance contract for their product(s), you can submit a support case or check the status of an existing case by making selections on the **Get Support** menu of the [Reverera Community](#).

Changes in Code Insight 2023 R2 SP1

The Code Insight 2023 R2 Service Pack (SP) 1 release contains the following changes:

- The new feature [Top-Level Inventory Now Detected in Debian Packages](#)
- Resolved issues described in [Issues Resolved in 2023 R2 SP1](#)

The remaining information in this document, which pertains to the previous Code Insight 2023 R2 release, required no additional updates to address this service pack.

New Features and Enhancements

Code Insight 2023 R2 release and its subsequent service packs introduce new features and enhancements in the following areas. (The description for a feature or enhancement introduced in a service pack states the specific service-pack release.)

- [Advanced Inventory Searches](#)
- [Application Life Cycle Management \(ALM\) Support](#)
- [Components and Licenses](#)
- [Jobs Queue](#)
- [Project Management](#)
- [Project Reporting](#)
- [Scan Agent Plugins](#)
- [Scanning and Automated Discovery](#)
- [Source Code Management \(SCM\) Support](#)
- [User Experience](#)
- [REST API Enhancements](#)

Advanced Inventory Searches

The following enhancements to the Advanced Inventory Search feature is now available.

Search Support for Blank Custom Fields in Inventory

The Advanced Inventory Search feature can now filter to published inventory items containing custom fields with no values. The option **Is Empty** has been added as an operator for custom-field criteria in the **Advanced Inventory Search** dialog.

Any

Inventory Custom Fields

Additional Comments: Contains Search Text:

Modification Details: Contains Search Text:

Vulnerability Ignore List: Is Empty Contains Equals Is Empty Search Text:

The new filter helps users to easily locate the inventory to add the missing field values.

Default Criteria Operator Changed to AND

The default operator (in the **Apply** field) that is applied to the search criteria on the **Advanced Inventory Search** dialog has been switched from **Or** to **And**. This enhancement supports the common search setup that requires multiple criteria be met.

Application Life Cycle Management (ALM) Support

The following enhancement to Code Insight's ALM integration is now available.

New “Authentication Type” Field for Creating Jira ALM Instances

The setup for a Jira ALM instance in Code Insight now includes the **Authentication Type** field. This property identifies the deployment mode of the Jira Server—on the Cloud or on premise—which, in turn, dictates the type of authentication credentials that Code Insight must provide to successfully connect to the server. This new field helps ensure that users enter the correct type of credentials and that these credentials are validated properly according the deployment type.

Instance #1 - Jira Instance #2 - Jira Instance #3 - Jira Instance #4 - Jira Instance #5 - Jira Instance #6 - Jira Instance #

Application: Jira

ALM Instance Name: anyInstancetest ?

JIRA Server URL: https://jira.flexera.com/ ?

Authentication Type: On Premise Jira: Bearer Token(Personal Access Token) ?

JIRA Username: Cloud Jira: Basic HTTP(Username & API Token) ?

JIRA Password/API Token: On Premise Jira: Basic Auth(Username & Password) ?

Default Project Key: On Premise Jira: Bearer Token(Personal Access Token) ?

For complete details about this new field, refer to the “Integrating with Application Lifecycle Management” section in the *Code Insight Installation & Configuration Guide*. This section also describes how pre-2023 R2 ALM Jira instances are migrated to the current Code Insight release.

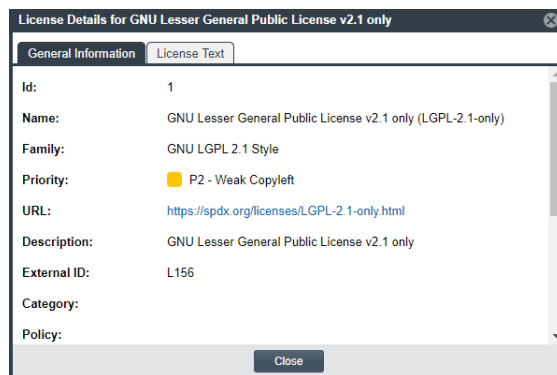
Components and Licenses

The following enhancements to component and license information in Code Insight data library are now available.

License Mapping to External IDs

A Code Insight system administrator can use the **Update Licenses External ID** API (see [New APIs](#)) or the **Create Custom License** API to map a specified license to its corresponding ID in an external system (such as your site's own license-tracking system). This external ID is saved with the license's information in the Code Insight data library and is thus visible in Code Insight, enabling users to easily locate the license in the external system.

The external license property is displayed in the **License Details** window (accessed from the information icon next to a license name in the UI) and on the **Licenses** tab in the Global Component & License Lookup feature.

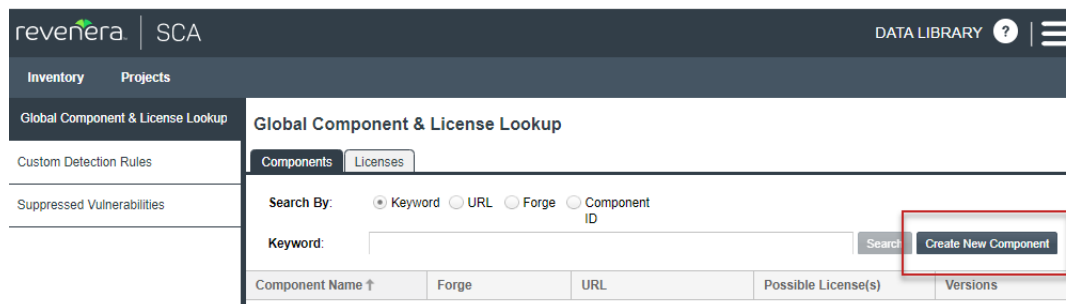


This property is also included in API responses that list license details. See [REST API Enhancements](#) for more information.

Creation of Custom Components and Licenses From the Global Component & License Lookup Feature

In previous releases, users could create a custom component or license only within the context of an inventory item that they were creating or editing. Starting in this release, users who cannot find a specific component or license during their searches using the Global Component & License Lookup feature can conveniently create the missing entity directly from this feature. When the component or license is saved, it is immediately available for lookups both in the Global Component & License Lookup UI and in the UI used to create or edit inventory.

The new **Create New Component** or **Create New License** button is available on the **Components** tab or **Licenses** tab, respectively, in the Global Component & License Lookup UI.

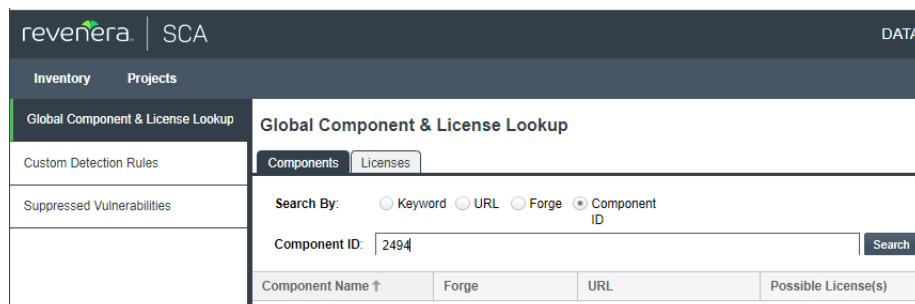


For more information, refer to “Exploring Components Globally” and “Exploring Licenses Globally” in the *Code Insight User Guide*.

Support for Component Lookup by Component ID in the Global Component & License Lookup Feature

Users can now search for a component by its ID in the Code Insight Data Library when using the Global Component & License Lookup feature. This new criterion is in addition to the previously available criterion selections (**Keyword**, **URL**, and **Forge**) on the **Components** tab.

For more information, refer to “Exploring Components Globally” in the *Code Insight User Guide*.



Data Library and Electronic Updates

The following enhancements related to the Code Insight data library and the Electronic Update are available in this release.

Enhancements to Processing Security Vulnerabilities in Post-Update Step

The Electronic Update includes a post-Update step that processes security vulnerabilities against your Code Insight instance. Specifically, the step determines whether new vulnerabilities included in the Update impact any inventory in the instance’s projects. For those projects impacted, the step sends a notification to project owners indicating that a new vulnerability is impacting specific inventory items in their project.

Previously, this step could take several days if a large number of inventory items were impacted by one or more vulnerabilities. Additionally, because Code Insight did not have proper logging to track the progress of vulnerability processing, customers believed that their system had hung.

The following enhancements are now available to address this behavior:

- Overall improved processing times during the post-Update phase.
- Improved logging during the post-Update phase. Users can now track the following information in the log.
 - The number new vulnerabilities included in the Electronic Update
 - The number of inventory items affected by the new vulnerabilities
 - A set of statistics for every 1000 inventory items processed to help users gauge the progress of vulnerability processing against inventory
- A new **skip.post.pdl.vul.processing** variable in the PAS_GLOBAL_PROPERTIES table, which, when set to **true**, skips the post-Update phase entirely. Skipping this phase can significantly shorten the Electronic Update process. However, project owners will not receive notifications about which inventory items are impacted by new vulnerabilities. (The default value for this variable is **false** to maintain the post-Update phase.)

Jobs Queue

The following enhancement to the Code Insight Jobs Queue feature is now available.

Support for “Export to SBOM Insights” and “Update Notices” Jobs

The **Jobs** queue has been updated to support jobs for the following two new operations introduced in this release:

- [Project Inventory Export to SBOM Insights](#)
- [Automatic Update of Notices Across Inventory in a Project](#)

As jobs, these operations are queued and run in the background without contention with other operations. Users can monitor the status of these jobs and, when needed, filter the queue on the new job types, **Export to SBOM Insights** and **Update Notices**, respectively.

These new operations can also be initiated and added to the **Jobs** queue through the REST interface, as described in [New APIs](#).

Project Management

The following enhancements to Code Insight project management are now available.

Project Inventory Export to SBOM Insights

This release introduces feature that exports inventory data from a Code Insight project to SBOM Insights.

About SBOM Insights

SBOM Insights (a Revenera SCA product) gives organizations the ability to manage security and legal risk by maintaining a complete, accurate SBOM (Software Bill of Materials) in the cloud. SBOM Insights aggregates this SBOM over multiple sources and provides full visibility of its contents to security and legal teams, as well as to supply chain partners.

The New Export Feature

If Code Insight has been configured to perform SBOM Insights exports, Project Analysts can now export inventory data from a given Code Insight project directly to SBOM Insights. When the export process is finished, SBOM Insights automatically imports the exported data to a bucket, where the data is managed and aggregated with SBOMs from other sources. (For complete information about SBOM Insights, click [here](#) to access the SBOM Insights user documentation.)

Configuration and Process Overview

Refer to the following table for an overview of the configuration tasks and the process involved in an export from Code Insight to SBOM Insights.

Phase	Performed By	Description	For More Information
1	Code Insight System Administrator	Configures Code Insight to enable SBOM exports.	Refer to “Configuring Code Insight for Exports to SBOM Insights” in the Code Insight Installation & Configuration Guide.
2	Code Insight Project Administrator	Assigns the Code Insight project to a specific SBOM Insights bucket.	Refer to “Assigning the Project to an SBOM Insights Bucket” in the <i>Code Insight User Guide</i> .
3	Code Insight Project Analyst	Initiates the process that exports the project’s inventory to SBOM Insights and imports it to the specified bucket.	Refer to “Exporting Project Inventory to SBOM Insights” in the <i>Code Insight User Guide</i> .
4	SBOM Insights	Automatically imports the exported inventory to the assigned bucket as a set of “SBOM parts”.	Click here to open to the section in the SBOM Insights help describing SBOM parts and their import into SBOM Insights.
5	Any Code Insight user	Accesses the Code Insight Jobs queue to track the progress of the export.	Refer to “Monitoring the Code Insight Jobs Queue” in the <i>Code Insight User Guide</i> .

Automatic Update of Notices Across Inventory in a Project

Code Insight offers a new feature that automatically updates all inventory items in a project with the appropriate third-party notices obtained from the Revenera Data Library. Users can choose to update the notices text for every inventory item in the project or only those inventory items with an empty **Notices Text** field. When the option to update the notices text for all inventory is performed, any existing notices text for inventory is overwritten.

When initiated, the notices update is scheduled in the Code Insight **Jobs** queue.

Only Project Analysts can perform a notices update through the UI. However, both Project Analysts and Project Reviewers can perform this operation through the REST interface. See [New APIs](#).

For complete information about using this new feature, refer to “Updating Third-Party Notices Across Inventory for a Project” in the *Code Insight User Guide*.

Project Reporting

The following enhancement to Code Insight reporting is now available.

Performance Improvement for the Project Vulnerability Report

In previous releases, when users generated the custom Project Vulnerability Report, performance could be degraded if a large number of files were associated with project inventory. This issue has been addressed with the addition of a new option **Include associated files** in the report’s UI, enabling users to control whether to include associated files in the report.

This option is passed to the new **includeFiles** filter in the **Get Project Inventory** REST API, which is called by the report. See [Updates to Existing APIs](#).

Scan Agent Plugins

The following enhancements to Code Insight remote scanning are now available.

Custom Temporary Directory for Scanning Docker Images

Previously, the Docker Images plugin both stored a specified image file and scanned its extracted contents in the `/tmp` directory on the machine where the plugin is installed. However, this directory did not always have sufficient space to process these files.

Users now have the option to use the `/tmp` directory by default or specify a directory of their choice for storing and scanning extracted files. (This custom directory is specified by including a `-tmpdir` parameter in the command that launches the plugin scan.) As with the `/tmp` directory, the artifacts are deleted from the custom directory once the scan completes.

For more information, see “Docker Images Plugin” in the *Code Insight Plugins Guide*.

Visual Studio Plugin Support Extended to Include Visual Studio 2019

The Visual Studio plugin has extended its support to include Visual Studio 2019.

Jenkins and Generic Plugin Support Extended to Include Open JDK 11

The Jenkins and generic plugins have extended their Java 11 support (previously for Oracle Java 11 only) to include OpenJDK 11. These plugins continue to support Java 8 as well.

Scanning and Automated Discovery

This release includes the following enhancements to Code Insight scans and the Automated Analysis techniques used to discover and report inventory during scans.

Top-Level Inventory Now Detected in Debian Packages

(Introduced in 2023 R2 SP1) Scans now properly discover top-level inventory in Debian (.deb) packages. If an inventory item discovered in a Debian package has a match in the Debian forge, the item is created as a published top-level inventory item with a High confidence level. Any item that does not have a match in the forge is created as an unpublished top-level inventory item with a “Work in Progress” designation and a Low confidence level.

Custom Detection Rules Based on File Paths

Code Insight enables users to create custom rules used by the Automated Analysis processes in detecting third-party or OSS components and generating inventory from these findings. A custom rule uses file criteria to detect a given component based on the one or more codebase files generally associated with the component.

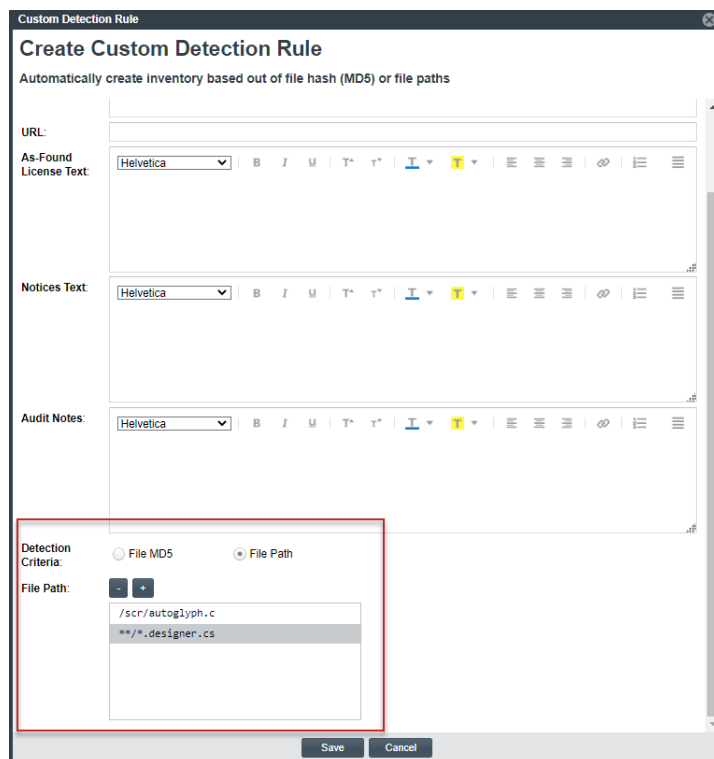
Until this release, custom rules supported the use of only MD5 values as the criteria for locating file matches in the codebase. In this release, custom rules support either MD5 values *or file paths* as the criteria for locating files. (The rule can be defined with only one type of file criteria, not a combination of MD5 values and file paths.)

This option is also supported in the **Rules** REST interface. See [Updates to Existing APIs](#).



Note - The new option is available only when creating or editing the rule from the **Custom Rules** tab on the **Data Library** page. It is not available when creating a custom rule within the context of an inventory item in the **Analysis Workbench**.

For complete details about using this new option, refer to the “Creating a Custom Detection Rule from Scratch” in the *Code Insight User Guide*.



System-Generated “Work in Progress” Inventory Created as “Unpublished”

Starting in this release, any Work in Progress inventory item generated by a scan (whether performed by the Scan Server or by a remote scan plugin) is no longer automatically published despite the settings in the project’s scan profile and the project’s **Auto-Publish** rule based on the confidence level of inventory.

Note the following:

- “Work in Progress” inventory items that have been manually created or edited are not impacted by this rule during a rescan.
- For projects last scanned prior to this release, this new rule is applied accordingly to inventory that will be generated during the next full rescan.
- User-invoked forced full rescans on the Scan Server and full rescans triggered internally by the different analysis techniques during a regular rescan will regenerate previous system-generated inventory (ignoring any edits). This behavior might unpublish any previously published Work in Progress inventory according to the new rule.

Inventory Detected by File Name Analyzer Generated as “Unpublished”

Inventory detected by only the File Name Analyzer during a scan is now always system-generated as “unpublished”.

Inventory Detection in Additional Gradle and Maven Files

Code Insight now supports the detection of inventory and dependencies in these additional files:

- Maven `.pom` file
- Gradle version catalogs
- Gradle `kts` files (Beta support only)

See the “Automated Analysis chapter in the *Code Insight User Guide* for details.

Cocoapod Packages Now Properly Mapped to the GitHub Forge

Top-level inventory items in a Cocoapod package are now properly detected based on their vendor and repository in the GitHub forge.

Dependencies of the top-level inventory, as found in `.podspec` files, will have no vendor or repository information available and consequently are generated as unpublished Work in Progress inventory.

Dependencies Now Generated for Top-level Inventory Not Explicitly Identified in Setup.py

Previously, if a top-level inventory item was not explicitly identified in the `Setup.py` file, its associated first-level dependencies in Pypi packages were not available in the scan results. This behavior occurred because no explicit top-level inventory existed with which to associate the dependencies. Code Insight now creates this top-level inventory item based on its folder name, enabling first-level dependencies to be associated with the item in the scan results. The top-level inventory is created as an unpublished Work in Progress item.

Source Code Management (SCM) Support

This release includes the following enhancement to Source Code Management (SCM).

Support for Multiple Repository URLs in a Single Git Instance

Instead of configuring a separate SCM Git instance for a each Git repository that will synchronize to the Scan Server, users can now specify multiple Git repository URLs in a single instance. Managing multiple Git repository connections from one SCM instance is more convenient than navigating between individual instances.

To support this enhancement, users now append the Git branch, tag, or commit ID to the end of a given URL defined in a Git instance. The **Git Branch**, **Git Tag**, and **Git Commit ID** fields have been removed from the Git instance UI.

Up to 50 repositories can be specified in a single Git SCM instance. All the repositories listed must use the same set of user credentials.

For complete details about this new feature, refer to “Git Configuration” in the “Integrating with Source Code Management” section in the *Code Insight User Guide*. This section also describes how pre-2023 R2 SCM Git instances are migrated to the current Code Insight release.

This new option to support multiple URLs in an Git SCM instance has also been added to the **sourceCodeManagement** REST interface. See [Updates to Existing APIs](#).

User Experience

This release includes the following enhancement to overall user experience.

Performance Improvements for the Code Insight Dashboard

The loading time of the Code Insight dashboard has been improved by excluding the file counts for unsuccessful scans and remote scans from the **scanned** file totals on the dashboard. However, as before, users can always view the file total for all scans—successful and failed per the Scan Server *and* remote scan plugins—at the project level by accessing the project dashboard or the **Analysis Workbench**.

REST API Enhancements

This release includes the following changes to the Code Insight REST interface.

- [New APIs](#)
- [Updates to Existing APIs](#)

New APIs

The following new APIs were added in this release.

Table 1 ▪ New APIs


Resource	API Name/Endpoint	Method	Function Change Description
Jobs	Export project inventory to SBOM Insights /jobs/sbomexport/{projectId}	POST	<p>Exports inventory data from the specified project to SBOM Insights. Once initiated, the export is scheduled in the Jobs queue. (The JobId is listed in the response.) To monitor the status of the job, use the jobs/{jobId} API.</p> <p>Only Project Analysts can perform this export.</p> <p>Calling this API requires that Code Insight and the project be properly configured to support exports to SBOM Insights. See Project Inventory Export to SBOM Insights for more information.</p> <div></div> <p>Note ▪ The export is not initiated (nor is a job added) if any of these jobs are already in progress or queued for the project: scan, rescan, Project Copy, or another SBOM Insights export.</p>
	Update project notices /jobs/notices/{projectId}	POST	<p>Automatically updates the notices text across inventory in a project. You can choose to update the notices text for all inventory (overwriting any existing notices text) or update only those inventory items that have no notices text assigned. See Automatic Update of Notices Across Inventory in a Project for more information.</p> <p>Once initiated, the update is scheduled in the Jobs queue. (The JobId is listed in the response.) To monitor the status of the job, use the jobs/{jobId} API.</p> <p>Project Analysts and Project Reviewers can perform a notices update through this REST API. (In the UI, only Project Analysts can perform the update.)</p> <div></div> <p>Note ▪ The notices update is not initiated (nor is a job added) if any of these jobs are already in progress or queued for the project: scan, rescan, Project Copy, Project Branch, or another notices update.</p>

Table 1 ▪ New APIs (cont.)

Resource	API Name/Endpoint	Method	Function Change Description
License	Update Licenses External Id /licenses/{licenseId}	PATCH	<p>Enables a Code Insight system administrator to map a specified license (identified by licenseId) to a corresponding ID in an external system (such as your site's license-tracking system). The following is an example request body identifying the external ID, which is a string value:</p> <pre>{ "externalId": "L156" }</pre> <p>For more information, see License Mapping to External IDs.</p>

Updates to Existing APIs

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

Table 2 ▪ Updates to Existing APIs

Resource	API Name/Endpoint	Method	Function Change Description
Component	Get Component /components/{componentId}	GET	<p>The response now includes the externalId property for a given license of a component version. This property shows the ID to which the license is mapped in an external system (such as your site's license-tracking system).</p> <p>For more information, see License Mapping to External IDs.</p>
Inventory	Get details of an inventory /inventories/{inventoryId}	GET	<p>The response now includes the externalId property for a given inventory license (selected or possible). This property shows the ID to which the license is mapped in an external system (such as your site's license-tracking system).</p> <p>For more information, see License Mapping to External IDs.</p>
Jobs	Get job details based on filters /jobs	GET	<p>The jobType filter in the request now supports the new Export to SBOM Insights and Update Notices job types, enabling you to filter the response to these jobs.</p>

Table 2 ▪ Updates to Existing APIs (cont.)


Resource	API Name/Endpoint	Method	Function Change Description
License	Create a custom license /licenses	POST	The request now includes the externalId property, enabling you to map the license being created to a corresponding ID in an external system (such as your site's own license-tracking system). The externalId property requires a string value. For more information, see License Mapping to External IDs .
	License Lookup /license/lookup	GET	The response now includes the externalId property for a given license. This property shows the ID to which the license is mapped in an external system (such as your site's license-tracking system). For more information, see License Mapping to External IDs .
	License lookup based on a short name /licenses/{shortName}		
Project API	Get Project Inventory /project/inventory/{projectId}	GET	The request includes a new filter includeFiles , which, when set to false , can improve the performance of this API when a large number of files are associated with project inventory.  Note ▪ This option can improve the performance of custom reports that call this API, such as the custom Project Vulnerability report available with Code Insight. For more information, see Performance Improvement for the Project Vulnerability Report . Also, the response now includes the externalId property for a given inventory license. This property shows the ID to which the license is mapped in an external system (such as your site's license-tracking system). For more information, see License Mapping to External IDs .
Rules	Create Rule /rules	Post	These APIs have been updated to support the option of using file or folder paths instead of MD5 values as criteria for detecting components based on the files associated with them. The fileInfo section (for the MD5 criteria) and the ruleInfo section (for file-path criteria) are mutually exclusive. For more information, see Custom Detection Rules Based on File Paths .
	Update Rule /rules	Put	
	Get Rule by Id /rules/{ruleId}	Get Rule by ID	

Table 2 ▪ Updates to Existing APIs (cont.)

Resource	API Name/Endpoint	Method	Function Change Description
sourceCode Management	scminstances /scminstances	GET	<p>As in previous releases, the response shows the properties used to connect to the different codebase repositories (across one or all SCM instances) to synchronize them to the Scan Server. The set of connection properties for each repository URL is listed in a separate “property block” (which includes the instanceID for the SCM instance in which the repository’s connection properties are configured).</p> <p>The slight difference in the response is that now repository URLs whose connection properties are configured within the same SCM Git instance will each have the same the instanceID value. This change supports the new feature Support for Multiple Repository URLs in a Single Git Instance.</p> <p>Additionally, if any URL in a Git SCM instance is defined with more than one delimiter (branch, tag, or commit ID), an error message similar to the following is displayed with status code 400. The message lists the URLs with the multiple delimited elements:</p> <pre>{ "errors": [{ "param": "[scmType: GIT; instanceId: 0; URL: https://github.com/sbn1/TestPublicRepo.git ~~master>>commit123, scmType: GIT; instanceId: 0; URL: https://github.com/ test/newtest^^tag123~~branchname]", "message": "Branch, Tag, Commit ID are mutually exclusive." }] }</pre>

Table 2 ▪ Updates to Existing APIs (cont.)

Resource	API Name/Endpoint	Method	Function Change Description
	scminstances /scminstances	POST	<p>The following revised or new error messages are displayed when a connection test for an SCM instance is unsuccessful.</p> <p>Testing Connections in an SCM Git Instance</p> <p>Previously, when the connection test for a given SCM Git instance was unsuccessful, an error message (with the status code 400) was displayed, stating that an error occurred connecting to the repository and that the connection properties needed to be checked. Now the following message (with the same status code) is displayed, identifying the one or more repository URLs to which Code Insight cannot connect. Multiple repositories are separated with commas. (The id value is the SCM instance ID.)</p> <pre>{ "errors": [{ "id": 0, "message": "Test connection failed for the following URLs: https://github.com/sbansal/ TestPublicRepo.git, https://github.com/ test/newtest" }] }</pre> <p>Testing the Connection in an SCM TFS Instance</p> <p>If users attempt to test a TFS instance connection when no TFS client is installed, the following error message is now displayed:</p> <pre>{ "errors": [{ "id": 0, "message": "com.palamida.plugin.prescan.api. PrescanPluginException: TFS client is not configured on scan server. Cannot run program \"tf\" (in directory \".\"):error=2, No such file or directory" }] }</pre>

Table 2 ▪ Updates to Existing APIs (cont.)

Resource	API Name/Endpoint	Method	Function Change Description
	Git scmInstances <code>/scminstances/Git</code>	POST	<p>The url property in the request to create an SCM Git instance now allows up to 50 comma-separated URLs. Additionally, you can add a single delimiter to the end of individual URLs to indicate a specific part of the repository with which to synchronize:</p> <ul style="list-style-type: none"> • To synchronize with a branch of the repository, add the branch name, using <code>~~</code> before the name. • To synchronize with a commit version of the repository, add the commit ID, using <code>>></code> before the ID. • To synchronize with a tagged part of the repository, add the tag name, using <code>^^</code> before the name. <p>The following URL example specifies a specific branch of the repository with which to synchronize:</p> <pre>https://github.com/scaqaadmin/ testgit_fnci.git~~dev-branch1</pre> <p>If only one URL is specified in the url field, you can alternatively specify the delimiter for the branch, commitID, or tag property in the request body. If multiple URLs are listed, a value specified for any of these properties is ignored.</p> <p>Validation of the URLs (including proper use of any delimiters) is performed during the connection test (POST scmInstances) or during synchronization.</p>
		PUT	<p>The update process of an SCM Git instance includes the same enhancements described previously for the POST Git scmInstances API. Ensure that you include the entire instance definition in the request body when making the updates. If the url property in the original instance definition includes multiple URLs, the url property in request body for the update must include all these URLs (except for those you are removing), even if you have not updated them.</p>

Resolved Issues

The following issues have been resolved in Code Insight 2023 R2 and its subsequent service packs:

- [Issues Resolved in 2023 R2 SP1](#)
- [Issues Resolved in 2023 R2](#)

Issues Resolved in 2023 R2 SP1

The following issues were resolved in the Code Insight 2023 R2 SP1 release.

Issue	Resolution Notes
SCA-43380	Previously, the Code Insights UI could take significant time to load the project tree. This process has now been optimized to provide faster load times.
SCA-44039, SCA-46489	The post-Electronic Update step, which processes new security vulnerabilities against inventory, could previously take up to 5 days or more to complete depending on the number of new vulnerabilities and the number of inventory items in the Code Insight instance. This issue has been addressed, as described in Enhancements to Processing Security Vulnerabilities in Post-Update Step .
SCA-48706	Code Insight reports generated using an HTTPS connection through Swagger or a cURL command were failing with a 500 status code. This issue has been resolved with the increase of the maxHttpHeaderSize default value from the 8192 to 16384 , defined in the server.xml file shipped with Code Insight.

Issues Resolved in 2023 R2

The following issues were resolved in the Code Insight 2023 R2 release.

Issue	Resolution Notes
SCA-37578	The Get Project Summary REST API previously returned the full license name instead of the expected SPDX identifier for the selectedLicenseSPDXIdentifier property. This issue has been resolved so that property now lists the SPDX identifier.
SCA-42215	The issue with project inventory missing from both the Inventory Items list in the UI and the Get Project Inventory REST API response has been resolved.
SCA-43347	The issue with inventory being associated with a component version different from the correct version (as listed in the requirements.txt file) has been fixed.
SCA-44064	The field Authentication Type has been added to the Jira ALM instance UI to address connection issues with the various types of Jira Server deployment. See New “Authentication Type” Field for Creating Jira ALM Instances for more details.
SCA-44325	An invalid user name provided in an ALM instance to access a Jira Server in the Atlassian Cloud was erroneously accepted as long as the provided Jira token was valid. Now, both the user name and token must be valid. Also see the previous issue SCA-44064 .
SCA-44554	Previously, the Code Insight UI for a project displayed inconsistent counts for files associated with project inventory. This has been corrected through improvements in the file-cleanup process.

Issue	Resolution Notes
SCA-46143	In previous releases, the generation of the Project Vulnerability custom report could take an extremely long time if inventory in the project was associated with a large number of files. A new option, Include associated files , has been added to the report's UI (and is predicated on the new includeFiles filter, which has been added to the Get Project Inventory REST API called by the report). When set to False , this option can improve performance when generating the report. See Performance Improvement for the Project Vulnerability Report .
SCA-46348	All folders explicitly specified for a scan agent plugin are now getting scanned. Previously, if multiple folders were listed, only the last folder was scanned.
SCA-46382	Steps in the <i>Code Insight Installation & Configuration Guide</i> describing how to migrate the Code Insight service have been updated to ensure 1) the previous Windows service has been removed and the new one installed and 2) proper Linux/Ubuntu permissions are in place to run <code>startup.sh</code> .
SCA-46490	The “underlying connection was closed” error that occurred during SCM synchronization with a TFS codebase has been resolved.
SCA-46733	The <i>Code Insight Installation & Configuration Guide</i> listed incorrect values for the minimum and maximum Tomcat JVM heap sizes required for running Code Insight as a Windows service. These values have been corrected.
SCA-46755	An input-string error when running the Get Project Information API is now resolved.
SCA-46788	The incorrect maximum packet-size value for MySQL listed in the <i>Code Insight Installation & Configuration Guide</i> has been corrected.
SCA-47320	In previous releases, the scan process on data synchronized to the Scan Server through a Git SCM instance could fail with a checkout error. This issue has been fixed.
SCA-47387	The decimal format and other numeric formats used in the Code Insight Audit report have been changed to the string format so that users in regions that use different decimal and numeric formats can successfully access the report.
SCA-47507	Security vulnerabilities that were introduced after an upgrade to 2023 R1 and that impact Apache Tomcat 8.5.84 and Commons-Fileupload 1.3.3 have been removed.

Known Issues

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

- [All-Project Inventory View](#)
- [Automated Workflow for Inventory Review/Publication](#)
- [Data Library and Electronic Updates](#)
- [Export and Import](#)
- [Installation, Upgrades, and Configuration](#)
- [Inventory History](#)
- [Manual Codebase Analysis](#)
- [Performance](#)
- [Project Inventory](#)
- [Project Management](#)
- [Project Reporting](#)
- [REST APIs](#)
- [Scan Agent Plugins](#)
- [Scanning and Automated Discovery](#)
- [Source Code Management \(SCM\) Support](#)
- [Vulnerability Suppression/Unsuppression](#)
- [Web UI](#)

All-Project Inventory View

The following are known issues in the **Inventory** view, which shows inventory across all Code Insight projects.

SCA-34403: Inventory details slide-out panel opening twice

When a user clicks an inventory item in the **Inventory** view, the panel showing the inventory's read-only details appears briefly on the right side of the view and then properly slides out from the right.

Workaround: None exists.

Automated Workflow for Inventory Review/Publication

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

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.

Data Library and Electronic Updates

The following are known issues related to the Code Insight data library and the Electronic Update, which keeps Code Insight systems up to date with the latest data-library information.

SCA-43625: Server shutdowns when simultaneous custom-component indexing and searching occur

As of 2022 R4, Code Insight starts the background process of indexing a custom component in the Code Insight data library as soon as the component is created or updated. Even though indexing takes only a half minute or less per component, a server shutdown can occur if you attempt to perform a component search against the data library while multiple components are being simultaneously indexed.

Workaround: Wait until the indexing process is finished for all components before you use the Global Component & License Lookup feature or the **Component Search** REST API to search components in the data library.

SCA-43568: Sequential creation of multiple custom components with similar names resulting in incorrect component search counts and pagination

As of 2022 R4, Code Insight starts the background process of indexing a custom component in the Code Insight data library as soon as the component is created or updated. If multiple custom components with similar names are sequentially created/updated and indexed in the background, the search results for these components might show incorrect search counts and pagination.

Workaround: After the custom-component updates are indexed, run an Electronic Update to fix the indexes.

SCA-40194: Duplicate inventory issues for MIT-related components

The Code Insight MIT data-library update does not fix inventory items with names that include multiple licenses separated by commas (instead of ORs), as shown in this example:

```
jquery (MIT, MIT License)
```

On a rescan, duplicates can be created for such inventory items:

jquery (MIT, MIT License)

jquery (MIT)

Two possible workarounds are available.

Workaround 1: Before starting the rescan, select the option **On data import or rescan, delete inventory with no associated files** on the **Manage Project > Edit Project > General** tab accessed from the project's **Summary** tab. This option deletes the original inventory item as long as it is system-generated.

Workaround 2: Manually delete the original inventory item in the **Analysis Workbench** by right clicking the item and selecting **Delete inventory**. You must repeat this step for each such inventory item.

SCA-31562: Component license remapping issues from MIT-Style to MIT for inventories

Remapping issues have occurred with Electronic Updates since Code Insight 2021 R4. These issues involve the remapping of licenses from MIT-Style to MIT for inventories. The next two sections combined illustrate a typical remapping issue.

Before running the Electronic Update available at the release of Code Insight 2021 R4 and later:

The following inventory mapping existed in inventory:

concurrent-ruby 1.1.9 (MIT License)

This component was mapped with License id 744.

After running the Electronic Update available at the release of Code Insight 2021 R4 and later:

The inventory item was remapped as follows:

concurrent-ruby 1.1.9 (MIT-Style)

The license short name had been changed (in this example, from MIT License to MIT-Style). However, the mapped license ID remained 744.

Ideally this component should be remapped to MIT, which is License id 7.

Workaround: Follow these steps:

1. Click **Inventory** on the main Code Insight window to open the **Inventory** view, showing inventory across projects.
2. Switch from **My Projects** to **All Projects**.
3. Search for the inventories containing the string *(MIT-Style)*.
4. Locate the **Possible Licenses** value for a given inventory. If this value is **MIT** (Id 7) *and* the term *MIT-Style* is in the inventory name or is the value of **Selected License**, then an incorrect license remapping has been performed for this specific inventory item. One incorrect license remapping is a possible indicator of other incorrect remappings.
5. Run the Code Insight cleanup SQL script to correct the license mappings for the inventory in your Code Insight system. (To obtain this script, download the codeinsight-MITCleanupPackage archive from the Product and Licensing Center, and extract the script and its instructions.)

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, Upgrades, and Configuration

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

SCA-35918: Upgrades to Code Insight possibly more time-consuming than previous upgrades

Upgrading to Code Insight might take longer than previous upgrades, especially if the number of inventory items in your Code Insight system has increased since the last upgrade. For example, an upgrade for a system with about 1 million inventory items can now take around 15-20 minutes, which might be longer than your previous upgrades. The extra time needed for the upgrade is due the **Inventory History** feature (introduced in 2021 R3), which requires that the inventory items for all projects be processed for inclusion in the history.

Note, however, that once an inventory item is included in the history, it does not need to go through this initialization process in subsequent upgrades.

Workaround: None exists. If you have any concerns about the time taken for this process, contact Reverera Support for assistance.

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. 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 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 results in an error.

If this blocking 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>.)

Inventory History

The following are known issues with the Inventory History feature.

SCA-36420: Inventory URL and Description attributes shown as updates in Inventory History without their being modified

After an initial transaction is performed against an inventory item (such as editing or viewing the item), entries for the **URL** and **Description** properties are displaying in the **Inventory History** window even though these properties were never modified as part of the transaction. These two initial entries will remain in the history. However, any future transactions against the inventory item will not create an update entry for the **URL** or **Description** property unless the value for either property has actually changed.

Workaround: None exists.

Manual Codebase Analysis

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

SCA-46104: Not able to retrieve Advanced File Search results when using same criteria but with distinct values and AND logic

The Advanced File Search feature does not retrieve the expected results when you define a filter using multiple criteria that are the same (but with a distinct value for each criterion) and apply AND logic to the criteria. Files known to meet all the specified criteria are not listed in the **File Search Results** pane.

SCA-44366: Error thrown when navigating file search results

When you use the **Enter search string...** field at the top of the **Codebase Files** pane to search for files by name, you can use the Next or Previous button adjacent to the field to navigate to the search results highlighted in the codebase tree. However, if you click these buttons a rapid pace, you can generate an error (although the UI does not hang).

Workaround: Click the buttons at a slower pace.

SCA-41440: “Show File Evidence” right-click option on “File Search Results” pane not working at node, folder, and sub-folder levels

When you right-click an alias node, codebase node, folder, or sub-folder in the **File Search Results** pane in the **Analysis Workbench**, and then select **Show File Evidence**, the **Evidence Details** tab on the right displays the message “No Evidences found”.

However, when you select **Show File Evidence** at the file level in the **File Search Results** pane, the evidences properly are listed on the **Evidence Details** tab as expected.

This behavior occurs whether the files were scanned by a Scan Server or a scan-agent plugin.

Workaround: None exists.

SCA-41964: Empty results when Advanced Search with “File Path” criterion attempts to fetch 2000 or more results

An **Advanced Search** using the **File Path** criterion can produce empty results in the **Analysis Workbench** if the search attempts to retrieve 2000 or more results. This issue can occur whether searching a file system scanned by a remote scan agent or a codebase scanned by a Scan Server.

This issue does not occur when the search fetches less than 2000 results.

Workaround: None exists.

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 Inventory

The following are known issues with the review process for Code Insight project inventory.

SCA-44107: Unable to delete an inventory item with a large number of associated files

Attempts to delete an inventory item associated with a large number files (50KB or more) can fail.

Workaround: None exists.

SCA-44077: Deletion of a top-level inventory item causing deletion of dependency inventory

When a user deletes a top-level inventory item, all of its dependent inventory items are also deleted.

Workaround: None exists.

SCA-41263: License text shown twice in As-Found License Text field in Analysis Workbench

In the **Analysis Workbench**, the text for a license can be repeated twice for some components (such as the component glob) when the license file contains more than one license.

Workaround: None exists.

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 selected, but policies are 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 Management

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

SCA-41957: Project Copy performance slower when the Code Insight database resides on a separate machine

Processing time for Project Copy increases when the Code Insight database resides on a machine different from the machine where the Core Server resides. Project Copy processing is most efficient when the Core Server, Scan Server, and database reside on the same machine.

Workaround: None exists.

SCA-41862: Increased time for Project Copy and other operations when Project Copy runs in parallel

If a Project Copy is triggered when any other operation—such as an import, export, scan, or report generation—is also running in your Code Insight system, the processing time for the Project Copy as well as for the other operation (especially an import, export, or scan) will be relatively greater than if these operations were run at separate times.

Workaround: In general, perform the listed operations at separate times for better performance. Ensure that Project Copy does not run in parallel with any of these operations.

SCA-41682: Project dashboard of copied project shows both Scanner and Remote Scans sections even though source project was only remotely scanned

The project dashboard of the copied project shows both Scanner and Remote Scans sections info even though the source project was scanned by a scan agent only. Only the Remote Scan section should be displayed.

Workaround: None exists.

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.

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.

Scan Agent Plugins

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

SCA-48543: Unable to install Jenkins scan-agent plugin on Jenkins Server

The Code Insight Jenkins scan-agent plugin requires certain Jenkins dependency plugins that Jenkins automatically installs before the scan agent is installed. Jenkins will download only those dependency plugin versions that are compatible with the baseline-support version of the Jenkins Server (currently, 2.332.1). For example, Jenkins will download the **Pipeline: Groovy** dependency version that has been updated to support Jenkins Server 2.332.1 or later.

Consequently, if you are running a pre-2.332.1 Jenkins Server, some of the downloaded dependencies might be incompatible your server version, causing the Jenkins scan-agent plugin installation to fail. In this situation, consider migrating the server to version 2.332.1 or later. If migration is not feasible, you must manually install an older version of the dependency plugins that is compatible with your server version. For the list of required dependency plugins for the Jenkins Server, refer to the [Plugins Index](#) on the Jenkins site.

SCA-46097: Docker Images name with “/” causing scan to fail

A Docker Images plugin scan on a Docker image fails if the image name contains a forward slash (/), but the command that runs the scan does not include a valid tag for the name.

Workaround: If the Docker image name contains a forward slash, be sure that the command that runs the scan includes a valid tag for the image name. The following example command illustrates the correct <name>:<tag> format required in the command:

```
./code-insight-docker-plugin.sh -image alpinelinux/darkhttpd:latest
```

In the example, **alpinelinux/darkhttpd** is the image name containing a forward slash, and **latest** is the added tag (preceded by a colon).

SCA-44239: Delta file calculation during rescan not synchronized with scan

The Docker Images plugin can sometimes acknowledge files that have not changed since the previous scan as changed in the rescan. This error can impact scan time.

Workaround: None exists.

SCA-44209: Associated files not available in Syft findings for Docker Images plugin scans on Centos

File associations are not available for inventories reported by Syft during a Docker Images plugin scan on a Centos agent machine. This issue does not occur for scans performed by the same plugin on RedHat Enterprise Linux and Ubuntu machines.

Workaround: None exists.

SCA-44073: Invalid file association for transitive dependencies generated from go.sum

During a transitive scan, inventory generated from the go.sum file can have an invalid association to go.mod.

Workaround: None exists.

SCA-43034: No valid error message for scan failure when using current plugin with older Code Insight release

A current scan-agent plugin is not compatible with an earlier Code Insight release. Therefore, any attempt to run a scan-agent plugin with a Code Insight release previous to the plugin release results in failure. However, no appropriate message for this type of failure is provided.

Workaround: None exists.

SCA-42606: Seemingly “Successful” completion of Docker plugin scan despite errors

A Docker plugin scan can fail on a codebase/artifact system containing large archive files but a small /tmp partition. However, the scan status can still show “SUCCESS” (although the agent log might record the error that caused the failure).

Workaround: None exists.

SCA-41197: SHA-1 calculated for only files scanned during agent rescans subsequent to re-enablement of SHA-1

When SHA-1 is disabled and then re-enabled, any subsequent rescan by a scan agent calculates a SHA-1 value for only those files that are scanned (that is, updated or new files). SHA-1 is not calculated for those files that are skipped by the scan because they remained unchanged since previous scan.

Workaround: None exists.

SCA-41154: No scan agent support for full rescans

Prior to Code Insight 2022 R2, scan agents plugins performed only full scans. Starting 2022 R2, scan agents now support *only* incremental rescans. After the scan agent’s initial full scan of a file system, any subsequent rescans are incremental only; no forced full rescans are supported. However, a full rescan should automatically occur whenever Automated Analysis rules change, a new Code Insight version introduces new rules or data library changes, or the scan-profile settings change. Currently, no logic exists to support such an automatic full rescan when these conditions exist.

Workaround: None exists.

SCA-40626: I/O exception during Jenkins plugin scan after deletion of “.codeinsight” folder from Jenkins agent

Users can delete the .codeinsight folder from the Jenkins agent if needed. However, once the folder is deleted, scans scheduled for the Jenkins plugin might fail with an I/O exception.

For your reference, this folder is identified as \$user_dir.codeinsight, where \$user_dir is as follows:

- /home/<user>/ on Linux
- C:/Users/<user>/ on Windows

Workaround: Restart the Jenkins server.

SCA-38346: NVD calls are not going through proxy for plugin scans

When a proxy is enabled for the generic scan-agent plugin or the Jenkins plugin, NVD calls bypass the proxy during scans.

Workaround: None exists.

SCA-33465: Scan agent inventory results impacted when CODEINSIGHT_ROOT variable set to wrong path

A scan agent can produce different inventory count results when the CODEINSIGHT_ROOT variable is set as environment variable and defined with an incorrect path compared to when the variable is set to the correct path or simply not used as an environment variable. (The scan agent does not require CODEINSIGHT_ROOT to be set as an environment variable.)

Workaround: If you are running the scan agent on the same machine as Code Insight Core Server, determine whether CODEINSIGHT_ROOT has been set as environment variable. If it has, ensure that it points to the correct path. Otherwise, do not set CODEINSIGHT_ROOT as an environment variable.

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 an upgrade to a Jenkins scan-agent plugin, a downgrade button option is available in the Web UI. Clicking on the option results in a 404 error.

Workaround: None exists.

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

For scan agent plugins not updated from 1.x (supports only legacy inventory-only projects) to 2.x, the scan results might show published inventory items that have no associated licenses. This occurs when the scan agent finds no license evidence in the codebase files or when Code Insight is able to map to the component, but multiple licenses are associated with it. In this case, the inventory item is created using Compliance Library data. It might show one or more *possible* licenses but most likely no selected license. Since the **Analysis Workbench** is not available for the legacy “inventory only” plugins, the user cannot not resolve the license issue.

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

Scanning and Automated Discovery

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

SCA-48341: Scans on Windows Server platform hang when codebase contains linux.tar files

When a Scan Server that runs on a Windows Server platform scans a codebase containing `linux.tar` files, the scan can hang indefinitely unless you stop and restart Tomcat.

Workaround: Perform *one* of these options before scanning the codebase:

- Untar the `linux.tar` file and archive the resulting folder in a zip file. Then replace the `linux.tar` file with the zip file in the codebase and upload the codebase to the Scan Server.
- In the scan profile, use a pattern to exclude the impacted files, `aux.c` and `aux.h`, from the scan, as shown in this example:

```
**/i2c/aux.c  
**/i2c/aux.h
```

See the “Creating Exclusion Patterns for Scan Profiles” section in the *Code Insight Installation and Configuration Guide* for more information about setting up file exclusions.

SCA-44154: Transitive dependencies not reported for golang.org/x/tools module

During a transitive scan of the tools module `golang.org/x/tools`, the Go Analyzer reports no inventory.

Workaround: The next Electronic Update will resolve this issue.

SCA-43792: Issue with Go module inventory names when associated component URL has a version suffix

When a discovered component in a Go module has a `/v<digit>` suffix in its URL, the inventory name is displayed as simply **v<digit>** in the Code Insight UI and API responses. For example, if the URL for the `blackfriday` component is `github.com/russruss/blackfriday/v2`, its inventory name is displayed as **v2**, instead of **blackfriday**.

Workaround: None exists.

SCA-43659: Security vulnerabilities not reported for Go components

Scans on Go packages are not reporting security vulnerabilities for Go components.

Workaround: None exists.

SCA-43103: Files with path change but same MD5 still being rescanned

Files whose path has changed but whose MD5 remains the same are still being rescanned even those the project's scan profile is configured *not* to rescan unchanged files.

Workaround: None exists.

SCA-34070: 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.

Source Code Management (SCM) Support

The following are known issues with Code Insight SCM support.

SCA-48045: scmInstances GET API not returning all URL details when any Git URL has multiple delimiters

Currently, if the scope for the **scmInstance** GET API includes at least one Git SCM instance with a repository URL that is defined with more than one delimiter (branch, tag, or commit ID), an error message similar to the following is returned. The message (with the status code 400) lists those Git URLs defined with multiple delimiters in the instance.

```
{
  "errors": [
    {
```

```

    "param": "[scmType: GIT; instanceId: 0; URL: https://github.com/sbni/
    TestPublicRepo.git~master>>commit123, scmType: GIT; instanceId: 0; URL: https://
    github.com/test/newtest^^tag123~branchname]",
    "message": "Branch, Tag, Commit ID are mutually exclusive."
  }
]
}

```

When this message is returned, details are not returned for repositories of the other URLs in the same Git SCM instance, nor are they returned for the repositories identified in the other SCM instances of any type in the project.

The missing details for the other URLs in the Git SCM instance as well as for the other SCM instances makes it difficult to obtain the information needed to update a given instance. (The request body for the PUT method requires the complete updated definition of the SCM instance.)

Workaround: When creating or updating a Git SCM instance, provide only one delimiter per URL in a Git SCM instance. Additionally, use the Code Insight UI to update SCM instance and retrieve their details.

SCA-47353: Unhelpful message when testing or synchronizing with invalid or missing credentials

When you attempt to test the connections for a specific SCM instance (or run a synchronization across all SCM instances in a project) *and* the connection credentials are invalid or missing for any instance, a message with an unhelpful error description is displayed.

Workaround: Refer to the core or catalina logs for an accurate description of the error.

SCA-46441: TFS repository failing to synchronize

The synchronization between a TFS codebase repository and a Code Insight project can fail even though the TFS instance connection is configured correctly (with a valid URL, user name, password, and other properties) in the project.

Workaround: On the **Version Control Settings** tab for the project, provide a personal access token (PAT) in the **Password** field instead of a password to enable successful synchronizations.

SCA-40067: SCM instance numbering systems used in REST API output and Web UI not in sync

The instance Ids shown in the **GET SCM Instance** API response are not in sync with SCM instance numbers generated in the Web UI.

Workaround: None exists

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.

Vulnerability Suppression/Unsuppression

The following are known issues with the Vulnerability Suppression/Unsuppression functionality.

SCA-37089: Unable to suppress/unsuppress a vulnerability for more than 2097 versions of a component all at once (in a SQL Server environment)

When a user attempts to suppress or unsuppress a security vulnerability for more than 2097 versions of a component all at once (using the **All Current Versions** scope or the **Specified Versions** scope with more than 2097 entries), the operation fails with an appropriate error message. This same problem occurs when running the **Suppress vulnerability** or **Unsuppress vulnerability** REST APIs.

This issue occurs only when the Code Insight database is SQL Server.

Workaround: Suppress or unsuppress the vulnerability using the **Specified Versions** scope with fewer entries. Repeat this operation until the vulnerability has been suppressed or unsuppressed for all desired versions.

SCA-36973: Open alert counts not automatically refreshed after vulnerability suppression

After a security vulnerability is suppressed for a component version with open an open alert associated with the vulnerability, the open alert count is not automatically refreshed to show the reduced count in the Code Insight Web UI.

Workaround: Manually refresh the browser screen.

SCA-36768: “Vulnerabilities” bar graph not automatically refreshed after vulnerability suppression

After a security vulnerability is suppressed for a component version, the count in the appropriate “severity” segment of the **Vulnerabilities** bar graph for the component version is not automatically reduced.



Note ▪ The issue has been fixed for the bar graph on the **Inventory** view and **Project Inventory** tab. However, the issue has not been fixed for the bar graph displayed in other locations.

Workaround: Manually refresh the browser screen.

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.

Workaround: None exists.

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 © 2023 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.