

Code Insight 2021 R3 Release Notes

August 2021

Introduction	2
About Code Insight	2
New Features and Enhancements.....	2
Automated Workflow for Inventory Review/Publication.....	2
Electronic Updates	3
Project Data Export and Import.....	3
Project Inventory	3
Scanning and Automated Discovery.....	4
Security Vulnerabilities.....	4
User Experience	6
REST API Enhancements.....	7
New APIs.....	7
Updates to Existing APIs	8
Resolved Issues.....	9
Special Notes	11
Known Issues	11
All-Project Inventory View	12
Automated Workflow for Inventory Review/Publication.....	12
Export and Import.....	12
Installation, Upgrades, and Configuration.....	13
Inventory History	14
Manual Codebase Analysis	14
Performance	15
Project Administration and Management.....	15
Project Inventory	15
Project Reporting	16
REST APIs.....	16
Scan Agent Plugins.....	16
Scanning and Automated Discovery.....	17
Source Control Management (SCM) Support	19
Vulnerability Suppression	20
Web UI.....	21
Legal Information	22

Introduction

These Release Notes provide the following information about the Code Insight 2021 R3 release:

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

New Features and Enhancements

The Code Insight 2021 R3 release provides new features and enhancements in the following areas:

- [Automated Workflow for Inventory Review/Publication](#)
- [Electronic Updates](#)
- [Project Data Export and Import](#)
- [Project Inventory](#)
- [Scanning and Automated Discovery](#)
- [Security Vulnerabilities](#)
- [User Experience](#)
- [REST API Enhancements](#)


Automated Workflow for Inventory Review/ Publication

The following are enhancements to the automated workflow for inventory review and publication in Code Insight. These include enhancements to policies that configure this workflow.

Ability to Create Custom Licenses from the Policy Details Window

Policy managers can now create a custom license when adding or editing a license policy from the **Policy Details** window. They create the license by clicking the new **Create Custom License** button on the **Add (or Edit) License and Usage Criteria** window. Once created, the license is added to the **License** dropdown list and is in focus for immediate association with the policy.

New Information Icons for License Policies

A new  information icon to the left of each license policy on the **Policy Details** window enables users to view information about the license associated with the policy, including its attributes and license text.

Electronic Updates

The following enhancement has been added to the Electronic Update process in this release.

Support for SFTP

By default, Electronic Update files are downloaded over HTTP. However, you can configure the update process to use SFTP instead, so that the update files are downloaded either from Revenera's SFTP server or from your own local SFTP server. For additional security, you can also configure a proxy server to handle communications between the SFTP server and Code Insight.

For complete details, see “Configuring the Use of SFTP for Obtaining Update Files” in the *Code Insight Installation & Administration Guide*. For instructions on running an Electronic Update over SFTP, see “Running Server Electronic Updates” and “Running Local Electronic Updates” in the same guide.

Project Data Export and Import

This release provides the following enhancement to the project data export and import processes.

New Option for Handling Inventory Usage Attributes During Imports

A new Inventory **Usage Handling** parameter has been added to the **Import Project Data** window. This parameter determines whether the import copies the current Usage attributes for inventory items to the target project or resets the attributes to their default value (Unknown) in the target project.

The **Import project data** REST API has also been updated to support this new parameter. See [Updates to Existing APIs](#).

Project Inventory

The following new feature is available for managing and reviewing project inventory in the **Analysis Workbench** or from the **Project Inventory** tab.

Inventory Update History

Users can now view the list of updates made to a given inventory item. By default, the updates are listed in descending order by date so that you see the most recent updates first. Each update record identifies—among other details—the update type, the user who made the update, and the before-and-after values in the update. Users can access this history by clicking the **View History** button on either the **Inventory Details** pane in the **Analysis Workbench** or the **Inventory Details** tab on the **Project Inventory** tab.

Scanning and Automated Discovery

This release includes the following enhancement to the Code Insight codebase scan and its Automated and Advanced Analysis techniques.

SHA-1 Support

Code Insight automatically calculates the MD5 digest for project files during a scan as a means to determine which files have changed between scans and to “exact match” scanned files with OSS or third-party files (whose digests are stored in the Code Insight Compliance Library).

Starting in this release, Code Insight also supports SHA-1 digests. A customer site has the option to configure Code Insight to calculate file SHA-1 digests along with MD5 digests during scans.

To enable or disable SHA-1 support, the Code Insight database administration sets a new global property in the Code Insight database. (By default, this support is disabled when a customer site first installs Code Insight version 2021 R3 or greater or migrates from a pre-2021 R3 version.) For complete details, see “Enabling Calculation of SHA-1 Digests for Scanned Files” in the *Code Insight Installation & Configuration Guide*.



Note - MD5 digests are always calculated whether or not SHA-1 support is enabled.

Users can view the SHA-1 digests for files in the responses for two new REST API, **Get details of a file by ID** and **Fetch all scanned files for a project**. For details, see [REST API Enhancements](#).

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:

- [Vulnerability Suppression](#)
- [Dates for Original Publication and Latest Revision Available for Security Vulnerabilities](#)

Vulnerability Suppression

This release introduces a new Vulnerability Suppression feature that enables a Code Insight System Administrator to suppress—that is, hide—a given security vulnerability at the Code Insight instance level. The following sections highlight aspects of this feature:

- [About Suppressing Security Vulnerabilities](#)

- [Code Insight Web UI to Support Vulnerability Suppression](#)
- [New REST Interface to Support Vulnerability Suppression/Unsuppression](#)
- [For More Information About This Feature](#)

About Suppressing Security Vulnerabilities

This new feature enables a customer to suppress a security vulnerability so that it is ignored in their Code Insight instance. The customer might want to do this, for example, if the vulnerability has proven to be a “false positive” (that is, is associated with an incorrect component version) or if the customer has taken remedial steps to protect their code against the vulnerability. Once a System Administrator suppresses the vulnerability, it is no longer published in reports, counted in vulnerability totals for inventory in projects, listed in the UI, or automatically associated with inventory during future project scans in your Code Insight instance.

During the suppression process, a System Administrator can choose to suppress the vulnerability for one, multiple, or all the component versions with which it is associated. The administrator can also monitor a list of all vulnerabilities suppressed across the Code Insight instance and unsuppress vulnerabilities as needed.



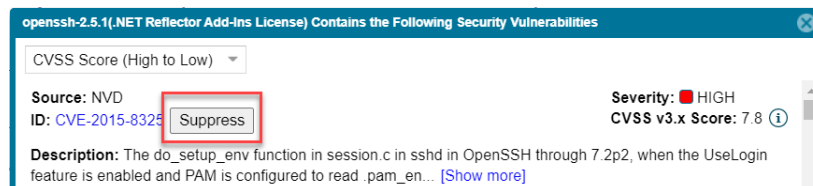
Note • Currently, vulnerabilities can be unsuppressed through the Code Insight REST interface only.

Code Insight Web UI to Support Vulnerability Suppression

Any type of security vulnerability can be suppressed, whether it is retrieved from the Code Insight data library during scans, is added later as an open alert, or is a custom vulnerability. To suppress a vulnerability, access the **Security Vulnerabilities** window that is displayed when you click on any **Vulnerabilities** bar graph within the context of an inventory item or component.



A new **Suppress** button (visible to only System Administrators) is displayed next to each vulnerability listed in window.



When clicked, the button opens an additional new window that enables the administrator suppress the vulnerability for selected component versions.

Additionally, a **Suppressed Vulnerabilities** view of all currently suppressed vulnerabilities is available from the **Data Library** option (formerly the **Custom Data** option) on the Code Insight system menu. (This menu is accessed by clicking in the upper right of the Code Insight UI.)

Vulnerability Id ↑	Affected Component	Affected Versions
① CVE-2005-1531	rhino	① 1.7.7
① CVE-2005-2096	madler-zlib	① 1.2.11.2.2
① CVE-2005-2261	rhino	① 1.7.7
① CVE-2007-2384	scriptaculous	① 1.8.1

New REST Interface to Support Vulnerability Suppression/Unsuppression

For a description of the new REST APIs that enable a System Administrator to suppress or unsuppress security vulnerabilities or to view a list of all suppressed vulnerabilities, see [New APIs](#).

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*.

Dates for Original Publication and Latest Revision Available for Security Vulnerabilities

As of 2021 R3, Code Insight stores the publication and latest revision dates of security vulnerabilities (as captured from the NVD) each time an Electronic Update is run. Currently, users can view these dates in the responses for the following Code Insight REST APIs: **Get Project Inventory**, **Get Component version vulnerabilities**, **Get vulnerability details of an inventory**, and **Get details of an inventory**. (For more information about these APIs, see [REST API Enhancements](#) and the Code Insight Swagger documentation.) These dates will be available in the Code Insight Web UI in a future release.

If you have migrated from a pre-2021 R3 release, you must run the latest Electronic Update to have access to these dates.

User Experience

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

Enhanced License Name Format

License names in lists, on the **Policy Details** page, and in other locations will now include the short license name, when available, along with the standard license name as another means of identifying the license. The short license name is displayed in parentheses next to the standard name:

BSD 3-Clause "New" or "Revised" License (BSD-3-Clause)

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
Component	Get Component version details components/versions/{Id}	GET	Retrieves details (such as the associated component name and license names and more) for a specific component version.
Vulnerability	Get suppressed vulnerabilities vulnerability/suppress	GET	Retrieves a list the suppressed security vulnerabilities filtered by a specific OSS or third-party component, a specific vulnerability, or both. Only a Code Insight System Administrator can perform this operation.
	Suppress vulnerability vulnerability/suppress	POST	Suppresses a security vulnerability for one, multiple, or all versions of a specific OSS or third-party component. Only a Code Insight System Administrator can perform this operation.
	Get vulnerability suppress details vulnerability/suppress/details	GET	Retrieves the details for suppressed security vulnerabilities filtered by the component version, the suppression ID, or both. Only a Code Insight System Administrator can perform this operation.
	UnSuppress vulnerability vulnerability/Unsuppress	Post	Unsuppresses a specific security vulnerability for specific versions of a component. Only a Code Insight System Administrator can perform this operation.

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
Component	Get Component version vulnerabilities components/{versionId}/vulnerabilities	GET	The response now includes the publishedDate and modifiedDate (latest revision date) of each security vulnerability listed.
Files	Get details of a file by ID files/{fileId}	GET	The response now includes a sha1 attribute, showing the SHA-1 digest for the file. If SHA-1 support is not enabled for Code Insight, the attribute most likely shows null (depending on when SHA-1 support was disabled and the type of scan most recently run).
Inventory	Get vulnerability details of an inventory inventories/{inventoryId}/vulnerabilities	GET	The response now includes the publishedDate and modifiedDate (latest revision date) of each security vulnerability listed.
	Get Details of an Inventory inventories/{inventoryId}/	GET	The response includes the publishedDate and modifiedDate (latest revision date) of each security vulnerability listed (if skipVulnerabilities is false in the request).
Project	Fetch all scanned files for a project /projects/{projectId}/allscannedfiles	GET	A new parameter includeSHA1Hash was added to the request to include the SHA-1 digest for each file listed in the response. <ul style="list-style-type: none">• If this parameter is set to true, the response includes a fileSHA1 attribute for each file, showing the SHA-1 digest for the file. If SHA-1 support is disabled for Code Insight, the attribute value for each file is most likely null (depending on when SHA-1 support was disabled and the type of scan most recently run).• If the includeSHA1Hash parameter is set to false in the request, the fileSHA1 attribute is omitted from the response.

Table 2 - Updates to Existing APIs

Resource	API Name/Endpoint	Method	Description
	Import project data /project/{projectId}/import	POST	A new parameter <code>resetInventoryUsage</code> was added to the request to define how to handle Usage attributes for inventory during the import. If set to <code>true</code> (default), the Usage attributes are reset to the system default value <code>Unknown</code> . If set to <code>false</code> , the existing Usage attributes are copied to the target project.
	Get Project Inventory /project/inventory/{projectId}	GET	The response includes the <code>publishedDate</code> and <code>modifiedDate</code> (latest revision date) of each security vulnerability listed (if <code>skipVulnerabilities</code> is <code>false</code> in the request).

Resolved Issues

The following issues are resolved in this release.

Table 3 - Resolved Issues

Issue	Resolution Notes
SCA-18733	New user documentation added, explaining how the <code>.git</code> folder is processed during scans (and why the <code>.git</code> directory is not impacted by scan exclusions). See “Note About Excluding the <code>.git</code> Directory from Scans” in the <i>Code Insight Installation & Configuration Guide</i> .
SCA-25836	Files for deleted inventory no longer showing in results for an Advanced Search of those files still associated with inventory.
SCA-29207	SCM (Source Code Management) Git connectors now successfully synchronizing with repositories that do not use a <code>.git</code> suffix (such as those repositories created through Azure DevOps).
SCA-29667	Total number of associated files for an inventory item now matching the number of files listed on the item’s Associated Files tab.
SCA-30052	Issues with <code>node.js</code> components (especially <code>core.js</code>) being published with the wrong component in inventory now resolved.
SCA-30205	Issue with re-uploading a codebase that contains a folder with the same name and path as a previously uploaded and scanned file has been resolved.

Table 3 - Resolved Issues (cont.)

Issue	Resolution Notes
SCA-30868	License Usage guidance for a published inventory item now properly updated when the inventory item is recalled, assigned a new license, and re-published based on a license policy with new guidance. The old license Usage guidance is replaced by the new. Or, if no new license Usage guidance exists, the current license Usage guidance is cleared.
SCA-31708	Scans now matching a detected Splunk logging artifact to its correct name in inventory.
SCA-32039	Issues with adding files to inventory now resolved. (The issues occurred when Filter to Selected Files was selected on Evidence Details tab.)
SCA-32509	Startup failures with <code>mysql-connector-java-8.0.23.jar</code> (and later) now resolved for Code Insight 2021 R3 and later.
SCA-33199	The Branch process for a large project now completing successfully.
SCA-34826	Newly generated Notices report now properly replacing old Notices report on the Reports page.
SCA-34974	Issue with MIT licenses being reported as FreeBSD licenses now corrected.
SCA-35174	New user documentation added to the <i>Code Insight Installation & Configuration Guide</i> to address the <code>db_ddladmin</code> role requirement for Code Insight migrations.
SCA-35330	New user documentation added to the <i>Code Insight Installation & Configuration Guide</i> to describe how to configure Code Insight timeout sessions.
SCA-35568	Rescans now successful when scans are configured to skip unchanged files associated with inventory. Previously, such rescans for certain projects resulted in “NonUniqueResultException” exceptions.
SCA-35722	Usage guidance text now showing only its most recent value (and not all the previous values as well).
SCA-36017	Automated Analysis now reporting direct and transitive dependencies with a “provided” scope in <code>.pom</code> files.
SCA-36423	Automated Analysis now properly reporting inventory and dependencies for Bower packages.
SCA-37139	New user documentation added to “Automated Analysis” in the <i>Code Insight User Guide</i> to describe support for the analysis of <code>.csproj</code> files in .NET packages.
SCA-37257	Git SSH connection failures with <code>git_prescan_plugin-1.0.0-17</code> (or later) now resolved.

Table 3 - Resolved Issues (cont.)

Issue	Resolution Notes
SCA-37334	Connection failures between the Git SCM (Source Code Management) plugin and Github.com URLs now resolved. The failures were due to GitHub's new requirement to use token-based input instead of a password for their authentication method. For more information see Special Notes .

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 instance 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](#)
- [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](#)
- [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 in Code Insight.

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.

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 2021 R3 possibly more time-consuming than previous upgrades

Upgrading to Code Insight 2021 R3 might take longer than previous upgrades, especially if the number of inventory items in your Code Insight instance has increased since the last upgrade. For example, currently the upgrade for an instance with about 1 million inventory items can take around 15-20 minutes, which might be longer than your previous upgrades. The extra time needed for the upgrade is due the new **Inventory History** feature, 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.

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 are 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 result 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-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 enabled and 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 a Jenkins plugin upgrade, 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: 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-30568: Significant space consumed by Perforce synchronization logs in Code Insight

When a user synchronizes a Code Insight project with a Perforce repository by clicking **Sync Now** from any SCM instance tab, the synchronization automatically adds Perforce log data to the Tomcat logs in Code Insight. This behavior can result in large Tomcat log files.

Workaround: Synchronize Code Insight with the Perforce repository directly through the Perforce command-line client installed on the Scan Server instance.

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

The following are known issues with the Vulnerability Suppression 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.