revenera™

Code Insight 2022 R2 Release Notes

May 2022

Introduction

These Release Notes provide the following information about the Code Insight 2022 R2 release:

- About Code Insight
- Revenera Resources
- New Features and Enhancements
- Resolved Issues
- Special Notes
- Known Issues
- Legal Information

About Code Insight

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

Revenera Resources

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

- In addition to providing case management, the Revenera Community site can help you quickly find answers to your questions by searching content from other customers, product experts, and thought leaders. You can also post questions on discussion forums for experts to answer. For each of Revenera’s product solutions, you can access forums, blog posts, and knowledge base articles.
- You can find documentation for Code Insight and all other Revenera products on the Revenera Product Documentation site.
- The Revenera Learning Center offers free, self-guided online videos to help you quickly get the most out of your Revenera products. You can find a complete list of these training videos in the Learning Center.
- For customers who have purchased a maintenance contract for their product(s), you can submit a support case or check the status of an existing case by making selections on the **Get Support** menu of the Revenera Community.

  https://community.revenera.com

New Features and Enhancements

The Code Insight 2022 R2 release provides new features and enhancements in the following areas:

- Project Inventory
- Project Management
- Scanning and Automated Discovery
- Security Vulnerability Reporting
- User Experience
- REST API Enhancements

Project Inventory

The following new enhancements are available for managing and reviewing project inventory in the **Analysis Workbench** or on the **Project Inventory** tab.

Details About Available Component Versions Now Available When Creating or Editing an Inventory Item

Once users select a component when creating or editing a component-based inventory item in the **Analysis Workbench** or **Project Inventory**, they have an opportunity to view details about all available versions for the component before finalizing the inventory item. They simply click the new **View all versions** link next to the **Component** field in the **Edit Inventory** or **Create Inventory** window. The read-only **Versions for** <componentName> window is opened, showing security vulnerability details and possible licenses for each component version. Users can then make an informed decision about which version to use.

Project Management

The following new enhancement is available for managing Code Insight projects.

New Project Copy Feature

Code Insight now has a Project Copy feature that copies the information from an existing Code Insight project—including its project settings, user information, source-code files and folders, scan evidence, inventory details, and alerts—to a new project. This new feature offers an alternative to project-branching and has the following advantages over the branching process:

- The branching process triggers a full scan of the branched project (which, in most cases, is not needed because the source project already contains base-line scan results that are copied to the branched project). Project Copy simply copies all scan results from the source project to the target project without running a scan on the target.
- The scan run on the target project during the branch process can pull in false-positive inventory that might have been cleaned up in the source project. On the other hand, once the Project Copy process copies inventory information from the source project to the target project, no scan is run.

If the information in the source project had been cleaned up, it remains cleaned up in the target project because no scan is triggered on the copied data.

- As part of the branch-project process, you must confirm or define individual project settings for the branched project. During the Project Copy, source project settings are simply copied to the target project without the need to confirm settings.

The Copy feature is run from the **Manage Project** > **Copy Project** option on a project **Summary** tab. For complete information on how to initiate the copy process and monitor its progress and what types of information are copied to target project during the copy, see “Copying a Project” in the *Code Insight User Guide*.

Scan Agent Plugins

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

Incremental Scanning

Scan-agent plugins now support incremental rescans.

Note ▪ *After the scan agent runs the initial full scan on a remote file system, all subsequent rescans on the file system are incremental (that is, the scan agent scans only those files that are new or have changed since the last scan). No forced full rescans are allowed.*

Scan Exclusions, Dependency Support, and Archive Processing Settings from Project Scan Profile Now Honored

During a scan on a remote file system, a scan-agent plugin now processes the following settings from the scan profile currently associated with the Code Insight project that stores the scan results.

- **Dependency Support**, which determines the how the scan handles dependencies of the top-level inventory item:
    - Processes direct (first-level) dependencies only
    - Processes both direct and transitive dependencies
    - Performs no dependency processing
- **Scan Exclusions**, which determines which files the scan will ignore.
- **Perform Package/License Discovery in Archives**, which enables the processing of archives.

Scan-agent plugins ignore the settings in the profile that deal with the matching of code against the Code Insight data library: **Exact Matches**, **Source Code Matches**, and **Search Terms**. The plugins also ignore **Rescan Options** and **Automatically Add Related Files to Inventory**.

For more information, see “Preparing to Use the Plugins” in the *Code Insight Plugins Guide*.

***Note** ▪ Scan-agent plugins released prior to 2022 R2 are still compatible with Code Insight 2022 R2 and later. However, they do not process scan profile settings, including settings for dependency processing, scan exclusions, and archive processing. Also, when using a pre-2022 R2 plugin to scan files in Code Insight 2022 R2 or later, dependency processing with use of a `codeaware.properties` file is no longer supported.*

Scanning and Automated Discovery

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

Automated Discovery Enhancements

The following automated discovery enhancements are available in this release:

- Support for reporting transitive dependencies in `.csproj` files
- Improved accuracy in reporting inventory in NPM packages

New Button to View Scan Profile Details in Read-Only Mode

A read-only view of the settings for a scan profile is now available from **Scan Profiles** tab (accessed from the **Administration** menu). A new **View** icon in the **Actions** column for each profile opens a window providing a quick overview the profile’s settings.

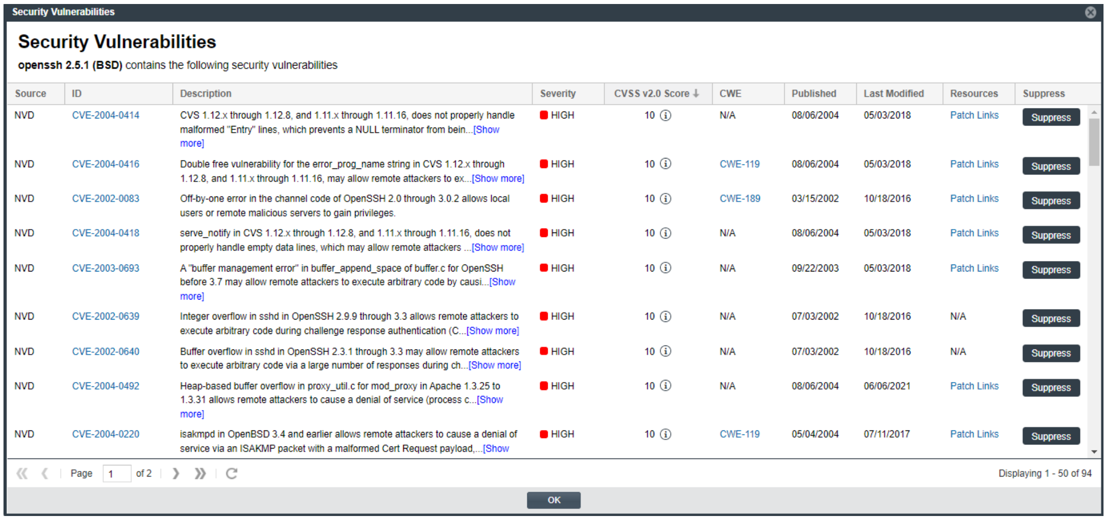
Security Vulnerability Reporting

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

New 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 a new look. The list of vulnerabilities are now shown as a flat list in grid format. The new list maintains all of the vulnerability details of the previous **Security Vulnerabilities** window (including the **Suppress** button) plus provides the following new features:

- A hyperlinked CWE (Common Weakness Enumeration) value for each vulnerability. The link opens to the CWE web page describing the type. (CWE types are developed by a community of national cyber-security organizations.)
- Sorting capabilities on the vulnerability ID and CVSS columns.
- Pagination (50 records per page), enabling you to navigate the list.



Security Vulnerabilities

openssh 2.5.1 (BSD) contains the following security vulnerabilities

Source	ID	Description	Severity	CVSS v2.0 Score ↓	CWE	Published	Last Modified	Resources	Suppress
NVD	CVE-2004-0414	CVS 1.12.x through 1.12.8, and 1.11.x through 1.11.16, does not properly handle malformed "Entry" lines, which prevents a NULL terminator from bein...[Show more]	🟥 HIGH	10 ⓘ	N/A	08/06/2004	05/03/2018	Patch Links	Suppress
NVD	CVE-2004-0416	Double free vulnerability for the error_prog_name string in CVS 1.12.x through 1.12.8, and 1.11.x through 1.11.16, may allow remote attackers to ex...[Show more]	🟥 HIGH	10 ⓘ	CWE-119	08/06/2004	05/03/2018	Patch Links	Suppress
NVD	CVE-2002-0083	Off-by-one error in the channel code of OpenSSH 2.0 through 3.0.2 allows local users or remote malicious servers to gain privileges.	🟥 HIGH	10 ⓘ	CWE-189	03/15/2002	10/18/2016	Patch Links	Suppress
NVD	CVE-2004-0418	serve_notify in CVS 1.12.x through 1.12.8, and 1.11.x through 1.11.16, does not properly handle empty data lines, which may allow remote attackers ...[Show more]	🟥 HIGH	10 ⓘ	N/A	08/06/2004	05/03/2018	Patch Links	Suppress
NVD	CVE-2003-0693	A "buffer management error" in buffer_append_space of buffer.c for OpenSSH before 3.7 may allow remote attackers to execute arbitrary code by causi...[Show more]	🟥 HIGH	10 ⓘ	N/A	09/22/2003	05/03/2018	Patch Links	Suppress
NVD	CVE-2002-0639	Integer overflow in sshd in OpenSSH 2.9.9 through 3.3 allows remote attackers to execute arbitrary code during challenge response authentication (C...[Show more]	🟥 HIGH	10 ⓘ	N/A	07/03/2002	10/18/2016	N/A	Suppress
NVD	CVE-2002-0640	Buffer overflow in sshd in OpenSSH 2.3.1 through 3.3 may allow remote attackers to execute arbitrary code via a large number of responses during ch...[Show more]	🟥 HIGH	10 ⓘ	N/A	07/03/2002	10/18/2016	N/A	Suppress
NVD	CVE-2004-0492	Heap-based buffer overflow in proxy_util.c for mod_proxy in Apache 1.3.25 to 1.3.31 allows remote attackers to cause a denial of service (process c...[Show more]	🟥 HIGH	10 ⓘ	N/A	08/06/2004	06/06/2021	Patch Links	Suppress
NVD	CVE-2004-0220	isakmpd in OpenBSD 3.4 and earlier allows remote attackers to cause a denial of service via an ISAKMP packet with a malformed Cert Request payload,...[Show	🟥 HIGH	10 ⓘ	CWE-119	05/04/2004	07/11/2017	Patch Links	Suppress

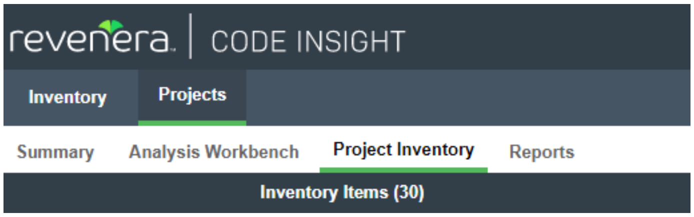
User Experience

This release includes the following enhancement to the user's overall experience in the Code Insight Web UI.

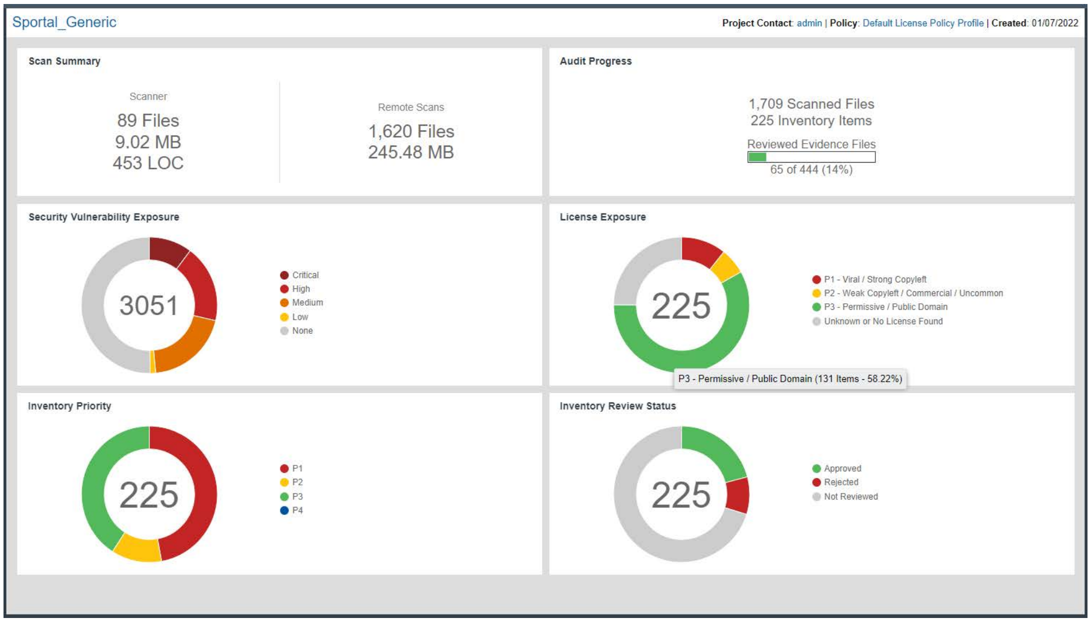
Web UI Facelift

The Code Insight Web user interface now has more modern appearance in its color scheme, the look of tabs, and cleaner project dashboard design.

The tab currently in focus is now under-highlighted.



The project dashboard now shows the legends to the right of the graphs instead of below them to conserve up-and-down space. Graph percentage information is no longer shown in text next to a graph but is available in tool tips as you hover over graph segments.



REST API Enhancements

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

- New APIs
- Updates to Existing APIs

New APIs

The following new REST APIs were added in this release:

Table 1 ▪ New APIs in this Release

Resource	API Name/Endpoint	Method	Description
License	**License lookup based on short name** `/licenses/{shortName}`	GET	Retrieves details for a license by its short name.
Scan profiles	**Get profiles for project** `/profiles/{projectId}`	GET	Retrieves the scan profile (and its settings) associated with a given project ID.

Updates to Existing APIs

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

Table 2 ▪ Updates to Existing APIs

Resource	API Name/Endpoint	Method	Function Description
Component	**Get Component** `/components/{componentId}`	GET	New **patchURLs** field for each security vulnerability listed in the response for the given component. The field lists the paths for any patches that address the vulnerability.
	Get Component version vulnerabilities `/components/{versionId}/vulnerabilities`	GET	New **patchURLs** field for each security vulnerability listed in the response for the given component version. The field lists the paths for any patches that address the vulnerability.
Inventory	**Get the inventories of file/folder ids** `inventories/search`	GET	New **patchURLs** field for each security vulnerability listed for an inventory item in the response. The field lists the paths for any patches that address the vulnerability.
	Get details of an inventory `inventories/{inventoryId}`	GET	New **patchURLs** field for each security vulnerability listed in the response for the given inventory item. The field lists the paths for any patches that address the vulnerability.
	Get vulnerability details of an inventory `inventories/{inventoryId}/vulnerabilities`	GET	New **patchURLs** field for each security vulnerability listed in the response for the given inventory item. The field lists the paths for any patches that address the vulnerability.
Project	**Get Project information** `/projects/{projectId}`	GET	New **deleteEmptyInventory** field added to response, so that users can see whether the project allows an import or scan to delete inventory with no associated files.
	Get Project Inventory `/projects/inventory/{projectId}`	GET	New **patchURLs** field for each security vulnerability listed for an inventory item in the response. The field lists the paths for any patches that address the vulnerability.
Users	**Search Users** `/users/search`	GET	Administrative permissions removed so that any user can use this API. Any user can now obtain user ID information required by **Task** APIs.

Resolved Issues

The following issues are resolved in this release.

Table 3 ▪ Resolved Issues

Issue	Resolution Notes
SCA-24642	Encryption of proxy credentials now supported. Users have the option to store the proxy password as an encrypted string in a secure vault (configured using a Tomcat Vault utility shipped with Code Insight). Instructions are found in “Configuring a Proxy Connection Using an Encrypted Password” in the *Code Insight Installation and Configuration Guide*.
SCA-33789	A user-defined name for **License Only** inventory no longer resetting to the default “Files under <licenseName>” on its own.
SCA-35874	The UI, reports, and API responses now showing files that have the same name but use different case spellings as individual files.
SCA-39928	User documentation enhanced to specify codebase size limitations for uploads and scans.
SCA-40070	In the response for the GET **scminstances** API, the masked value '******' for the user **password** field is no longer displayed for those SCM instances that have no user credentials defined.
SCA-40004	Issues with loading or adding component libssh 0.7.3 now resolved.
SCA-40488	User documentation for storing Git credentials during the configuration of an SCM (Source Code Management) Git instance now updated with additional pertinent details.
SCA-40677	Synchronization with Git repository no longer failing with a “too many arguments” or “empty string is not a valid pathspec” exception. Previously, this exception occurred when SCM instance settings contained trailing white space, which the synchronization process now trims.
SCA-41118	Deletion of inventory that has dependencies with custom fields now completing successfully.
SCA-41274	When the length of an unresolved component version is more than 64 bytes, the Jenkins scan agent is now creating the inventory with an unknown version instead of a custom version, enabling the scan to complete successfully.
SCA-41300	Proprietary inventory now flagged as Medium or Low confidence instead of High confidence (insinuating a false-positive).
SCA-41479	Project names defined with double spaces now properly displayed as such and are processed properly during searches.

Special Notes

The following Code Insight notes discuss special changes or deprecations in functionality.

Support for the JFrog Artifactory Plugin Temporarily Removed

Support for the JFrog Artifactory plugin for remote scans has been temporarily removed as of Code Insight 2022 R1.

GitHub.com Change in Authentication Requirements for Git URLs

Starting on August, 16, 2021, connections to GitHub URLs require token-based input instead of a password for authentication. This requirement affects those Code Insight SCM (Source Code Management) processes that obtain scan data through synchronization with a remote GitHub repository. Note that Code Insight handles this authentication change internally, allowing users to continue to set up the SCM instance for their connection to a GitHub repository as they normally do.

CVE-Feed APIs (1.0) Deprecated/Discontinued by NVD

Code Insight relies on feeds from the National Vulnerability Database (NVD) to obtain the latest CVE information. Recently, NVD switched the feed version from 1.0 to 2.0. In Code Insight 2020 R4, updates were made to accommodate the schema changes incurred by the switch.

To ensure your Code Insight system obtains the latest security vulnerability information, you must migrate to Code Insight 2020 R4 or later.

Known Issues

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

- All-Project Inventory View
- Application Life Cycle Management (ALM) Support
- Automated Workflow for Inventory Review/Publication
- Electronic Updates
- Export and Import
- Installation, Upgrades, and Configuration
- Inventory History
- Manual Codebase Analysis
- Performance
- Project Inventory
- Project Management
- Project Reporting
- REST APIs

- Scan Agent Plugins
- Scanning and Automated Discovery
- Source Code Management (SCM) Support
- Vulnerability Suppression/Unsuppression
- Web UI

All-Project Inventory View

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

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

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

Workaround: None exists.

Application Life Cycle Management (ALM) Support

The following are known issues with Code Insight ALM support.

SCA-39709: Invalid user name accepted in ALM instances configured for Jira in the Cloud

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

Workaround: None exists.

Automated Workflow for Inventory Review/ Publication

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

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

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

Workaround: None exists.

Electronic Updates

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

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

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

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

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

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

```
jquery (MIT)
```

Two possible workarounds are available.

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

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

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

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

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

The following inventory mapping existed in inventory:

```
concurrent-ruby 1.1.9 (MIT License)
```

This component was mapped with License id 744.

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

The inventory item was remapped as follows:

```
concurrent-ruby 1.1.9 (MIT-Style)
```

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

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

Workaround: Follow these steps:

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

Export and Import

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

SCA-3222: Import overrides inventory details

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

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

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

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

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

Installation, Upgrades, and Configuration

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

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

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

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

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

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

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

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

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

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

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

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

Inventory History

The following are known issues with the Inventory History feature.

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

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

Workaround: None exists.

Manual Codebase Analysis

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

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

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

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

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

Workaround: None exists.

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

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

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

Workaround: None exists.

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

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

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

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

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

Workaround: None exists.

SCA-22398: Licenses not highlighted even though evidence exists

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

Workaround: None exists.

SCA-22308: “Email/URLs” evidence truncated

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

Workaround: None exists.

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

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

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

Performance

The following are known issues with Code Insight performance.

Performance slower with MySQL 8 than with MySQL 7

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

Project Inventory

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

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

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

Workaround: None exists.

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

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

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

Project Management

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

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

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

Workaround: None exists.

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

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

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

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

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

Workaround: None exists.

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

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

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

Project Reporting

The following are known issues with Code Insight reporting.

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

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

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

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

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

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

REST APIs

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

SCA-32608: Get Project Inventory REST API Returns Duplicate Inventory

The **Get Project Inventory** REST API can intermittently return duplicate inventory when Code Insight is configured with a SQL Server database.

Workaround: None exists.

SCA-40410: “Component Search” REST API Not Consistently Retrieving Custom Component Data

The **Component Search** REST API currently does not retrieve information about a custom component if either of these conditions exist:

Condition 1: The custom component is newly created.

Condition 2: The name of the custom component contains an upper-case letter.

Workaround:

For Condition 1: Run an Electronic Update to index the new custom component.

For Condition 2: 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. However, the issue will be addressed in an upcoming release.

Scan Agent Plugins

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

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

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

Workaround: None exists.

SCA-41154: No scan agent support for full rescans

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

Workaround: None exists.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Workaround: None exists.

Scanning and Automated Discovery

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

SCA-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-34070: Scan status not immediately in effect after “Stop Scan” issued

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

Workaround: None exists.

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

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

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

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

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

Workaround: None exists.

Inventory automatically published during previous scan now unpublished after rescan

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

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

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

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

Workaround: None exists.

SCA-7820: Some NPM version patterns are not supported

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

Workaround: None exists.

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

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

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

Source Code Management (SCM) Support

The following are known issues with Code Insight SCM support.

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

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

Workaround: None exists

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

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

Workaround: None exists.

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

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

The following issue has been logged with TFS:

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

Workaround: None exists.

Vulnerability Suppression/Unsuppression

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

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

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

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

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

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

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

Workaround: Manually refresh the browser screen.

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

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

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

Workaround: Manually refresh the browser screen.

Web UI

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

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

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

SCA-20683: Project details not automatically updating after scan

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

Workaround: Refresh the screen.

Legal Information

Copyright Notice

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

Intellectual Property

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

Restricted Rights Legend

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