

Code Insight 2021 R4 Release Notes

November 2021

Introduction	2
About Code Insight	2
Revenaera Resources	2
New Features and Enhancements	3
Automated Workflow for Inventory Review/Publication	3
Electronic Updates	3
Installation, Upgrades, and Configuration	6
Project Inventory	7
Scanning and Automated Discovery	9
Security Vulnerabilities	10
REST API Enhancements	11
New APIs	11
Updates to Existing APIs	12
Resolved Issues	12
Special Notes	14
Known Issues	14
All-Project Inventory View	15
Automated Workflow for Inventory Review/Publication	15
Electronic Updates	15
Export and Import	16
Installation, Upgrades, and Configuration	17
Inventory History	18
Manual Codebase Analysis	18
Performance	19
Project Administration and Management	19
Project Inventory	19
Project Reporting	19
REST APIs	20
Scan Agent Plugins	20
Scanning and Automated Discovery	21
Source Control Management (SCM) Support	23
Vulnerability Suppression/Unsuppression	23
Web UI	24
Legal Information	25

Introduction

These Release Notes provide the following information about the Code Insight 2021 R4 release:

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

Reverera Resources

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

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

<https://community.reverera.com>

New Features and Enhancements

The Code Insight 2021 R4 release provides new features and enhancements in the following areas:

- [Automated Workflow for Inventory Review/Publication](#)
- [Electronic Updates](#)
- [Installation, Upgrades, and Configuration](#)
- [Project Inventory](#)
- [Scanning and Automated Discovery](#)
- [Security Vulnerabilities](#)
- [REST API Enhancements](#)

Automated Workflow for Inventory Review/ Publication

The following enhancements to the automated work flow for inventory publication and review have been added in this release.

Access to Details About the Component Used in a Component Policy

An information icon is now provided next to each component policy defined on the **Policy Details** window. When you click the icon, a window opens, displaying pertinent details about the component for which the policy is defined.

Electronic Updates

The following enhancements have been added to the Electronic Update process in this release.

Notification Banner Displayed When an Electronic Update Is in Progress

Whenever an Electronic Update is in progress, a banner is displayed across the top of the Code Insight screen, indicating that an update is running and that scheduled scans will resume once the update completes. The banner is shown for any Electronic Update—whether server or local, forced or automatically run by schedule—and persists across the top of all Code Insight pages until the update is complete.

Automatic Remapping of Existing Inventory Names According to Changes in the Data Library

Once an Electronic Update (in Code Insight 2021 R4 or later) is complete, a new post-update service will automatically update names of existing inventory based on the following changes made to the Code Insight Data Library:

- The latest short names for licenses (to support the common convention of using the license's short name in inventory names)

- The latest component-license mapping changes



Note • *This automatic remapping applies to only system-generated inventory, not to custom inventory.*

The following sections provide more information about this remapping effort:

- [Short Name Changes](#)
- [Component-License Remapping](#)
- [Electronic Update and Post-Update Service Scenarios](#)
- [Remapping of Inventory Names: Impact on the Project Import Process](#)

Short Name Changes

When a specific license short name is changed, it is released as part of an Electronic Update and updated to your Code Insight Data Library. For example, suppose the License Id 744 currently in the library has the short name “MIT License”. After the Electronic Update, the short name for License Id 744 is updated to “MIT-Style” in the Data Library.

Once the Electronic Update completes, the post-update service is automatically run to update existing inventory names with the latest associated license short name. Without this update, an inconsistency can exist between an inventory item’s actual short name and the one used in the inventory name.

Component-License Remapping

If the Electronic Update applies a component-license mapping change to the Data Library (for example, the Acorn component is now mapped to the Apache License), this change is not reflected in the names of your already scanned inventory items, thus resulting in an inconsistency between the actual mapping and the inventory name.

Once the Electronic Update completes, the post-update service is automatically triggered to update existing inventory names with their latest component-license mappings (which can also incorporate new license short names).

Additional Examples

The following examples show how a change to a license short name or a component-license mapping is propagated to the name of an inventory item in your project.

Example Short Name Change

Apache-1.0 is renamed to **Apache License-1.0**.

- **Current inventory:** jquery (**Apache-1.0**)
- **Expected inventory after the Electronic Update and post-update service:** jquery (**Apache License-1.0**)

Example Component-License Mapping Change

Acorn (**MIT**) is remapped to the **GPL** license.

- **Expected inventory after the Electronic Update and post-update service:** Acorn (**GPL**)

Electronic Update and Post-Update Service Scenarios

For your reference, the following table compares the results of license-remapping scenarios in Code Insight 2021 R4 or later (or in a pre-2021 R4 version) when you run or do not run the latest Electronic Update. Note the following about the table:

- The “Latest Electronic Update Run?” column refers to latest Electronic Update that is available at the time of the Code Insight 2021 R4 release and thereafter.
- The “Results” column refers to the previous examples in the [Additional Examples](#) section.

Release	Latest Electronic Update Run?	License-Remapping Results for Inventory	Notes
2021 R4 (post-update service provided)	Yes	jquery (Apache License-1.0) Acorn (GPL)	The correct license short name is applied to jquery; and the Acorn component is remapped to its new license.
2021 R4 (post-update service provided)	No	jquery (Apache-1.0) Acorn (MIT)	No license-remapping is performed on your inventory.
2021 R3 and earlier (post-update service not provided)	Yes	jquery (Apache-1.0) Acorn (MIT)	<p>No license-remapping is performed on your inventory. However, in this scenario, the value for Possible Licenses will show the newly mapped license for the component, as stored in the Code Insight Data Library. (For example, the Possible Licenses value for “Acorn (MIT)” shows GPL.)</p> <p>To correct license mappings for inventory throughout your Code Insight system, users in this scenario can run the cleanup SQL script found in the codeinsight-MITcleanupPackage archive. (Download this archive from the Product and Licensing Center.)</p>
2021 R3 and earlier (post-update service not provided)	No	jquery (Apache-1.0) Acorn (MIT)	No remapping is performed on your inventory.

Remapping of Inventory Names: Impact on the Project Import Process

When you are using Code Insight 2021 R4, projects that are exported after running an Electronic Update available at the time of the 2021 R4 release (and thereafter) will have no problem importing the project data. However, projects that are exported *before* this current Electronic Update is run will have import issues with license-mapping inconsistencies in the target projects. For a successful import of such projects, perform the following steps. (Be sure that you have already run the current Electronic Update.)



Note - *These same steps can be used by 2021 R3 and earlier users to perform an import after they have run the current Electronic Update.*

1. Import the source project to the target project.
2. Run the Code Insight cleanup SQL script to correct the license-mapping inconsistencies in the Code Insight system, including the target project. (To obtain this script, download the codeinsight-MITCleanupPackage archive from the Product and Licensing Center, and extract the script and its instructions.)
3. For the target project, select the **On data import or rescan, delete inventory with no associated files** option on the **Edit Project** window. (From the project **Summary** tab, select **Manage Project | Edit Project | General** tab.)
4. Upload the codebase and scan.



Note - *Only system-generated inventories can have incorrect license mappings are removed. License mappings for Custom inventory are not processed.*

Installation, Upgrades, and Configuration

This release provides the following enhancement to the Code Insight installation, upgrade, and configuration processes.

Support for Windows 2019

Code Insight can now be installed on the Windows 2019 platform.

Silent Installation Instructions Added to User Documentation

Instructions for performing a silent installation of Code Insight are now available in the *Code Insight Installation & Configuration Guide*.

Project Inventory

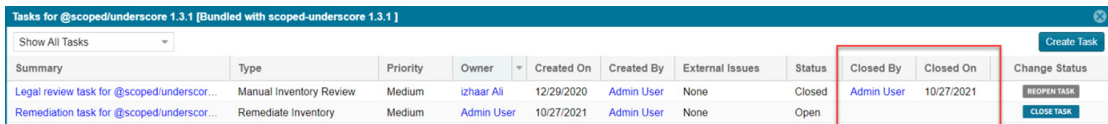
The following new enhancements and features are available for managing and reviewing project inventory in the **Analysis Workbench** or on the **Project Inventory** tab.

- [New Information About Closed Tasks](#)
- [Custom Fields for Inventory](#)

New Information About Closed Tasks

The **Tasks** list for a given inventory item now includes two new columns—**Closed By** and **Closed On**—to indicate who closed the task and when. You can click the **Closed By** link to send an email to the user who closed the task.

If a task is open, these fields are blank.



The screenshot shows a table titled "Tasks for @scoped/underscore 1.3.1 [Bundled with scoped-underscore 1.3.1]". The table has columns: Summary, Type, Priority, Owner, Created On, Created By, External Issues, Status, Closed By, Closed On, and Change Status. Two rows are visible: "Legal review task for @scoped/underscore..." (Manual Inventory Review, Medium, izhaar Ali, 12/29/2020, Admin User, None, Closed) and "Remediation task for @scoped/underscore..." (Remediate Inventory, Medium, Admin User, 10/27/2021, Admin User, None, Open). The "Closed By" and "Closed On" columns are highlighted with a red box, showing "Admin User" and "10/27/2021" respectively for the closed task.

Custom Fields for Inventory

The standard fields used to describe OSS and third-party inventory in Code Insight might not provide all the detail that your site requires to process and finalize a Bill of Materials for your product. For example, you might want to know whether a thorough inbound review of a given component has been completed or what encryption algorithms are used for a given inventory item.

To address this need for additional detail, Code Insight now enables the System Administrator to create and manage custom fields that are available for inventory across all projects in your Code Insight system. Analysts and reviewers can then update the field's value for any inventory item. They can also filter inventory on custom field values at the project and global levels.

The following sections provide an overview of managing and using custom fields:

- [Creating and Managing Custom Inventory Fields](#)
- [Example Custom Field in the Web UI](#)
- [New Fields to Search Inventory by Custom Field Values](#)
- [Accessing Custom Field Values through the REST Interface](#)

Creating and Managing Custom Inventory Fields

Custom inventory fields are created and managed from the new **Custom Fields for Inventory** section on the **System Settings** tab, located on the **Administration** page.



The screenshot shows the "Flex Fields for Inventory" management interface. It includes an "Add Field" button and a table with columns: Enabled, Visible in UI, Field Label, Help Text, and Action. Two fields are listed: "Exclude from Notices Report" and "Encryption Algorithms".

Enabled	Visible in UI	Field Label	Help Text	Action
Yes	Yes	Exclude from Notices Report	Set to 'N' to make this inventory item NOT part of notific...	
Yes	Yes	Encryption Algorithms	Specify a comma separated list of supported algorit...	

Depending on its configuration, a custom inventory field can be made available in the Code Insight Web UI (that is, both on the **Project Inventory** tab and in the **Analysis Workbench**) and through REST API. Alternatively, the field can be configured to *not* be visible in the Web UI but be available through REST API only.

Currently, a maximum of five custom inventory fields can be created.

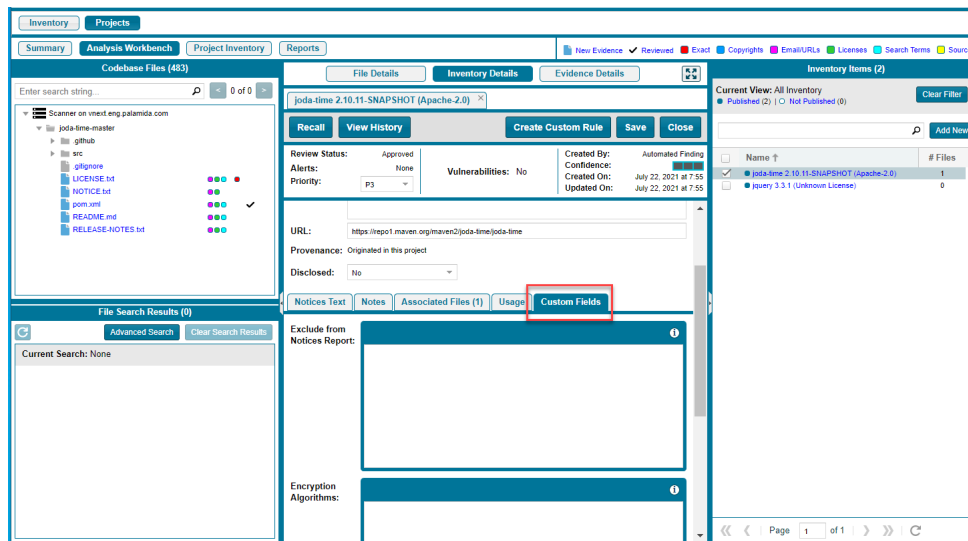


Note - Once a custom field is created, it cannot be deleted. However, it can be disabled and re-enabled as needed.

For more information about creating and managing custom inventory fields, see the “Configuring Code Insight” chapter in the *Code Insight Installation & Configuration Guide*.

Example Custom Field in the Web UI

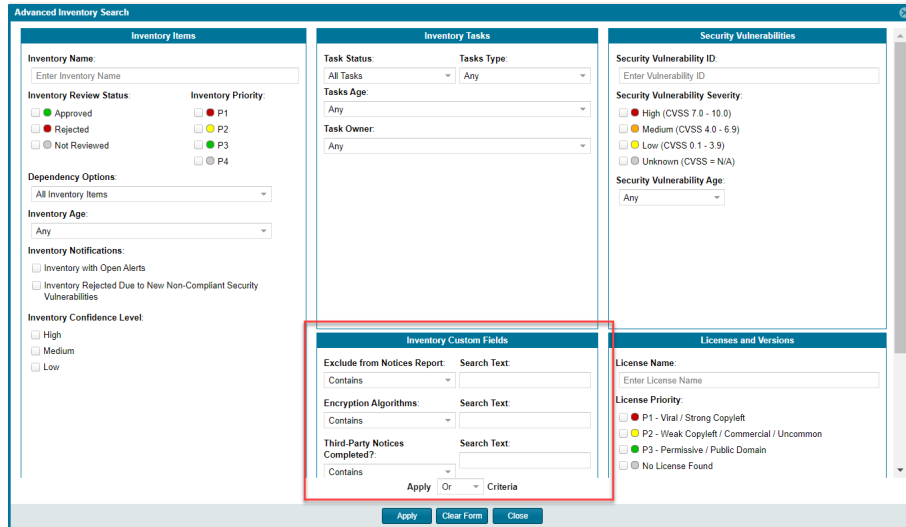
In the **Analysis Workbench**, custom fields are listed on a new **Custom Fields** tab on the **Inventory Details** tab for a specific inventory item, as shown in this example:



In **Project Inventory**, the custom fields are available on the **Inventory Details** tab for a specific inventory item. For information about adding and editing values in the custom fields in the Web UI, refer to the *Code Insight User Guide*.

New Fields to Search Inventory by Custom Field Values

The **Advanced Inventory Search** dialog (for project inventory or global inventory) includes a new section that enables users to search inventory by custom field values. In the following example, three custom fields have been created in the Code Insight system and are therefore available to set up as search criteria.



Accessing Custom Field Values through the REST Interface

Users can use the **Get details of an inventory** and **Get project inventory** REST APIs to view custom-field values for inventory items.



Note - The ability to use the **Create inventory** and **Update inventory** REST API to create and update the custom-field values for inventory items will be added in an upcoming release.

For information about using these REST APIs, refer to the *Rest API Guide* Swagger documentation.

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.

SHA-1 Support Enabled by Default

The SHA-1 feature is now automatically enabled when a customer site first installs Code Insight version 2021 R4 or greater or migrates from a pre-2021 R4 version. (In the previous release, this feature was disabled by default, causing the System Administrator to perform an extra step to enable the feature.) This feature calculates the SHA-1 digests for files during scans. (MD5 digests are always calculated whether or not SHA-1 support is enabled.)

For complete details about this feature, see “Enabling Calculation of SHA-1 Digests for Scanned Files” in the *Code Insight Installation & Configuration Guide*.

Support for the GitLab Forge

Automated Analysis has added support for the detection of OSS and third-party components in repositories in the GitLab forge.

Support for Direct Dependencies Go Modules

Automated Analysis has added support for the detection of direct dependencies in `go.mod` and `_go.mod` manifest files. Currently, this detection is supported from the Github forge only.

Security Vulnerabilities

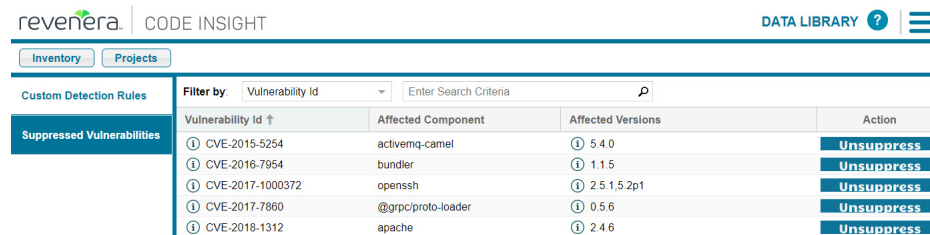
This release provides the following enhancements to Code Insight's reporting of the security vulnerabilities found in open-source or third-party components:

- [Web UI Support for Unsuppressing Vulnerabilities](#)
- [Vulnerability Dates in the Web UI](#)

Web UI Support for Unsuppressing Vulnerabilities

Previously, securities vulnerabilities could be unsuppressed through the Code Insight REST interface only.

The System Administrator can now use the Web UI to unsuppress a security vulnerability for one, some, or all of the component versions for which it was previously suppressed. This operation is initiated by clicking the new **Unsuppress** button for a vulnerability listed on the **Suppressed Vulnerabilities** view (accessed from the **Data Library** option on the Code Insight system menu).



The screenshot shows the Code Insight web interface. At the top, there is a navigation bar with 'revenera | CODE INSIGHT' on the left and 'DATA LIBRARY ?' on the right. Below the navigation bar, there are tabs for 'Inventory' and 'Projects'. A 'Custom Detection Rules' section is visible on the left. The main content area displays a table of 'Suppressed Vulnerabilities'. The table has columns for 'Vulnerability Id', 'Affected Component', 'Affected Versions', and 'Action'. Each row includes an information icon, a vulnerability ID, the affected component name, the affected versions, and an 'Unsuppress' button.

Vulnerability Id ↑	Affected Component	Affected Versions	Action
📘 CVE-2015-5254	activemq-camel	📘 5.4.0	Unsuppress
📘 CVE-2016-7954	bundler	📘 1.1.5	Unsuppress
📘 CVE-2017-1000372	openssh	📘 2.5.1.5.2p1	Unsuppress
📘 CVE-2017-7860	@grpc/proto-loader	📘 0.5.6	Unsuppress
📘 CVE-2018-1312	apache	📘 2.4.6	Unsuppress

The new **Unsuppress a Vulnerability** window opens, enabling you to complete the unsuppression operation:



The screenshot shows the 'Unsuppress Vulnerability' dialog window. It contains the following fields and information:

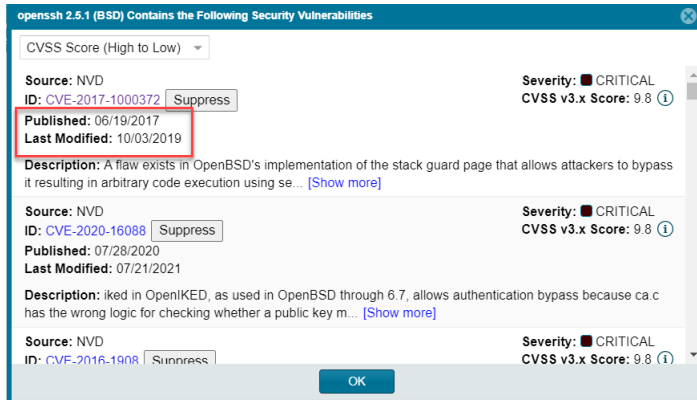
- Vulnerability Id:** CVE-2019-5421
- Source:** NVD
- Severity:** High
- CVSS v2.0 Score:** 7.5 ⓘ
- Description:** Plataformatec Devise version 4.5.0 and earlier, using the lockable module contains a CWE-367 vulnerability in The 'Devise::Models::Lockable' class, more specifically at the '#increment_failed_attempts' method. File location: lib/devise/models/lockable.rb that can result in Multiple concurrent requests can prevent an attacker from being blocked on brute force attacks. This attack appear to be exploitable via Network connectivity - brute force attacks. This vulnerability appears to have been fixed in 4.6.0 and later.
- Affected Component:** devise (Id: 13028101)
- Version Scope:** All Suppressed Versions (dropdown menu)
- Select Version:** (dropdown menu)
- Unsuppress Remarks:** (text area)

For More Information About This Feature

For more information about the Vulnerability Suppression feature, refer to “Suppressing/Unsuppressing Security Vulnerabilities” in the *Code Insight User Guide*.

Vulnerability Dates in the Web UI

The **Security Vulnerabilities** dialog now shows the dates of original publication and last revision for security vulnerabilities, as captured from the vulnerability source (NVD, Secunia, or another advisory). In the previous release, these dates were available only through the REST interface.



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
Inventory	Get history of an inventory inventories/ {inventoryId}/history	GET	Retrieves the history of revisions for a given inventory item. Revisions are grouped by Revision IDs.

Updates to Existing APIs

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

Table 2 - Updates to Existing APIs

Resource	API Name/Endpoint	Method	Description
Inventory	Get details of an inventory inventories/ {inventoryId}	GET	Response contains a new customFields section, listing the custom fields and their values for the given inventory item.
Project	Get project inventory project/inventory/ {projectId}	GET	Response contains a new customFields section for each project inventory item, listing the custom fields and their values for that item.

Resolved Issues

The following issues are resolved in this release.

Table 3 - Resolved Issues

Issue	Resolution Notes
SCA-30568	In previous releases, synchronizing a Code Insight project with a Perforce repository to obtain a codebase could result in large amounts of Perforce log data being added to Tomcat logs. This issue has been fixed.
SCA-32993	Clicking the Search Files button on the Evidence Details tab (Analysis Workbench) to locate files containing selected evidence now successfully produces results, despite the number of evidence lines selected or the number of files found.
SCA-32994	When multiple inventory items are selected for deletion, all selections are now successfully deleted.
SCA-32995	The time required for deleting multiple inventory items has improved.
SCA-33017	Users can now successfully rename projects from within the Project Tree.
SCA-35884	Export/import times have improved.
SCA-36137	Transitive dependencies are now found as expected in Google Maven repositories.
SCA-36148	When Code Insight is run in offline mode, first-level dependencies are now being reported as expected for certain package managers.
SCA-36784	The issue in which scan and report-generation tasks remain indefinitely in queue in Scheduled mode has been resolved.

Table 3 - Resolved Issues (cont.)

Issue	Resolution Notes
SCA-36868	Top-level inventory items are now being reported as expected during scans when Code Insight is run in offline mode.
SCA-37009	A new attribute, <code>SCHEMA_POPULATED_WARNING</code> , has been added to the Code Insight silent installation to control whether the existing Code Insight database should be overwritten during installation. If this attribute value is missing, the installation is rolled back. For more information, see the <i>Code Insight Installation & Configuration Guide</i> .
SCA-37301	The user's authentication token is now masked in the Jenkins scan-agent plugin and Jenkins Scheduler plugin.
SCA-37488	Instructions on how to perform a silent Code Insight installation are now available in the <i>Code Insight Installation & Configuration Guide</i> .
SCA-37495	The Swagger description for the Create Project REST API now includes a note to inform users that the <code>folderName</code> property does not support the full path name.
SCA-37577	Usage Handling options in the import or project-branching UI have been relabeled for clarity.
SCA-37668	Proxy issues with the Jenkins scan-agent plugin and the Jenkins Scheduler plugin are now resolved.
SCA-37780	The upgraded Git SCM connector in this release resolves issues with user credentials being erroneously exposed in file contents (as part of URL text) in the Analysis Workbench . Additional configuration is required secure these credentials, as described in "Configuration to Ensure Proper Storage of User Credentials" in the <i>Code Insight Installation & Configuration Guide</i> .
SCA-37861	Records for revisions to inventory priority values that never occurred are no longer erroneously added to Inventory History .
SCA-37941	The calls made by the Jenkins scan-agent plugin to Amazon Web Services now properly acknowledge proxy configuration information so that the calls no longer fail.
SCA-38356	The WIP (Work in Progress) inventory items created during a scan for <code>.cproj</code> files that have no <code>rootnamespace</code> value are no longer published. This fix can save users time in cleaning up unnecessary inventory.
SCA-38363	A record for a Notices Text field revision that never occurred is no longer erroneously added to Inventory History for a custom inventory item. Previously, the erroneous revision was added after the first update to the inventory item in the Analysis Workbench .

Special Notes

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

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 has been addressed for those Code Insight SCM (Source Code Management) processes that obtain scan data through synchronization with a remote GitHub repository. 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](#)
- [Automated Workflow for Inventory Review/Publication](#)
- [Electronic Updates](#)
- [Export and Import](#)
- [Installation, Upgrades, and Configuration](#)
- [Inventory History](#)
- [Manual Codebase Analysis](#)
- [Performance](#)
- [Project Administration and Management](#)
- [Project Inventory](#)
- [Project Reporting](#)
- [REST APIs](#)
- [Scan Agent Plugins](#)
- [Scanning and Automated Discovery](#)
- [Source Control Management \(SCM\) Support](#)
- [Vulnerability Suppression/Unsuppression](#)

- [Web UI](#)

All-Project Inventory View

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

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

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

Workaround: None exists.

Automated Workflow for Inventory Review/Publication

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

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

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

Workaround: None exists.

Electronic Updates

The following are known issues with the Code Insight Electronic Update.

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 Reverera Support for assistance.

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

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

Workaround: Should you encounter the above error, install the JRE manually. Download JRE 8u192 [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 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>.)

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

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

Workaround: None exists.

SCA-22398: Licenses not highlighted even though evidence exists

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

Workaround: None exists.

SCA-22308: "Email/URLs" evidence truncated

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

Workaround: None exists.

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

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

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

Performance

The following are known issues with Code Insight performance.

Performance slower with MySQL 8 than with MySQL 7

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

Project Administration and Management

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

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

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

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

Workaround: None exists.

Project Inventory

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

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

The triggering event for applying policy to project inventory is “Publish” (not scan). Policies are applied during the initial scan if the default setting **Automatically publish system-created inventory items** is 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 Reporting

The following are known issues with Code Insight reporting.

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

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

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

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

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

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

REST APIs

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

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

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

Workaround: None exists.

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

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

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

Scan Agent Plugins

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

After 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-31486, 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 Control Management (SCM) Support

The following are known issues with Code Insight SCM support.

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

Copyright © 2021 Flexera Software

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

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

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

Intellectual Property

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

Restricted Rights Legend

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