

# Code Insight 2025 R2 Release Notes

May 2025

<b>Introduction .....</b>	<b>3</b>
<b>About Code Insight .....</b>	<b>3</b>
<b>Revenera Resources .....</b>	<b>3</b>
<b>New Features and Enhancements.....</b>	<b>4</b>
Advanced Inventory Searches.....	4
Alert Management.....	5
Components and Licenses .....	5
Installation, Upgrades, and Configuration.....	7
Jobs Queue .....	8
Scanning and Automated Discovery .....	9
Security Vulnerability Reporting .....	11
Source Code Management (SCM) Support .....	12
Vulnerability Management.....	13
Web UI.....	13
REST API Enhancements.....	14
Updates to Existing APIs .....	15
<b>Resolved Issues.....</b>	<b>17</b>
<b>Known Issues .....</b>	<b>17</b>
Advanced Inventory Searches.....	18
Alert Management.....	18
All-Project Inventory View .....	19
Automated Workflow for Inventory Publication and Review .....	19
Custom Detection Rules .....	20
Data Library, Library Refreshes, and Electronic Updates .....	20
Export and Import.....	22
Installation, Upgrades, and Configuration.....	23
Inventory History .....	24
Manual Codebase Analysis .....	25
Performance .....	27
Project Inventory .....	27
Project Management .....	29
Project Reporting .....	29
REST APIs .....	30
Scan Agent Plugins.....	31
Scanning and Automated Discovery.....	35
Source Code Management (SCM) Support .....	41

Vulnerability Suppression and Unsuppression .....	42
Web UI .....	45
Code Insight Security Issues .....	46
<b>Legal Information .....</b>	<b>47</b>

# Introduction

These Release Notes provide the following information about the Code Insight 2025 R2 release:

- [About Code Insight](#)
- [Reverera 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.

## 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 [Support Hub](#) page of the [Reverera Community](#).

# New Features and Enhancements

The Code Insight 2025 R2 release and its subsequent service packs offer new features and enhancements in the following areas:

- [Advanced Inventory Searches](#)
- [Alert Management](#)
- [Components and Licenses](#)
- [Installation, Upgrades, and Configuration](#)
- [Jobs Queue](#)
- [Scanning and Automated Discovery](#)
- [Security Vulnerability Reporting](#)
- [Source Code Management \(SCM\) Support](#)
- [Vulnerability Management](#)
- [Web UI](#)
- [REST API Enhancements](#)

## Advanced Inventory Searches

The following enhancement has been added to the Advanced Inventory Search feature (available on the **Project Inventory** tab and in the **Analysis Workbench**).



**Note** - For more information, refer to [Advanced Inventory Search Dialog](#) in the Code Insight User Guide.

- [Support for Filtering Inventory Items Based on Known Exploited Vulnerabilities](#)

### Support for Filtering Inventory Items Based on Known Exploited Vulnerabilities

Code Insight introduces a new field named **Show KEV inventories** in the **Security Vulnerabilities** section of the **Advanced Inventory Search** dialog that enables you to filter the list of inventory items based on the Known Exploited Vulnerabilities (KEVs) associated with the inventory items. You can select one of the following options from the **Show KEV inventories** field dropdown list:

- **Yes**—Selecting this option filters the inventory items to display only those associated with at least one known Exploited Vulnerability (KEV).
- **No**—Selecting this option filters the inventory items to display only those that are not associated with any Known Exploited Vulnerability (KEV).
- **Any**—Selecting this option displays all inventory items associated with security vulnerabilities, regardless of the Known Exploited Vulnerability (KEV) status.

The following displays the **Show KEV inventories** field in the **Security Vulnerabilities** section of the **Advanced Inventory Search** dialog box:

## Alert Management

This release includes the following enhancement to the management of security vulnerability alerts:

- [Enhanced Handling of Security Vulnerability Alerts in Project Copy](#)

### Enhanced Handling of Security Vulnerability Alerts in Project Copy

Previously, when a project was copied, all security vulnerability alerts (with the **Open** or **Closed** status)—associated with inventory items—were copied from the source project to the target project. Additionally, all copied security vulnerability alerts were automatically set to the **Open** status in the target project.

Starting in this release, Code Insight refines the project copy process by allowing only security vulnerability alerts with the **Open** status—associated with inventory items—to be copied from the source project to the target project. All security vulnerability alerts with the **Closed** status are no longer included in the project copy process.

This enhancement ensures that only relevant, actionable security vulnerability alerts are copied.

## Components and Licenses

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

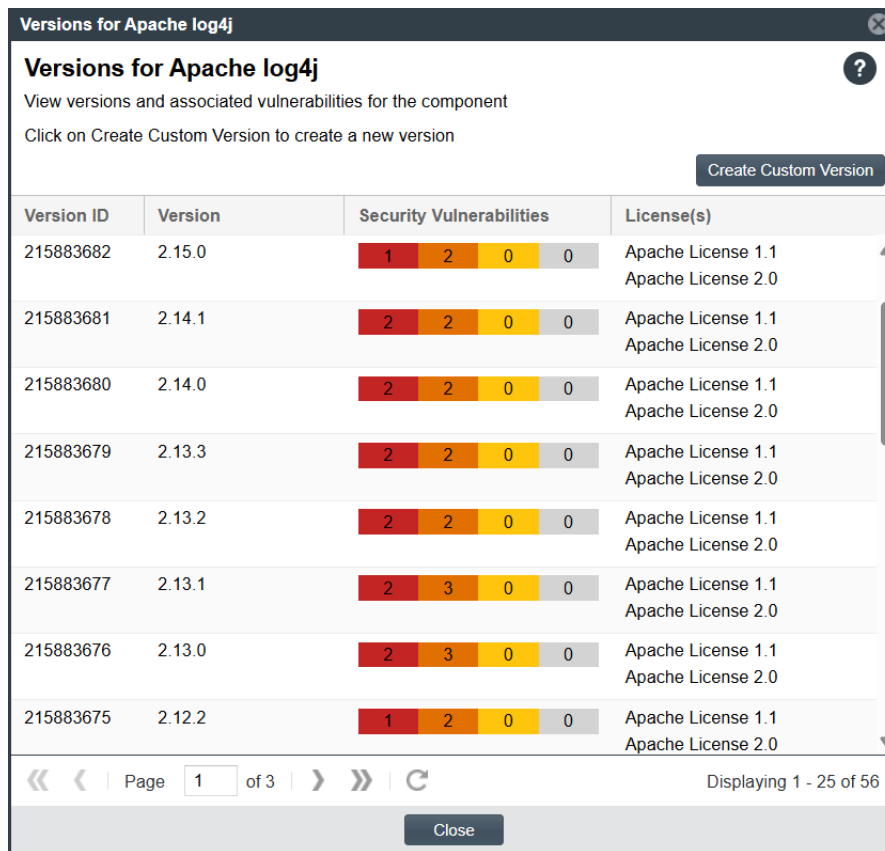
- [Enhanced "Versions for <component>" Window with Version ID Details](#)
- [Enhanced Components Tab with Operator Dropdown for More Refined Results](#)

## Enhanced "Versions for <component>" Window with Version ID Details

Previously, the component version ID details, associated with each version (in the **Version** Column) of a given component were not displayed in the **Versions for <component>** window.

Starting in this release, the **Versions for <component>** window has been enhanced by introducing a new column named **Version ID**. This new column displays the version ID associated with each version (in the **Version** column) of the given component. With this enhancement, the **Versions for <component>** window now displays version IDs, along with each associated version, licenses, and vulnerability totals (by severity) for the given component.

The following displays the **Versions for <component>** window for a component:



Version ID	Version	Security Vulnerabilities	License(s)
215883682	2.15.0	1 2 0 0	Apache License 1.1 Apache License 2.0
215883681	2.14.1	2 2 0 0	Apache License 1.1 Apache License 2.0
215883680	2.14.0	2 2 0 0	Apache License 1.1 Apache License 2.0
215883679	2.13.3	2 2 0 0	Apache License 1.1 Apache License 2.0
215883678	2.13.2	2 2 0 0	Apache License 1.1 Apache License 2.0
215883677	2.13.1	2 3 0 0	Apache License 1.1 Apache License 2.0
215883676	2.13.0	2 3 0 0	Apache License 1.1 Apache License 2.0
215883675	2.12.2	1 2 0 0	Apache License 1.1 Apache License 2.0

## Enhanced Components Tab with Operator Dropdown for More Refined Results

Starting in this release, Code Insight introduces the **Operator** dropdown on the **Components** subtab of the **Global Component & License Lookup** tab that enables you to select a required search defining criteria from the dropdown list prior to defining the search input in the **Keyword** field. Using the **Keyword** field in accordance with the **Operator** dropdown selection allows for more refined search results. The **Operator** dropdown lists the following search criteria:

- **Contains (Any Term)**—Enables you to search by entering one or more character strings, found within a component name, in the **Keyword** field.
- **Begins With**—Enables you to search by entering one or more character strings that match the prefix of a component name, in the **Keyword** field.

- **Exact Match**—Enables you to search by entering the full component name, exactly as it appears in the Code Insight Data Library, in the **Keyword** field.
- **All Terms**—Enables you to search by entering multiple strings, found within a component name, in the **Keyword** field. Multiple strings must be separated with spaces (not commas), and they can appear in any order.

For instance, to find components that contain both Tomcat and Apache, enter: **Tomcat Apache** in the **Keyword** field.

The **Operator** dropdown is available only when the **Keyword** search option is selected in the **Search By** section.

The following displays the **Operator** dropdown on the **Components** subtab of the **Global Component & License Lookup** tab:

The screenshot shows the Code Insight SCA interface. The top navigation bar includes 'revenera | SCA' and 'DATA LIBRARY'. The main section is titled 'Global Component & License Lookup'. On the left, there are tabs for 'Inventory' and 'Projects', and a sidebar with 'Custom Detection Rules' and 'Suppressed Vulnerabilities'. The main area has two subtabs: 'Components' (selected) and 'Licenses'. Under 'Components', there is a 'Search By' section with radio buttons for 'Keyword', 'URL', 'Forge', and 'Component ID'. The 'Keyword' radio button is selected. Below this is a 'Keyword' input field. To the right of the input field is an 'Operator' dropdown menu, which is currently set to 'Contains (Any Term)'. To the right of the dropdown are 'Search' and 'Create New Component' buttons. Below the search section is a table with the following columns: 'Component Name', 'Forge', 'URL', 'Possible License(s)', and 'Actions'.

For more information, see [Keyword Search](#) in the *Code Insight User Guide*.

## Installation, Upgrades, and Configuration

The following enhancements have been added to the Code Insight installation, upgrade, or configuration experience:

- [Support for Ubuntu 24.04.2 LTS](#)
- [Support for CentOS 9.x](#)
- [Support for CycloneDX 1.6](#)

### Support for Ubuntu 24.04.2 LTS

Code Insight can now run on the Ubuntu 24.04.2 LTS platform in addition to previously supported Ubuntu platform versions.

## Support for CentOS 9.x

Code Insight can now run on the CentOS 9.x platform, in addition to previously supported CentOS platform versions.

## Support for CycloneDX 1.6

Starting in this release, Code Insight introduces a support for generating CycloneDX reports compliant with the v1.6 version of the specification.

## Jobs Queue

The following enhancement to the Code Insight Jobs queue is now available:

- Ability to Filter and Reorder Core Server Jobs on Active Jobs Tab

## Ability to Filter and Reorder Core Server Jobs on Active Jobs Tab

Starting in this release, Code Insight allows you to filter the **Jobs** queue for Core Server jobs on the **Active Jobs** tab in the **Jobs** Window. Selecting **Core Server** from the **Server name** field dropdown in the **Active Jobs** tab filters the **Jobs** queue to display only active and scheduled jobs for the selected **Core Server**.

On the **Active Jobs** tab, you can also manage or reorder only scheduled jobs using the icons on the **Actions** column, which are enabled only for scheduled Core Server jobs.

The **Actions** column icons are disabled for an active job and for the following job types:

- Library Refresh
- PDL Update (Electronic Update)

As a result, users are restricted to managing or reordering these job types (listed above) and an active job in the **Jobs** queue on the **Active Jobs** tab. If both the Library Refresh and PDL Update (Electronic Update) types of jobs are scheduled, by default, these jobs are positioned in the second and third rows of the **Jobs** queue, respectively.

The following displays the **Jobs** queue filtered for Core Server jobs on the **Active Jobs** tab:

Jobs						
<b>Jobs</b>		Show jobs for 15 Days				
All Jobs Active Jobs						
Server name:	Core Server					
Job ID	Job Type	Project Name	Status	Triggered By	Queued On	Actions
4492	Project Export	test-codebase-ag	Active	Admin User	03/17/2025 at 06:07 PM	⌵ ⬆ ⬇ ⬅ ⬶ ⬷ ⬸ ⭕
4494	Library Refresh	N/A	Scheduled	Admin User	03/17/2025 at 06:08 PM	⌵ ⬆ ⬇ ⬅ ⬶ ⬷ ⬸ ⭕
4495	PDL Update	N/A	Scheduled	Admin User	03/17/2025 at 06:08 PM	⌵ ⬆ ⬇ ⬅ ⬶ ⬷ ⬸ ⭕
4493	Project Copy	multiple-top-level transitive	Scheduled	Admin User	03/17/2025 at 06:07 PM	⌵ ⬆ ⬇ ⬅ ⬶ ⬷ ⬸ ⭕
4496	Project Export	export-multiple-codebase	Scheduled	Admin User	03/17/2025 at 06:08 PM	⌵ ⬆ ⬇ ⬅ ⬶ ⬷ ⬸ ⭕

For more information, see [Reordering the Jobs Queue on Active Jobs Tab](#) in the *Code Insight User Guide*.



# 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.

- [Reporting Dependencies from Conan Packages](#)
- [Support for .dist-info Files in PyPI Ecosystems](#)
- [Reporting Top-Level Inventories from Implementation Files](#)
- [Ability to View Added, Updated, and Removed Inventory Items in Latest Scan](#)

## Reporting Dependencies from Conan Packages

Project scans now report top-level inventory items and direct dependencies found in the Conan ecosystems, specifically in the following manifest files: `conanfile.py` and `conanfile.txt`.

For more information, see [Supported Ecosystems](#) in the *Code Insight User Guide*.

## Support for .dist-info Files in PyPI Ecosystems

Previously, Code Insight retrieved top-level inventory items and direct (first-level) dependencies from post-build artifacts, specifically `.whl` and `.egg` files, in PyPI ecosystems. Now, top-level inventory items and direct dependencies are also retrieved from the `.dist-info` files (post-build artifacts) in PyPI ecosystems. Top-level inventory items and direct dependencies are reported from the METADATA file, which also resides within the `.dist-info` file.



**Note** - Currently, Code Insight also identifies transitive dependencies—those that are dependencies of other dependencies—by scanning `requirements.txt`, `setup.py`, `.whl`, `.egg`, and `.dist-info` (METADATA) files, and classifies them as direct (first-level) dependencies.

For more information, see [Supported Ecosystems](#) in the *Code Insight User Guide*.

## Reporting Top-Level Inventories from Implementation Files

Code Insight now reports top-level inventory items found within the Implementation files. This enhancement applies specifically to the following C and C++ based manifest file: `.c`, `.h`, `.cpp`, `.cxx`, `.cc`, `.hpp`, `.hxx`, and `.hh`.

During an automated analysis, Code Insight scans these files to detect and report top-level inventory items based on the user-defined header statements in the same files.

Additionally, If you want Code Insight to generate unpublished inventory items with the Work in Progress (WIP) inventory type—in addition to the usual published inventory items—when scanning C/ C++ files, set the `enable.cpp.unpublished.inventory.detection` property to `True`. This property is found in the `PAS_GLOBAL_PROPERTIES` table in the Code Insight database.

By default, the `enable.cpp.unpublished.inventory.detection` property is set to `False`.

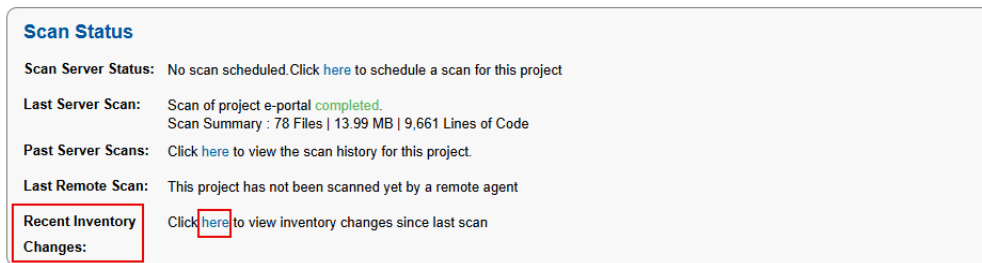
For more information, see [Supported Ecosystems](#) in the *Code Insight User Guide*.

## Ability to View Added, Updated, and Removed Inventory Items in Latest Scan

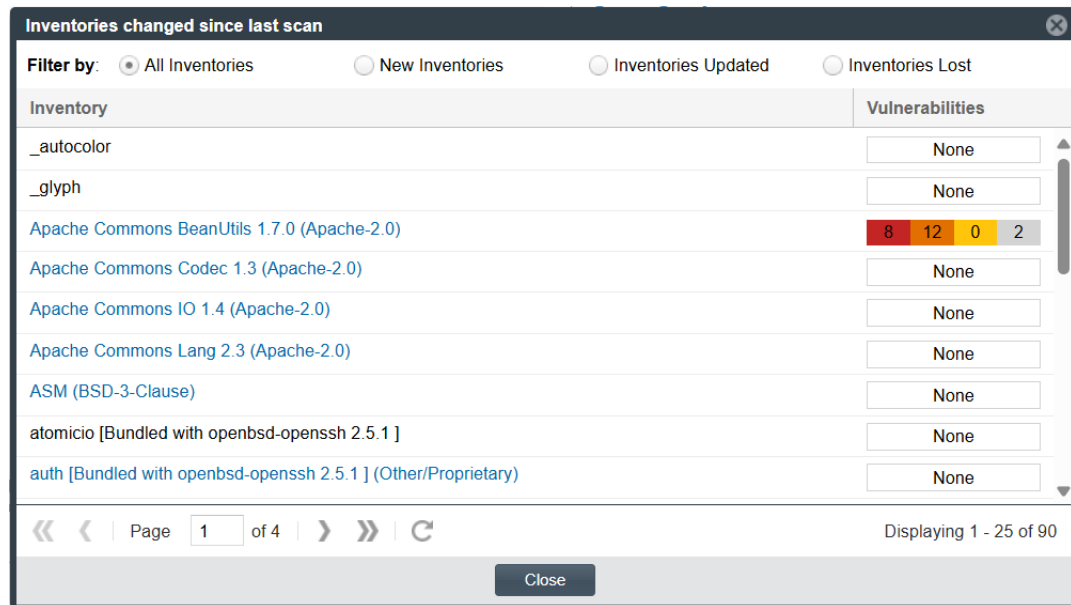
Starting in this release, the **Scan Status** section on the **Project Summary** tab has been enhanced with a new field named **Recent Inventory Changes**. This new field allows you to open the **Inventories changed since last scan** window via clicking the hyperlinked term **here**. The **Inventories changed since last scan** window displays a list of all inventory items that were added, modified, or removed in the latest project scan. You can use the following filter options available at the top of the **Inventories changed since last scan** window to refine the displayed inventory items:

- **All Inventories**—Selecting this option displays a list of all inventory items that were added, updated, or removed in the latest project scan. By default, this filter option is selected.
- **New Inventories**—Selecting this option displays a list of inventory items that were added in the latest project scan.
- **Inventories Updated**—Selecting this option displays a list of inventory items that were modified or updated in the latest project scan.
- **Inventories Lost**—Selecting this option displays a list of inventory items that were removed or are no longer present in the latest project scan.

The following displays the **Recent Inventory Changes** field and the associated hyperlinked term **here** within the **Scan Status** section, as well as the **Inventories changed since last scan** window:



**Figure 1:** Recent Inventory Changes field



**Figure 2:** Inventories changed since last scan window

For more information, see [Summary Tab](#) in the *Code Insight User Guide*.

## Security Vulnerability Reporting

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

- [Support for Identifying Known Exploited Vulnerabilities in Security Vulnerabilities Window](#)

### Support for Identifying Known Exploited Vulnerabilities in Security Vulnerabilities Window

The **Security Vulnerabilities** window, which is displayed when you click the **Vulnerabilities** bar graph for a specific component or inventory item, has been enhanced by adding a new property named **Is KEV**. This new property indicates whether a security vulnerability, listed in the **Security Vulnerabilities** window, is already included in the Known Exploited Vulnerability (KEV) Catalog. The available values indicated by the **Is KEV** property are **Yes** and **No**.

The following displays the **Is KEV** property value for all security vulnerabilities in the **Security Vulnerabilities** window:



```
git@git.eng.flexera.com:org1/  
repo8.git>>337b811c76f9dff572d53d9d42e1163aaadb9549**Folder4
```

For more information, see [Fields Used to Configure a SCM Git Instance](#) in the *Code Insight User Guide*.

## Vulnerability Management

This release includes the following enhancements to the management of security vulnerabilities:

- [Ability to Copy Suppressed Vulnerabilities and Exclusion Analysis](#)
- [Enhanced Support for Exporting and Importing Suppressed Vulnerabilities and Exclusion Analysis](#)

### Ability to Copy Suppressed Vulnerabilities and Exclusion Analysis

Previously, users could not copy suppressed security vulnerabilities and exclusion analysis of all security vulnerabilities—associated with copied inventory items—from the source project to the target project during a project copy.

Starting in this release, Code Insight supports copying all suppressed security vulnerabilities and exclusion analysis of all security vulnerabilities—associated with copied inventory items—from the source project into the target project as part of the project copy process.

All suppressed security vulnerabilities and exclusion analysis of security vulnerabilities—associated with the copied inventory items in the target project—appear in the **Security Vulnerabilities** window (which opens when you click the **Vulnerabilities** bar graph for a copied inventory item) and on the **Project** subtab of the **Suppressed Vulnerabilities** tab on the **Data Library** page.

### Enhanced Support for Exporting and Importing Suppressed Vulnerabilities and Exclusion Analysis

Previously, suppressed security vulnerabilities and exclusion analysis of all security vulnerabilities—associated with exported or imported inventory items—were not included during the project export or import process.

Starting with this release, Code Insight now supports exporting and importing of all suppressed security vulnerabilities (suppressed at the project level only) and exclusion analysis of all security vulnerabilities—associated with exported or imported inventory items—as part of the project export or import process.

After a project import, all suppressed security vulnerabilities (suppressed at the project level only) and exclusion analysis of all security vulnerabilities—associated with the imported inventory items in the target project—appear in the **Security Vulnerabilities** window (which opens when you click the **Vulnerabilities** bar graph for a copied inventory item) and on the **Project** subtab of the **Suppressed Vulnerabilities** tab on the **Data Library** page.

## Web UI

This release includes the following enhancement to the FlexNet Code Insight Web UI:

- [Ability to Consolidate Data on Project Dashboard for Parent and Child Projects](#)

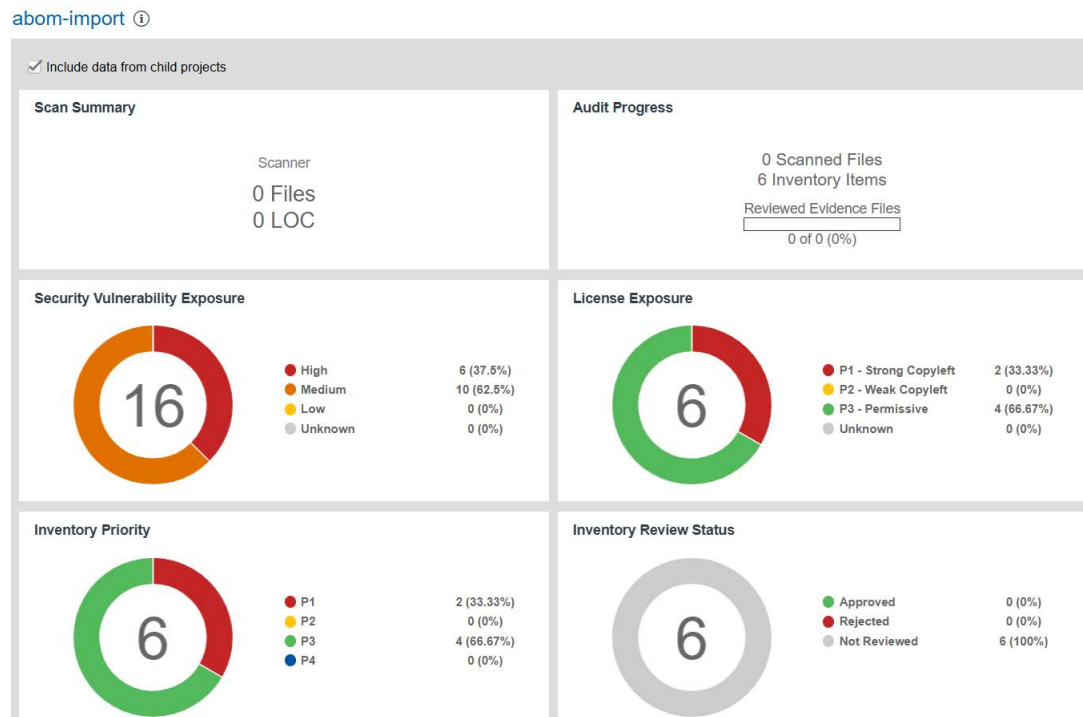
## Ability to Consolidate Data on Project Dashboard for Parent and Child Projects

Starting in this release, the project dashboard has been enhanced by introducing a check box labeled as **Include data from child projects**. When you select this check box, the data from a given project and all of its child projects is consolidated and displayed on the **Scan Summary**, **Audit Progress**, **Security Vulnerability Exposure**, **License Exposure**, **Inventory Priority**, and **Inventory Review Status** tiles.

By default, this check box is cleared.

The check box labeled as **Include data from child projects** is enabled only when a given project includes one or more child projects.

The following displays the project dashboard for a project that has child projects with the **Include data from child projects** check box selected:



## REST API Enhancements

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

- [Updates to Existing APIs](#)

## Updates to Existing APIs

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

Resource	API Name/Endpoint	Method	Function Change Description
vulnerability	<b>Get suppressed vulnerabilities</b>  vulnerability/ suppress	GET	<p>The response now includes the following properties for a given vulnerability suppression:</p> <ul style="list-style-type: none"><li>● <b>itemNumber</b>—Indicates the number for each vulnerability suppression record.</li><li>● <b>suppressionScope</b>—Indicates whether the given vulnerability is suppressed for a project or suppressed globally. If the vulnerability is suppressed at the project level, value is <b>PROJECT</b>.</li><li>● <b>suppressionDetails</b>—Indicates detailed information about the suppression, when the given vulnerability is suppressed at the project level, via the following sub-properties:<ul style="list-style-type: none"><li>● <b>projectId</b>—The ID of the project for which the vulnerability was suppressed.</li><li>● <b>state</b>—The state of the suppressed vulnerability.</li><li>● <b>justification</b>—The reason for suppressing the vulnerability.</li><li>● <b>response</b>—Any response or action taken related to the suppressed vulnerability.</li></ul></li></ul>
	<b>Suppress vulnerability</b>  /vulnerability/ suppress	POST	<p>The request now includes the two new properties, <b>suppressionScope</b> and <b>suppressionDetails</b>. These properties enable you to define the scope of a specified vulnerability suppression, either at the project level or globally:</p> <ul style="list-style-type: none"><li>● Setting the <b>suppressionScope</b> property to <b>PROJECT</b> enables you to set the following sub-properties of the <b>suppressionDetails</b> property for project-level suppression:<ul style="list-style-type: none"><li>● <b>projectId</b>—The ID of the project for which the specified vulnerability should be suppressed.</li><li>● <b>state</b>—The current state of the specified vulnerability.</li><li>● <b>justification</b>—The reason for suppressing the specified vulnerability.</li><li>● <b>response</b>—Any response or action taken related to the specified vulnerability.</li></ul></li></ul>

Resource	API Name/Endpoint	Method	Function Change Description
(Continued)	(Continued)	(Continued)	<ul style="list-style-type: none"> <li>Setting the <b>suppressionScope</b> property to the <b>GLOBAL</b> suppresses the specified vulnerability globally across all projects. If the <b>suppressionScope</b> property is kept undefined, by default, the specified vulnerability suppresses globally across all projects.</li> </ul>  <p><b>Important</b> - To suppress the specified vulnerability at the project level, the <b>versionScope</b> property must be set to <b>SPECIFIC_VERSIONS</b> and setting the <b>reason</b> property is optional.</p> <p>This API also enables you to globally suppress a vulnerability that was initially suppressed for a project; however, you cannot suppress a globally suppressed vulnerability at the project level.</p> <p>The project's Security Contact (also called Security Reviewer) and Developer Contact (also called Remediation Developer) can invoke this API only for project-level suppression, and the System Administrator can invoke the API only for global-level suppression.</p>
	<b>Get vulnerability suppress details</b>  /vulnerability/suppress/details	GET	<p>The response now includes a relevant error message when attempting to call the API for a given vulnerability that was suppressed at the project level.</p> <p>Only the System Administrator can invoke this API successfully.</p>
	<b>UnSuppress vulnerability</b>  /vulnerability/unSuppress	POST	<p>The request now includes a new property, <b>projectId</b>, which allows you to unsuppress a specified vulnerability at project level:</p> <ul style="list-style-type: none"> <li>If the <b>projectId</b> property is set to a value (required project ID), the specified vulnerability will be unsuppressed only for that specified project.</li> <li>If the <b>projectId</b> property is kept undefined, the specified vulnerability will be unsuppressed globally across all projects.</li> </ul>



Resource	API Name/Endpoint	Method	Function Change Description
<i>(Continued)</i>	<i>(Continued)</i>	<i>(Continued)</i>	The project's Security Contact (also called Security Reviewer) and Developer Contact (also called Remediation Developer) can invoke this API only for project-level unsuppression, and the System Administrator can invoke the API only for global-level unsuppression.

## Resolved Issues

The following issues were resolved in the Code Insight 2025 R2 release:

Issue	Description
<b>SCA-57239</b>	Scanning a requirements.txt file failed to generate inventory items with appropriate versions. This issue has been resolved.
<b>SCA-57214</b>	A failure was observed while updating the Project report. Instead of reflecting the correct count of unique copyright entries, the Project report displayed duplicate entries. This issue has been resolved.
<b>SCA-56790</b>	Scanning a requirements.txt file failed to detect the certifi version This issue has been resolved.
<b>SCA-56281</b>	Inconsistencies were observed in the resulting inventory items when a .NET SDK project was scanned twice with only minor changes to package references. This issue has been resolved.
<b>SCA-51677</b>	A user was able to create tasks for an inventory item that was generated from a different project scan, even though the same user was not permissible to edit and create tasks for the same inventory item. This issue has been resolved.
<b>SCA-51080</b> <b>SCA-50964</b>	Scanning the NPM codebase, including the v1 version of a package-lock.json file, failed to generate the dependency inventory items. This issue has been resolved.
<b>SCA-46385</b>	Scanning a .csproj file with multiple dependency references resulted in generating an inventory item only for the last dependency referenced. This issue has been resolved.
<b>SCA-56648</b>	A discrepancy was observed between the <b>Get Project Inventory</b> API response and Code Insight user interface. The API response included all possible licenses for an inventory item, even when a valid component version (CV) was already selected. In contrast, the user interface displayed only license(s) associated with the selected valid component version. This issue has been resolved.

## Known Issues

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

- [Advanced Inventory Searches](#)

- [Alert Management](#)
- [All-Project Inventory View](#)
- [Automated Workflow for Inventory Publication and Review](#)
- [Custom Detection Rules](#)
- [Data Library, Library Refreshes, 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 and Unsuppression](#)
- [Web UI](#)
- [Code Insight Security Issues](#)

## Advanced Inventory Searches

The following known issue exists for the Advanced Inventory Search feature (available on the **Project Inventory** tab, in the **Analysis Workbench**, and in the **Inventory View**).

See the following in the **Vulnerability Suppression/Unsuppression** section:

- [SCA-53859: Advanced inventory searches in global “Inventory” view taking more time when security vulnerability filters are applied](#)

## Alert Management

The issues exist for managing vulnerability alerts associated with inventory items in a project.

### SCA-53632: Alerts not being deleted for inventory updated to new component version having no alerts

When you update an inventory item currently associated with open alerts to another component version that has no alerts, the alerts are not removed for the updated item.

**Workaround:** None exists.

### SCA-53629: Closing alert for an inventory item not being applied to duplicate inventory in the project

When you close an alert for a given inventory item in a project, this status change should be applied to duplicate inventory within the project (that is, inventory having the same component version but a different license or relationship such as “dependency of”). Currently, the alert for duplicate inventory are not being closed.

**Workaround:** To close the alert for all duplicate inventory, perform a project-level suppression of the vulnerability associated with that alert.

## All-Project Inventory View

The following is known issue in the **Inventory** view, which shows inventory items 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 Publication and Review

The following is known issue 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.

# Custom Detection Rules

The following are known issues when managing custom detection rules.

## SCA-48572: No error message indicating “Inventory Name” value in rule exceeds limit

When you attempt to save a custom detection rule with an **Inventory Name** value that exceeds its 255-character limit, the rule is not saved, and no error message is displayed to describe the problem.

**Workaround:** If you enter a value for **Inventory Name**, ensure that has no more than 255 characters.

## SCA-48564: Changes to “Inventory Name” in custom detection rules not applied to inventory during rescans

When you update an existing value in the **Inventory Name** field for a custom detection rule, a rescan or forced full rescan does not apply the change to the inventory name.

**Workaround:** Create a new project and perform a fresh scan so that the name change is correctly applied to the inventory item.

## SCA-55447: Custom license is not being deleted from custom detection rules

When you attempt to delete a custom license using the **Delete a custom license** Rest API, the license fails to be removed from the associated custom deletion rules.

**Workaround:** None exists.

# Data Library, Library Refreshes, and Electronic Updates

The following are known issues related to the Code Insight data library, the daily Library Refresh, which reports new vulnerabilities associated with inventory, or the Electronic Update, which keeps Code Insight systems up to date with the latest data-library information.

## SCA-51662: Electronic Update banner and job showing status as active when job is actually waiting for scans to complete

The Electronic Update banner and the **PDL Update** job for an Electronic Update is showing that the job is active when it is actually waiting for scans to complete, as recorded correctly in the log.

**Workaround:** None exists.

## SCA-51313: Electronic Update banner displaying even though the Update is not executing

The Electronic Update banner, indicating that an update is currently running, is being displayed even though the Update is not running. This error occurs under these circumstances:

- An Electronic Update that is added to the **Jobs** queue during a currently running scan or rescan is flagged as **Active** in the queue even though its state should be **Scheduled**. (However, the Update

is actually waiting for the scan or rescan to finish.) See [SCA-51296: Electronic Update or License Refresh showing “Active” when added to Jobs queue during an “Active” scan or rescan](#).

- An Electronic Update is added to the **Jobs** queue while a License Refresh is currently running. (The Electronic Update is properly placed in a **Scheduled** state and is waiting for the Refresh to finish.)

**Workaround:** None exists.

### **SCA-51296: Electronic Update or License Refresh showing “Active” when added to Jobs queue during an “Active” scan or rescan**

An Electronic Update or Library Refresh that is added to the **Jobs** queue during a currently running scan or rescan is flagged as **Active** in the queue even though its state should be **Scheduled**. Note, however, that the Update or Refresh is actually waiting for the scan or rescan to finish, as correctly recorded in the log file.

**Workaround:** None exists.

### **SCA-51293: Electronic Update or License Refresh failing with “Cannot delete or update a parent row: a foreign key constraint fails”**

An Electronic Update or License Refresh can fail when orphan custom components (that is, custom component versions not linked to any inventory items) have licenses mapped to them.

**Workaround:** Run a SQL query to clean the component version and their licenses. Contact Reverera Support for details.

### **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 might 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.

## Export and Import

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

### SCA-52508: Customers not able to open certain manually created inventory items that have been imported

When project data is exported, the data includes whether the inventory item was created by the system or manually by a user. When the exported data is then imported *and* it contains inventory that was flagged as manually created, consider the following import scenarios:

- **Scenario 1**—The data is imported to the same machine from which it was exported, but a given user who created one or more inventory items in the data has since been deleted from the Code Insight database.
- **Scenario 2**—The data is imported to a different machine, and the given user who created one or more inventory items does not exist on this machine.

In either scenario, the import process successfully completes, but customers are not able to open the inventory items created by the deleted or non-existing user.

**Recommendation for Scenario 1:** Do not delete the user (who created the inventory item) from database. Instead, disable the inactive user.

**Workaround:** Contact Technical Support for assistance.

### 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".

### SCA-55178: Relationship attribute fails to report all direct parent inventory items while data export from 2024 R3 project and import to 2024 R4 project

Exporting data from a Code Insight 2024 R3 project and importing it into a code insight 2024 R4 or later project results in a failure of the **Parent Inventory** value of the **Relationship** attribute to indicate all direct parent inventory items associated with the inventory item.

During the import of project data exported from a 2024 R3 project, inventory items with multiple direct parent relationships fail to update (report) all direct parent relationships. After import, only few direct parent inventory items are indicated by the **Parent Inventory** value of the **Relationship** attribute for these inventory items.

**workaround:** None exists

## Installation, Upgrades, and Configuration

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

### SCA-48759: Longer Tomcat startup during migration to 2023 R3 or later due to new column creation

A new column was added to the `pse_inventory_groups` table in Code Insight 2023 R3 to support the reporting of dependency scope. During a migration to Code Insight 2023 R3 or later, the creation of this column (performed through Liquibase) can slow down the initial Tomcat startup if the number of inventory items is large. (For example, if the inventory count is 15,000, the initial Tomcat startup can take 30 minutes to complete.)

**Workaround:** None exists.

### 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 Amazon Corretto OpenJDK JRE 8u412 from [Downloads for Amazon Corretto 8](#). 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 Code Insight user interface

Users who are deleted from the LDAP server or disabled in LDAP still appear on the **Users** page in the Code Insight user interface 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 Reverera 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 Reverera Support, access the **Get Support** menu in the Reverera Community at <https://community.reverera.com/s/>.)

## SCA-54423: Longer Code Insight Migration to 2024 R3 due to New Columns Addition

Inclusions of new columns to the PDL\_COMPONENT table are time-consuming while migration of Code Insight to 2024 R3.

**Workaround:** None exists



---

**Note** • Customers may have to wait for 30 minutes to 3 hours for the successful migration of Code Insight application to 2024 R3.

## SCA-54402: Deletion of a parent inventory item results the Constraint Violation Exception error During an imported project migration

For an imported project's inventory item if any parent inventory item is deleted from the project and child inventory items are available, migrating the project from an older version to a new version of Code Insight or restarting the Tomcat leads to display the Constraint Violation Exception error message and the migration continues.

**Workaround:** None exists

# Inventory History

The following are known issues with the Inventory History feature.

## SCA-52088: Inventory history incorrectly recording an “Associated Files” update after manual creation of an inventory item

When an inventory item is manually created or updated through the Code Insight user interface or the REST API, the **View History** window is registering an **Associated Files** update that never occurred. The PSE\_INVENTORY\_GROUPS\_AUD table in the Code Insight database is also recording this update.

**Workaround:** None exists.



### SCA-51192: “Associated Files” record not displayed when other modified fields have been saved along with it

A separate **Associated Files** record is not displayed in the **Inventory History** window if other fields such **Encryption**, **URL**, and more have been updated and saved along with it.

**Workaround:** None exists.

### 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 user interface 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.

### SCA-54661: Files associated with inventory item fail to appear when navigating to the next and last page on the Associated Files tab

On the **Associated Files** tab in the **Project Inventory** view and **Analysis Workbench**, when navigating to next page by clicking the > (next-page) icon and to last page by clicking the >> (last-page) icon, files associated with the inventory item—having 3k or more files—are not being displayed.

**Workaround:** None exists.

## SCA-54998: Inventories display failure for large codebases scans using scan-agent plugin in the SQL server environment

For a plugin scans a large number of codebase files, right-clicking the scan-agent plugin alias node in the **Codebase Files** pane of the **Analysis Workbench** and then selecting **Show File Inventory** from the pop-up menu leads to a failure to display the associated inventory items in the **Inventory Items** pane.



**Note** • Consider the following conditions contributing to this issue:

- When Code Insight scanned only the large number of codebases, generating a large number of inventory items.
- When Code Insight used only the SQL Server database.
- When inventory items are filtered only by remote plugin alias.

**Workaround:** Select and right-click the main codebase folder node or any folder/subfolders nodes directly under the scan-agent plugin alias node in the **Codebase Files** pane from which you want the inventory items, and then select the **Show file Inventory** from the pop-up menu to display the correct associated inventory items in the **Inventory Items** pane.

## 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).

### SCA-56298: The file deletion or dissociation does not remove the copyright related to that file for the inventory item during rescan

Deleting a file from a codebase or dissociating it from an inventory item fails to remove the copyright related to that file for the inventory item during the project rescan.

**Workaround:** None exists.

## Project Inventory

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

See also [SCA-53169: Project-suppressed vulnerabilities considered not suppressed when policy is applied](#) in the **Vulnerability Suppression and Unsuppression** section.

### SCA-53837: Top-level inventory deletion not deleting all inventory items in the case of NPM cyclic dependencies

When a top-level NPM inventory item is deleted, some of the inventory items are not being deleted in the case of cyclic dependencies.

**Workaround:** The user can manually delete the inventory items individually or in a multiple selection.

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

### SCA-54517: Creating inventory items with zero files association for the REST API project import data with the “On the data import or rescan, delete inventory with no associated file” option enabled for the project

When the **On the data import or rescan, delete inventory with no associated file** option at the project settings is checked/enabled and the REST API import project data is performed, inventory items with zero file association are generated.

**Workaround:** Import the data from an another Code Insight project via selecting the **Import Project Data** option from the **Manage Project** menu on the project's **Summary** tab, which restricts the creation of inventory items without associated files.

### SCA-56254: Entire copyright text removed from “Copyrights” field after exceeding the maximum character limit in the same field

If the copyright text exceeds the maximum character limit while adding a new or editing an existing open-source or third-party copyright for an inventory item in the **Copyrights** field on the **Copyrights & Usage** tab in the **Analysis Workbench**, a popup displays with an error message stating The Copyright text should not exceed 512 characters, and the entire text is removed from the **Copyrights** field.

**Workaround:** None exists.

### SCA-56306: The “Copyrights and Usage” tab on the “Inventory Details” tab fails to populate copyrights when associated files exceed 20k.

The **Copyrights and Usage** tab on the **Inventory Details** tab in the **Analysis Workbench** fails to display open-source or third-party copyrights for an inventory item when its associated files count exceeds 20k in the SQL server database.

**Workaround:** None exists.

# 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.

See also [SCA-53390: Project-level suppressed vulnerabilities getting fetched by the “Get suppressed vulnerabilities” REST API](#) in the **Vulnerability Suppression and Unsuppression** section.

### SCA-52409: Execution of the same configured “Update inventory” REST API triggering automatic review

When you call the **Update inventory** REST API to update a specific inventory item, an automatic review (by policy) is automatically triggered on the item once the update is complete. (The review is triggered only if the inventory’s component, license, or usage properties were edited.) However, if you call this API again on the inventory item even though no attributes of the item have changed since the previous update, the review is erroneously triggered again. The policy should not be triggered again since no new edits have occurred.

**Workaround:** None exists

### 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.

### SCA-54968: Discrepancy between Provenance ID value in Inventory History window and GET Inventory Details API response

For an inventory item in the target project, the Provenance ID value displayed in the **Inventory History** window in code Insight user interface fails to sync with the Provenance ID value reflected in the **GET Inventory Details** REST API response.

**workaround:** None exists

### SCA-55151: Project Reviewer is unable to update the inventory priority from Update Inventory API

Project Reviewers fails to update the priority value of an inventory item via the **Update Inventory** REST API.

**Workaround:** Project Reviewers can use the Code Insight user interface to update the priority values of inventory items.

## Scan Agent Plugins

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

### SCA-51042: Generic plugin “transitive” scan with non-runtime-dependency reporting disabled still reporting such dependencies in Gradle codebase

A generic plugin scan whose profile is configured with **All Transitive Dependencies** and has **Report Non-Runtime Dependencies** disabled is still reporting non-runtime dependencies in a Gradle codebase.

**Workaround:** None exists.

### SCA-50489: Generic plugin scan on Gradle codebase reporting duplicate inventory and file associations

A Gradle-codebase scan performed by the generic plugin using an **Only First Level Dependencies** or **All Transitive Dependencies** scan profile with **Report Non-Runtime Dependencies** enabled or disabled can incorrectly report the following from the `build.gradle` and `libs.versions.toml` files.

- Duplicate top-level inventory
- Duplicate dependency inventory
- Duplicate associated files

**Workaround:** None exists.

### 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.

### SCA-54521: Docker plugin rescan fails to remove Docker layer IDs information for the inventory items having no associated files

Performing a docker plugin scan for an image (for instance, Ubuntu) leads to display the Docker layer IDs information on the **Inventory Details** tab for inventory items. But, performing a docker plugin rescan for an another image with the same alias and project fails to remove the Docker layer IDs information on the **Inventory Details** tab for the inventory items that have no associated files.

**Workaround:** None exists.

### SCA-54591: Scanning of Docker image using older release Docker plugin in the FlexNet Code Insight of new version fails to create all inventory items

Performing a Docker plugin scan for an image using a Docker plugin of 2023 R3 build and the FlexNet Code Insight of 2024 R3 build leads to generating the few inventory items. Although the scan is successful, the inventory items from Syft are not reported.

**Workaround:** Use the Docker plugin of 2024 R3 build to scan the Docker images.

## Scanning and Automated Discovery

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

### SCA-53834: Some dependencies missed if Gradle command failures occur due to unset variables, insufficient permissions for variable values, or plugins not being initialized

If a plugin or the variables for a Gradle project are not initialized (for example, the plugin is not imported or the files passing the variables values are missing), the Gradle commands used to retrieve dependencies fail, causing the regular text parser to be triggered. Additionally, if the value for a variable requires access permissions for initialization (for example, if the variable holds a URL and an internal URL is passed), the system must have access to that URL.

**Workaround:** Ensure that variables and plugins can be properly initialized and that any given variable value is accessible to the system.

### SCA-50977: Non-runtime dependencies marked as runtime during “transitive” scans on Gradle codebases

Non-runtime dependencies are being reported as runtime dependencies during scans (configured with **All Transitive Dependencies** in their profiles) on Gradle codebases. However, the total number of inventories is still correct. The issue might be the result of the use of an external API to collect transitive dependencies.

**Workaround:** None exists.

### SCA-50958: “build.gradle” files incorrectly associated with top-level inventory reported from libs.version.toml during “transitive” scans

Transitive scans on Gradle codebases might incorrectly associate the build.gradle and build.gradle.kts files with top-level inventory reported from the libs.versions.toml file. This issue occurs when a libs.versions reference is available in the build.gradle file.

**Workaround:** None exists.

### SCA-50448: Invalid duplicate transitive dependencies reported for Gradle codebases

A Gradle-codebase scan using an **Only First Level Dependencies** or **All Transitive Dependencies** scan profile with **Report Non-Runtime Dependencies** enabled or disabled can sometimes report invalid duplicate transitive dependencies for a given dependency.

**Workaround:** None exists.

### SCA-49499: Multiple top-level inventory items associated with a single file in a project resulting in incorrect child-parent relationship within inventory

When a file in a project is associated with multiple top-level inventory items, incorrect child-parent relationships within the inventory can occur.

**Workaround:** None exists.

### SCA-49181: Migrated project scan showing incorrect detection notes for inventory though mapping to Debian forge and URL is successful

After a scan on a migrated project, an inventory item whose component is found in the Debian forge is showing incorrect detection notes even though the component is successfully mapping to the Debian forge and URL. As a result, the inventory is not getting published.

**Workaround:** Create a new project and do a fresh scan of the codebase.

### 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
```

Refer to “Creating Exclusion Patterns for Scan Profiles” in the *Code Insight Installation & Configuration Guide* for complete 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.

## SCA-54544: Scan times for JAR files are longer in comparison

Performing a scan of jar files, including those with the pom.xml files that contains dead License URLs, are taking longer. The overall scan time is expected to increase approximately 3 to 5 minutes for each jar file with such issue.

**Workaround:** None exists.



---

**Note** - The Scan is taking more time to complete but there is no deviation in the reported inventory items.

## SCA-56266: Scan Jobs have a status of “Waiting on update” or “Waiting on library refresh” are unable to stop

From the **Jobs** queue on the **Jobs** window, user is unable to stop the scan jobs that have a status of the **Waiting on update** or **Waiting on library refresh**.

**Workaround:** None exists.

## SCA-56882: Relationship mapping failure for a parent and child inventory items due to the existed relationship mapping of same child inventory item and different parent inventory item

The relationship between a parent and child inventory items, identified as transitive dependencies, fails to map if relationship between the same child inventory item and an another parent inventory (with the same component name but a different version) was initially mapped.

**Workaround:** To ensure uniqueness and accurately capture all parent-child relationships during scanning, the relationship mapping format of the parent and its child inventory item must include the component version of the parent inventory item.

## SCA-57240: Inventory items with incorrect component versions from setup.py and .dist-info (METADATA) files

Scanning setup.py and .dist-info (METADATA) files may result to inventory items with incorrect component versions. This issue occurs due to presence of comma operators in the dependency texts within the same files.

**Workaround:** None exists.

### **SCA-57236: Failure to generate inventory items from setup.py with install\_requires=requirements statement**

When scanning a setup.py manifest file, certain inventory items may not be generated. This occurs mainly due to the lack of support for the `install_requires=requirements` statement within the same file, which prevents the detection of certain components.

**Workaround:** None exists.

### **SCA-57231- Transitive scan generates duplicate inventory items with different package versions**

Performing a transitive scan for a project generates duplicate inventory items with different package versions. This indicates that the transitive scan for the project fails to resolve the correct package version for inventory item.

**Workaround:** None exists.

### **SCA-57229- Direct or transitive scan generates inventory items without package versions**

Performing a direct or transitive scan for a project—including package versions in 1.xa or 1.x.xb patterns—may lead to generate inventory items without package versions.

**Workaround:** None exists.

### **SCA-57270- Inventory items without component versions from a METADATA file**

Scanning a METADATA file may result to inventory items generation without component versions. This issue arises due to the presence of certain operators, such as brackets and semicolons, within the same file.

**Workaround:** None exists.

### **SCA-54203- Transitive dependencies incorrectly classified as direct in codebase transitive scan**

When Code Insight performs a transitive scan on a codebase package (except NPM package), all identified transitive dependencies may incorrectly classified as direct (first-level) dependencies.

**Workaround:** None exists.

### **SCA-57230- Inventory items with invalid component names on setup.py scan**

Scanning a setup.py manifest file can result in the generation of certain inventory items that do not include valid component names.

**Workaround:** None exists.



# Source Code Management (SCM) Support

The following are known issues with Code Insight SCM support.

## SCA-52522: Credentials entered in Git URL not a best practice

GIT allows users to pass credentials within the repository URL if an HTTP (or HTTPS) URL is used. Consequently, when setting up SCM synchronization between Code Insight and Git (*and* Git SSH is not used), users can include credentials in the **Git Repository URL(s)** value. Note, however, that these credentials are displayed in the URL value when it is shown in other parts of the Code Insight.

Code Insight also provides the **Git Username** and **Git Password** fields in which to enter the credentials during synchronization setup. Credentials passed in these fields are *not* displayed in the URL value when it is shown in other locations in the product. Therefore, when Git SSH is not used, the best practice is to always use the **Git Username** and **Git Password** fields, not the **Git Repository URL** field, to pass the credentials.

**Workaround:** Use Git SSH *or* pass the user credentials through the user interface fields if an HTTP or HTTPS URL is used.

## 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/sbnl/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 and Unsuppression

The following are known issues when suppressing and unsuppressing vulnerabilities.

## SCA-53859: Advanced inventory searches in global “Inventory” view taking more time when security vulnerability filters are applied

An Advanced Inventory Search in the global **Inventory** view takes more time when **Security Vulnerabilities** filters are applied *and* the Code Insight system has a large number of projects, inventory items, and associated vulnerabilities. The following shows approximate search times for various system sizes when any **Security Vulnerability ID**, **Severity**, or **Age** filter (alone or in any combination) is defined:

- An inventory load of **1 million** inventory items across more than **10K** projects takes approximately **11** minutes.
- An inventory load of **0.5 million** inventory items across **5K** projects and takes approximately 5 minutes.
- An inventory load of **0.1 million** inventory items across **2.5K** projects takes approximately **3** minutes.

**Workaround:** None exists.

## SCA-53845: Under CVSS v2.0 scoring system, “Vulnerabilities” bar graph in component version lookups not showing counts for known vulnerabilities with no available severity

When Code Insight is configured to use the CVSS V2.0 scoring system and a given component version is associated with vulnerabilities that have no severity information available, the **Vulnerabilities** bar graph in the following locations is incorrectly showing **0** in the gray (no severity available) box:

- **Show Versions** section for the component in **Component Lookup** (accessed when editing project inventory)
- **View Versions** window for the component in **Global Component & License Lookup**

Additionally, the response for the **Get Component** REST API, when set to **V2** for **cvssVersion**, is also returning **0** for the **Unknown** property of a component version associated with those vulnerabilities that have no available severity information.

**Workaround:** None exists.

## SCA-53390: Project-level suppressed vulnerabilities getting fetched by the “Get suppressed vulnerabilities” REST API

The **Get Suppressed Vulnerabilities** REST API is fetching vulnerabilities suppressed at the project level in the results. (This API is designed to fetch only vulnerabilities suppressed at the global level; it should not be fetching vulnerabilities suppressed at the project level.)

**Workaround:** None exists.

## SCA-53335: “Vulnerabilities” bar graph on “Component Details” tab in “Project Inventory” erroneously reflecting vulnerabilities suppressed/unsuppressed at project level

The **Vulnerabilities** bar graph on the **Component Details** tab for an inventory item in **Project Inventory** and the **Analysis Workbench** should reflect only current global vulnerability counts for the component version. That is, the graph totals should not be impacted by the suppression or unsuppression of

vulnerabilities at the project level. However, the graph on the **Component Details** tab in **Project Inventory** is currently reflecting the suppression or unsuppression of vulnerabilities at the project level.

**Workaround:** None exists.

### SCA-53169: Project-suppressed vulnerabilities considered not suppressed when policy is applied

Policy is still considering vulnerabilities suppressed at the project level as if they were not suppressed. For example, if you suppress a vulnerability that has a High severity or a CVSS score of 7.5 and have defined a policy that rejects inventory with a CVSS score of 7.4 and above, any inventory associated with the suppressed vulnerability is still being rejected when the policy is applied.

**Workaround:** None exists.

### SCA-52900: Projects containing a vulnerability suppressed at the project level still being retrieved in project search based on that vulnerability ID

In the **Projects** view, you can filter the **Projects** list to those projects currently associated with a specific vulnerability ID. However, projects for which that vulnerability has been suppressed are still showing in the resulting list.

**Workaround:** None exists.

### 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 at the global level 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 user interface.

**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.

### SCA-54637: “Vulnerabilities” bar graph appearing for zero vulnerabilities

When vulnerabilities for a component version suppresses to zero by using the **Suppress Vulnerability** window, the vulnerabilities bar graph still appears for the same component version on the **Versions for <component>** window.

**Workaround:** None exists.

## Web UI

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

### 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:** Refresh the screen.

### SCA-20683: Project details not automatically updating after scan

Project details are not automatically updating after a scan in the Code Insight user interface.

**Workaround:** Refresh the screen.

### SCA-48317: User Interface hangs during project deletion in SQL Server environment

The Code Insight user interface appears to hang while deleting a large codebase scanned project.

**Workaround:** Manually refresh the user interface screen when the required log messages appear. For instance, the following types of log messages appear when the Code Insight user interface gets hanged:

2024-07-05 10:52:03 +0530 WARN [TaskExecutorThread-1413] [ProjectServiceImpl] Project <project-name> and all associated data has been deleted successfully.

2024-07-05 10:52:03 +0530 INFO [TaskExecutorThread-1413] [SchedulerDriverImpl] Completed task: com.palamida.datamodel.model.SchedulerTaskImpl@10e1d7e9[task ID=1413,server ID=1,type=Project Deletion,description=Deletion of Project : <project-name>( Project Id: <project-id> ) ,state=active,context=#Fri Jul 05 10:52:02 IST 2024 ,parent=,message=<null>]

### SCA-54659: "Lookup Component" window displaying the hyperlink text as "Show Version" instead of "Show Instance"

The **Lookup Component** window-accessible while editing or creating an inventory item in the **Analysis Workbench** and on the **Project Inventory** tab-initially fails to display the hyperlink text as **Show Instance** and instead displays it as **Show Version**.

**Workaround:** None exists.

## Code Insight Security Issues

The following is current security issue involving Code Insight.

### SCA-52416: New White Hat vulnerability finding—"Insufficient Transport Layer Protection"

According to a new White Hat vulnerability finding (**50934239**) in Code Insight, the SSL/TLS endpoint used by Code Insight is configured with weak SSL/TLS cipher suites. This issue will be resolved in the near future.

# Legal Information

## Copyright Notice

Copyright © 2025 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.reverera.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.