Code Insight 2022 R4 Release Notes

November 2022

Introduction

These Release Notes provide the following information about the Code Insight 2022 R4 release:

- About Code Insight

- Revenera Resources

- 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.

Revenera 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 Revenera 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 Revenera's product solutions, you can access forums, blog posts, and knowledge base articles.

- You can find documentation for Code Insight and all other Revenera products on the Revenera Product Documentation site.

- The Revenera Learning Center offers free, self-guided online videos to help you quickly get the most out of your Revenera 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 Revenera Community.

  https://community.revenera.com

New Features and Enhancements

The Code Insight 2022 R4 release provides new features and enhancements in the following areas:

- Data Library

- Installation, Upgrades, and Configuration

- Project Inventory

- Scan Agent Plugins

- Scanning and Automated Discovery

- REST API Enhancements

Data Library

The following is a new enhancement to the functionality that enables users to update the Code Insight data library with custom components and licenses that represent OSS, third-party, and commercial software entities not found in the library.

Immediate Indexing of Custom Components in Data Library

Newly created custom components or updates to an existing custom component updates are saved immediately to your Code Insight database. However, until this release, the process of indexing a new or updated custom component in the Code Insight data library was performed only during an Electronic Update. Consequently, the custom component or its updates were not globally available for user searches (through the UI or REST API) against the data library until the Electronic Update occurred.

In this release, the process of indexing a new or updated custom component begins in the background as soon as the component is created or updated. Indexing takes only a half minute or less per component. (However, to avoid issues, you are advised to wait until the indexing is finished before using the Global Component & License Lookup feature or the **Component Search** REST API to search components in the data library.)

For more information, refer to the "Creating a Custom Component" section in the *Code Insight User Guide*.

Installation, Upgrades, and Configuration

The following enhancement is now available for Code Insight installation, upgrade, and configuration processes.

Documentation for Code Insight Upgrades in Offline Environments

The user documentation describing how to upgrade to a new version of Code Insight has been enhanced with instructions on performing this process in an offline environment. You can find this new information in the "Upgrading Code Insight" chapter in the *Code Insight Installation & Configuration Guide*.

Project Inventory

The following enhancement is now available for managing and reviewing inventory in the **Analysis Workbench** or on the **Project Inventory** tab or in both locations.

Advanced Search for Inventory in Analysis Workbench

The Advanced Inventory Search feature is now available for inventory in the **Analysis Workbench**. Previously this feature was available for only project inventory.

The Advanced Inventory Search feature enables you to filter the list of inventory items to those of interest based on many available criteria—inventory attributes, selected license attributes, and associated security vulnerabilities, tasks, security alerts and more. The search enables you to refine the inventory list to only those inventory items in which you are interested.

Scan Agent Plugins

The following enhancement is now available for one or more of the Code Insight scan-agent plugins.

Syft Integration in the Dockers Images Plugin

Syft, an open-source scanning tool, is now integrated in the Code Insight Docker Images plugin. This tool generates a Software Bill of Materials (SBOM) from the discovery of packages and libraries in container images, file systems, archives, and other artifacts. Its integration with the Docker Images plugin enables the plugin to report findings from Docker images containing Alpine, RPM, and Debian Linux distribution packages that reside in RedHat Enterprise Linux, Ubuntu, and CentOS Linux operating systems. See the following sections for more details:

* Supported for Package Forges

* Inventory Detection Notes

Also see the Scan Agent Plugins section in these Release Notes for known issues related to the Syft integration in the Docker Images plugin.

For instructions on using the Docker Images plugin, see "Docker Images Plugin" in the *Code Insight Plugins Guide*.

Supported for Package Forges

The following table shows the supported forges (by package type) for inventory detected by Syft.

Table 1 ▪ Forge Support

Package	Forge Support for Inventory
RPM	Inventory items are associated with components from the following forges: • centos • fedora • gnu • fsf • github • savannah If the component is not found in any of these forges, a custom component is created for the inventory item.
Alpine	Inventories are associated with components from the following forges: • Alpine[*] • centos • fedora • gnu • github If the component is not found in any of these forges, a custom component is created for the inventory item.
Debian	Library collection is currently not available for Debian packages. All inventories detected in this package type are associated with a custom component.

[*] Support for the Alpine forge is planned to begin with the Code Insight Electronic Update in November 2022.

Inventory Detection Notes

An inventory item discovered by the Syft detection process shows the following system-generated content in the **Notes** field for the inventory item:

```
Detected By: SyftParser
Attributes:
Source: Syft parser attribute
   This item is created as per scan data from Syft
```

The **Notes** field can include other Syft parser attributes as well, as shown in this example:

Scanning and Automated Discovery

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

Enhancements to Go Package Discovery

Code Insight now supports the discovery of transitive dependencies in Go modules (as found in the `go.sum` file).

REST API Enhancements

The following new REST APIs were added in this release:

Table 2 ▪ New APIs in this Release

Resource	API Name/Endpoint	Method	Description
Jobs	**Get All Job Details** `/jobs/all`	GET	Retrieves details for all jobs, currently running and historical. The details include the current job status and the timestamps indicating when the job was queued, when it was activated, and when it completed. (No time estimates are provided for how long a job will be in queue or when it will complete.) Supported job types include: ● Project branching ● Project copying ● Project scan and re-scan ● Electronic Update (PDL update) ● Data garbage collection (cleanup after the deletion of project or scan folders) ● Report generation (Audit, Notices, Project, or custom reports)
	Get Job Details Based on Job Id Provided `/jobs/{jobId}`	GET	Provides the status and details for a given job, identified by its ID. (You can obtain the job ID by calling the **Get All Jobs** REST API.)

Resolved Issues

The following issues are resolved in this release.

Issue	Resolution Notes
SCA-13558	When an inventory item is associated with 4000 or more files, SQL Server no longer throws an exception when users attempt to add and view the files for the item.
SCA-40410	Global component searches through the Code Insight UI and REST API are now fetching information about new and updated custom components. Previously, users had to wait until an Electronic Update to fetch this information. See Immediate Indexing of Custom Components in Data Library.

Issue	Resolution Notes
SCA-41692	The Component Lookup search by URL was previously producing different results when the user tried various combinations of upper and lower case in the same search string. The URL search is now case-insensitive. No matter what case is provided in the search string, the results include all components containing the string.
SCA-42991	The `core.update.log` file no longer erroneously includes additional information from `core.log`.
SCA-43141	All audit records for a deleted inventory item are now deleted from the Code Insight database.
SCA-43238	The maximum length for project names is now 256 characters. Previously, SQL Server would not accept more than 60 characters for the name. Both SQL Server and MySQL now support this new maximum.
SCA-43145	Previously, associating or disassociating a file for an inventory item was creating an audit record. (No audit record should be created for this event.)
SCA-43256	Previously in Go modules, projects were not detected as top-level inventory, resulting in their first-level dependencies not being reported. As a fix, the scan now creates an unpublished 'Work in Progress" inventory item for any project in these modules, enabling its first-level dependencies to be reported.
SCA-43346	When the PyPI analyzer searched dependencies in the `requirements.txt` file, those dependencies that contained an inline comment (along with a version) were reported without versions in the scan results. This issue is now fixed so that versions are reported.
SCA-44158	Previously during a Project Copy, symbolic links in a codebase caused issues, such as recursive behavior that consumed the hard drive. The Project Copy process now ignores symbolic links.

Known Issues

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

- All-Project Inventory View

- Application Life Cycle Management (ALM) Support

- Automated Workflow for Inventory Review/Publication

- Data Library

- 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.

Application Life Cycle Management (ALM) Support

The following are known issues with Code Insight ALM support.

SCA-44325: Invalid user name accepted in ALM instances configured for Jira in the Cloud

Even though an invalid user name is used in an ALM instance configured for a Jira server in the Atlassian Cloud, the user is still able to connect to the Jira server as long as the API token in the instance is valid. This issue occurs because credential validation in a Cloud-based Jira server is performed against the token only.

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

The following list the known issue related to the functionality that enables users to update the Code Insight data library with custom components and licenses that represent OSS, third-party, and commercial software entities not found in the library.

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.

Electronic Updates

The following are known issues with the Code Insight Electronic Update and related data library updates.

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 once the latest Electronic Update (available from Code Insight 2021 R4 and later) has been run. These issues involve the remapping of licenses from MIT-Style to MIT for inventories. The following is an example.

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 Revenera 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 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 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 results 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.)

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-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-32546: Marking codebase files as reviewed/not reviewed in batch or rapid succession causing the UI to hang

In the **Analysis Workbench**, when users mark multiple codebase files as reviewed or unreviewed in a batch or individually in rapid succession, the Code Insight UI might hang. This issue occurs whether you are selecting files in the **Codebase Files** pane or in the **File Search Results** pane (both on the left side of the **Analysis Workbench**). The call to change the review status of any number of files involves the processing of evidence for all files, an event that can significantly increase response time and cause the UI to hang. A fix to this problem is underway. In the meantime, the following workaround is available.

Workaround: Before selecting files to mark as reviewed or unreviewed, click the **Evidence Details** tab in the middle pane of the **Analysis Workbench**. From this tab, select **Filter to selected files**. Also ensure that all evidence types are selected in the **Select Evidence Types** dropdown list. Then proceed to mark the codebase files as reviewed/unreviewed. This workaround reduces the time to obtain a response because it filters the evidence to be processed to that belonging to the selected files only.

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-44421: Some previously published inventory showing as unpublished

When a server undergoes a "mini" Electronic Update (that is, when certain data, not a full update, is pushed), some inventory associated with DLL and TAR files no longer match exact components in the Code Insight data library. Consequently, these inventory items are reverted to "unpublished".

Workaround: This issue will be resolved in the next full Electronic Update.

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 "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-44189: Parallel deletion of projects causing deadlock exception

The deletion of projects in parallel can cause a deadlock exception, resulting in no project deletion.

Workaround: Delete projects one at a time.

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 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 hows 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. 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-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-44030: Increased scan times for Docker Image plugin in 2022 R4

Starting in 2022 R4, the scan times for the Docker Image plugin have doubled when compared to the scan times in 2022 R3. This increase in scan time is due in part by the extra processing incurred by Syft findings and by enhancements to the component-matching process.

Workaround: None exists.

SCA-43034: Inappropriate 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, an appropriate message for this type of failure is not 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 scanned files 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.

Scanning and Automated Discovery

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

SCA-44372: Incorrect licenses detected for certain components

Incorrect licenses are detected for some components during scans.

Workaround: The next Electronic Update will resolve this issue.

SCA-44290: Incorrect URL displaying for certain newly added components

The URL displayed for some newly added components is incorrect and will show a 404 error when you click the its link.

Workaround: The next Electronic Update will resolve this issue.

SCA-44154: Transitive dependencies not reported for goland.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-42588: Direct dependencies without version in pom files not reported for scans enabled for transitive dependencies

Direct dependencies that are found in pom files but that have no version are not being reported during scans enabled for transitive-dependency reporting.

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.

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 Code Management (SCM) Support

The following are known issues with Code Insight SCM support.

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.

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

Intellectual Property

Restricted Rights Legend