

Code Insight 2020 R4 Release Notes

December 2020

Introduction	3
About Code Insight	3
New Features and Enhancements	3
Installation and Configuration	3
TLS Upgrade for HTTPS Configuration.....	4
Tomcat Upgrade to 8.5.57	4
Enhanced User Documentation for the Code Insight Upgrade Process.....	4
Project Administration	4
Changes to Code Insight User Roles.....	4
Improved Options for Handling Archives During Codebase Uploads (Web UI)	5
New Right-Click Menu in Projects List.....	6
New File Path Format.....	6
Confirmation of Saved Notices Content Added	8
Project Inventory Review	8
CPE Details Now Included for Components.....	8
Scan Agent Plugins	9
Additional Plugins Upgraded to Support Single-Project Type	9
Scanning and Automated Discovery	10
New NG-Bridge Digest Data to Complement Compliance Library.....	10
New Global Scan Queue.....	10
REST API Enhancements	10
New APIs	11
General Changes to Existing APIs to Accommodate New User Roles.....	12
Updates to Existing APIs.....	12
Other Enhancements	13
Easy Access to Your Code Insight License Expiration Date	13
Resolved Issues	13
Known Issues in this Release	14
Automated Workflow for Inventory Review/Publication	15
Export and Import	15
Installation and Configuration.....	16
Manual Codebase Analysis	16
Project Administration	17
Project Inventory	17
Reporting	17
REST APIs	18
Scan Agent Plugins	18
Scanning and Automated Discovery	19

Source Control Management (SCM) Support	21
Web UI.....	21
Legal Information	23

Introduction

These Release Notes provide the following information about the Code Insight 2020 R4 release:

- [About Code Insight](#)
- [New Features and Enhancements](#)
- [Resolved Issues](#)
- [Known Issues in this Release](#)
- [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 2020 R4 release provides new features and enhancements in the following areas:

- [Installation and Configuration](#)
- [Project Administration](#)
- [Project Inventory Review](#)
- [Scan Agent Plugins](#)
- [Scanning and Automated Discovery](#)
- [REST API Enhancements](#)
- [Other Enhancements](#)

Installation and Configuration

The following the new features and enhancements are available for the installation and configuration of Code Insight:

- [TLS Upgrade for HTTPS Configuration](#)
- [Tomcat Upgrade to 8.5.57](#)
- [Enhanced User Documentation for the Code Insight Upgrade Process](#)

TLS Upgrade for HTTPS Configuration

Code Insight has upgraded its TLS (Transport Layer Security) component to version 1.2 for security purposes. To support this upgrade, this release has provided updates to the `<CODEINSIGHT_ROOT_DIR>\tomcat\https\server.xml` file. For more information, see “Enabling Secure HTTP Over SSL” in the *Code Insight Installation & Configuration Guide*.

Tomcat Upgrade to 8.5.57

Code Insight has upgraded to Tomcat 8.5.57 to obtain the latest Tomcat security fixes.

Enhanced User Documentation for the Code Insight Upgrade Process

The documentation for performing a Code Insight upgrade (as found in the “Upgrading Code Insight” chapter in the *Code Insight Installation & Configuration Guide*) has been enhanced to include the following:

- A designation of which server (Core, Scan, or Database) to which a specific upgrade step applies
- More details for migrating your HTTPS configuration
- More details for migrating your configuration for running Code Insight as service

Project Administration

The following are the new features and enhancements available for managing Code Insight projects:

- [Changes to Code Insight User Roles](#)
- [Improved Options for Handling Archives During Codebase Uploads \(Web UI\)](#)
- [New Right-Click Menu in Projects List](#)
- [New File Path Format](#)
- [Confirmation of Saved Notices Content Added](#)

Changes to Code Insight User Roles

In this release, a new Project Administrator user role has been introduced to appropriately offload many of the project responsibilities assigned to the Project Owner in previous releases. Also in this release, the Project Owner is now called the *Project Contact*; and the previous Administrator is now known as the *System Administrator*. The Analyst, Reviewer, and Observer roles remain basically the same.

For a detailed matrix of the Code Insight user responsibilities and the roles that can perform these responsibilities, see the “Code Insight User Roles and Permissions” appendix in either the *Code Insight User Guide* or the *Code Insight Installation & Configuration Guide* for the 2020 R4 release.

The following sections describe the basic responsibilities of the new and changed user roles in this release:

- [System Administrator Role](#)
- [Project Contact Role](#)

- [Project Administrator Role](#)

System Administrator Role

The initial Code Insight System Administrator, identified during Code Insight installation, can assign users to system-level roles for managing Code Insight policies and creating Code Insight projects. The System Administrator can also create other System Administrators and define default Project Administrators, Analysts, and Reviewers that are automatically assigned to every new project at its creation.

Project Contact Role

Starting in this release, the user who creates a project automatically becomes the Project Contact and, by default, is also assigned to the Project Administrator and Analyst roles in the project.

The Project Contact is the default contact for all task-workflow notifications generated during the inventory review process. That is, if a Legal, Security, or Development contact has not been explicitly assigned to the project through system Project Defaults (by the System Administrator) or at the project level (by the Project Administrator), that contact defaults to the Project Contact. Additionally, the Project Contact is the default contact for any “miscellaneous” tasks created during an inventory review.



Note • *When a project is migrated from a previous Code Insight version (2020 R3 or earlier), by default the Project Owner becomes the Project Contact and is assigned to the Project Administrator and Analyst roles.*

The current Project Contact, a Project Administrator, or a System Administrator can transfer the Project Contact role to different user. That user automatically inherits any additional roles that the previous Project Contact user held.

Project Administrator Role

In essence, the Project Administrator takes over most of the responsibilities that were held by the Project Owner in previous releases.

A Project Administrator manages project users, assigning users to project roles that enable these users to analyze and review project scan results. The administrator can also remove a user from any project role as needed, whether the user was manually assigned the role or had inherited it.

Additionally, Project Administrators manage project settings, upload and scan codebases, as well as rename, export, import, branch, and delete projects. They also manage Manage Source Control Management (SCM) and Application Lifecycle (ALM) instances.

Improved Options for Handling Archives During Codebase Uploads (Web UI)

Code Insight now provides additional settings on the **File Upload** dialog to define the behavior of the codebase-upload process once first-level or deeper archives are expanded. Both settings are optional.

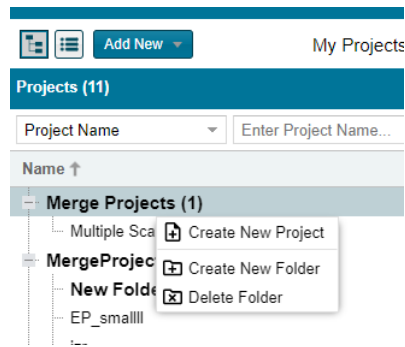
- The **Delete archive files after expansion** enables you to remove those archives that have been expanded during an upload. (The archives are removed once the upload is finished.)

- The [Append value to expanded archive directory name](#) lets you define a string to append to the name of any folder automatically created during the upload to store an archive's contents. After a scan, this appended string helps you to identify those folders in the codebase tree whose contents were extracted from archives, especially if the original archives were removed from the codebase during the upload (as described in the previous option).

New Right-Click Menu in Projects List

A new right-click menu in the Code Insight project list (in the **Projects** pane) enables you to do the following, depending on the list format:

- In the simple list format, create and delete projects.
- In the project tree format, add and delete folders and sub-folders, create projects within the context of a folder, and delete projects.



New File Path Format

The codebase files paths in Code Insight no longer show the absolute scan-root path; instead, the absolute scan-root path is replaced with an alias—a unique, user-defined name introduced in 2020 R3 for the purpose of representing the scan-root container.

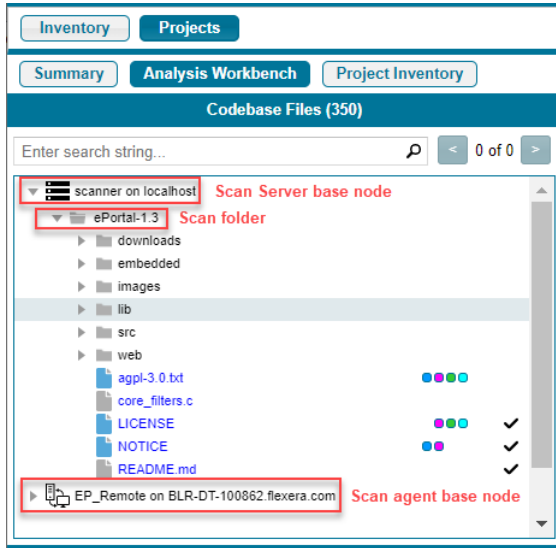
The following shows how files paths are now represented in different parts of the Code Insight Web UI and in reports:

- [Codebase Files and File Search Results Panes in Analysis Workbench](#)
- [File Details Tab in Analysis Workbench](#)
- [Files Associated with Inventory](#)
- [Reports](#)

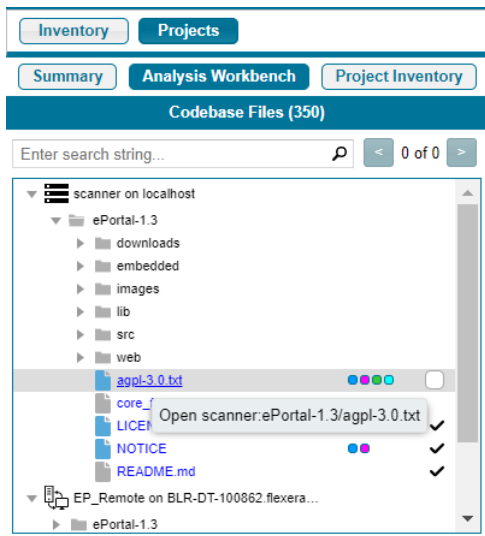
Note that you can still see the absolute scan-root path for each scanner (Scan Server or remote scan agent) used by a project on the project's **Summary** page.

Codebase Files and File Search Results Panes in Analysis Workbench

The codebase tree in either the **Codebase Files** or the **File Search Results** pane no longer shows the scan-root path as a separate node. Instead the codebases are listed under a base node in the format `<scannerAlias> on <scannerHost>`. For example, for a codebase scanned by a Scan Server, the base node might be **Scanner03 on localhost**. For a codebase scanned by a scan agent, it might **EP_Remote on BLR-DT-100555.ECompany.com**. Directly under each base node is the top-level (scan) folder.



When you hover over a file name in the codebase tree, the name is shown in an `<alias>:<relativeFilePath>` format, where `<alias>` is the alias of the Scan Server or scan agent and `<relativeFilePath>` is the file path relative to the absolute scan-root path on host instance. (See the following example where, when a user hovers over the codebase file **agpl-3.0.txt**, located directly under the scan folder **ePortal-1.3**, the file name is shown as **scanner:ePortal-1.3/agpl-3.0.txt**.)



File Details Tab in Analysis Workbench

On the **File Details** tab in the **Analysis Workbench**, the codebase file is identified (depending on whether the tab header is collapsed or expanded) in an `<alias>:<relativeFilePath>` format or as separate **Name**, **Alias**, and **Path** properties (shown here in an expanded header).



Files Associated with Inventory

The **Associated Files** tab in the **Analysis Workbench** and on the **Project Inventory** tab lists each file associated with inventory with an alias and the relative file path.

Reports

The Project and Audit reports list a given codebase file in `<alias>:<relativeFilePath>` format or as separate **Alias name**, **File Path**, and **Name** properties.

Confirmation of Saved Notices Content Added

On the **Inventory Details** pane for a selected inventory item on the **Project Inventory** tab, a message dialog now displays after you have saved edits to **Notices Text**, **Audit Notes**, **Usage Guidance**, or **Remediation Notes** content to let you know your edits were successfully saved. Additionally, the **Save** button for any of these content fields is enabled only when you make edits to the content.

Project Inventory Review

The following are new features and enhancements available for managing project inventory in this release:

- [CPE Details Now Included for Components](#)

CPE Details Now Included for Components

Starting in this release, the Code Insight data library stores the CPE (Common Platform Enumeration) names for an OSS for third-party component, as published in the NVD. This information is available in the Code Insight Web UI and REST API responses.

CPE is a structured naming scheme for a component that includes the component's vendor name and product name and uses the following format:

```
cpe://<part>:<vendor>:<product>
```

where `<part>` is either **a** (applications), **h** (hardware platforms), or **o** (operating systems).

The CPE vendor and product properties are key in distinguishing between multiple components with the same name.

CPE information for a given component is displayed in the following locations in the Code Insight Web UI:

- **Lookup Component** window accessed when creating or editing an inventory item
- **Component Details** window accessed when you click the ⓘ icon for the **Component** property on the **Inventory Details** tab in the **Analysis Workbench**
- **Component Details** tab in the **Project Inventory Details** pane for the selected inventory item in **Project Inventory**

Additionally appropriate REST APIs now include component CPE vendor and product names in responses and allow filtering by these names. See [REST API Enhancements](#).

Scan Agent Plugins

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

- [Additional Plugins Upgraded to Support Single-Project Type](#)

Additional Plugins Upgraded to Support Single-Project Type

The process of upgrading Code Insight scan-agent plugins 1.x to 2.0 started in the Code Insight 2020 R3 release.

The 1.x plugins require an inventory-only project on the Code Insight Core Server to which to send the inventory results from the remote scans. (No codebase-file information is captured by the 1.x plugin scans.) However, the 2.0 plugins, whose scans now capture both *inventory and codebase-file information*, send scan results to a new project type (introduced in the 2020 R3 release) that is capable of managing the data from both server scans (performed by the Scan Server) and remote scans.

Code Insight continues to support existing inventory-only projects, enabling users to scan these projects using version 1.x plugins installed from previous Code Insight releases. However, inventory-only projects will be deprecated in a future release. If you want to manually migrate your inventory-only projects to the new project type, refer to the following Knowledge Base article in the Reverera Community:

<https://community.flexera.com/t5/FlexNet-Code-Insight-Customer/Code-Insight-2020-R3-Changes-to-Projects/ta-p/160059>

Plugins Not Yet Upgraded

As of this release, the following scan-agent plugins have not been upgraded. These 1.x plugins continue to require inventory-only projects, sending only inventory information in the scan results.

- GitLab
- JFrog Artifactory
- TeamCity

When these scan-agent plugins are updated, you can retrieve the updated documentation from either the [Reverera Product Documentation](#) site or the Flexera Product and Licensing Center.

Scanning and Automated Discovery

This release provides the following enhancements to the Code Insight codebase scan and Code Insight Automated and Advanced analyses:

- [New NG-Bridge Digest Data to Complement Compliance Library](#)
- [New Global Scan Queue](#)

New NG-Bridge Digest Data to Complement Compliance Library


Starting with the 2020 R4 release, Code Insight will support a secondary data source, NG-bridge, for digest matches as an overlay to the data in the Compliance Library. NG-bridge is Code Insight's next generation bridge solution that complements the Compliance Library (CL) with digest-match data beyond that provided in CL 2.43. The NG-bridge component is included with Code Insight and is a separate module that runs along-side the product to support exact-matching functionality.

Updates to the NG-bridge data source are planned on a regular basis and will keep the MD5 data for exact-file matching up to date. Each NG-bridge data update release is incremental, providing only changes since the last update release.

For more information about the NG-bridge data updates, how to configure the updates, and how the NG-bridge data is processed during scans, see "Managing NG-bridge (Digest Data) Updates for Code Insight" in the *Code Insight Installation & Configuration Guide*.

New Global Scan Queue

Code Insight provides a new global Scan Queue feature that lets you monitor the current scan queues for all active Scan Servers from a single location. You can access this feature from the Code Insight main menu. (Click

the  icon in the upper-right corner of the Code Insight Web UI to open the menu).

REST API Enhancements

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

- [New APIs](#)
- [General Changes to Existing APIs to Accommodate New User Roles](#)
- [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 Endpoint	Method	Description
Component	/components/search	GET	Searches for OSS or third-party components: <ul style="list-style-type: none">Retrieves components based on component Name, URL, or CPE (Common Product Enumeration) name:<ul style="list-style-type: none">For Name, one or more searchTerm strings are accepted. Filters are available for multiple keywords: ALL_TERMS, ANY_TERM, BEGINS_WITH, EXACT_MATCH.For URL, only one searchTerm string is accepted.For CPE, a vendor or product string is required for the search. (A searchTerm is optional.) If both vendor and product values are supplied, the component's CPE name must satisfy both criteria. If a searchTerm value is added, the CPE name must satisfy all vendor, product, and searchTerm criteria.Provides an option in the request to include or omit component versions.Returns the CPE (Common Product Enumeration) name, CPE vendor name, and CPE product name for each retrieved component.
	/components/{versionId}/vulnerabilities	GET	Retrieves a list of security vulnerabilities associated with a component version, providing complete details for each vulnerability (name/ID, description, CVSS score and severity, and more).
Project	/projects/inventorySummary/{projectId}	GET	Provides a simplified view of the inventory for a specific project, with options for the following: <ul style="list-style-type: none">Filtering by published or unpublished inventory.Including a security vulnerability summary for each inventory item. (This summary is a list of severity-level totals by CVSS version; it does not describe individual vulnerabilities.) A related option lets the user to select the CVSS version(s) for which to show the summary.
Inventory	/inventories/{id}/vulnerabilities	GET	Retrieves details for each security vulnerability associated with a specified inventory item. Details include name/ID, description, CVSS score and severity, and more.

General Changes to Existing APIs to Accommodate New User Roles

The following are general changes that have occurred across the Code Insight REST APIs to accommodate the new Project Administrator and Project Contact roles:

- The “owner”, “ownerId”, and “ownerName” properties, still used in the requests and responses for the Project APIs, have been remapped internally to the new Project Contact role. These properties will be relabeled accordingly to refer to the Project Contact role in a future release.
- Authorization to invoke the APIs has changed for many APIs. For a detailed matrix of the Code Insight user responsibilities and the roles that can perform these responsibilities (and thus who can call corresponding APIs), see the “Code Insight User Roles and Permissions” appendix in either the *Code Insight User Guide* or the *Code Insight Installation & Configuration Guide* for the 2020 R4 release.

Updates to Existing APIs

In addition to the changes described in [General Changes to Existing APIs to Accommodate New User Roles](#), the following updates to existing APIs have occurred in this release.

Table 2 • Updates to Existing APIs

Resource	API Endpoint	Method	Description
Component	/components/ {componentId}	GET	Updates include: <ul style="list-style-type: none">• New option to show a summary of security vulnerability totals by severity level as detected for a given component version, instead of detailed information for each vulnerability. A related option lets the user to select the CVSS version(s) for which to show the summary.• Retrieval of CPE (Common Product Enumeration) data for each retrieved component in the response.
Projects	/project/inventory/ {projectId}	GET	Updates include: <ul style="list-style-type: none">• New option to show or hide security vulnerability details associated with the specified inventory item.• New option to filter inventory by CPE (Common Product Enumeration) vendor or product (or both) strings.• Retrieval of CPE (Common Product Enumeration) data for each retrieved inventory item in the response.
	/projects/{projectId}	PUT	Updates include changes to support the project roles introduced in this release.

Table 2 • Updates to Existing APIs


Resource	API Endpoint	Method	Description
	/projects/{projectId}/	GET	Updates include: <ul style="list-style-type: none">• A summary of security vulnerability totals by severity level as detected in the project's inventory.• A summary of the license totals by priority as detected in the project.
	/projects/{projectId}/users	POST	Updates include changes to support the project roles introduced in this release.
	/projects/{projectId}/users	DELETE	Updates include changes to support the project roles introduced in this release.
Inventory	inventories/{inventoryId}	GET	Updates include: <ul style="list-style-type: none">• New option to show or hide security vulnerability details associated with the specified inventory item.• Retrieval of CPE (Common Product Enumeration) data for each retrieved component in the response.

Other Enhancements

Other enhancements in this release include the following:

- [Easy Access to Your Code Insight License Expiration Date](#)

Easy Access to Your Code Insight License Expiration Date

You can now see your Code Insight license expiration date by clicking the icon  in the upper right corner of the Code Insight Web UI to display the Code Insight main menu. The expiration date is displayed in the footer content at the bottom of the menu.

Resolved Issues

The following issues are resolved in this release.

Table 3 • Resolved Issues

Issue	Description
SCA-3256, SCA-29630	Unresponsive Code Insight Web UI when attempting to navigate the UI or load projects.
SCA-23942	Incorrect path copied when Copy Folder Path is selected for any file in the Advanced Search pane in Analysis Workbench .

Table 3 • Resolved Issues (cont.)

Issue	Description
SCA-26046	Only one license reported for <code>html-parser.js</code> during a scan on <code>vue 2.6.11</code> , even though three possible licenses exist.
SCA-26476	Unable to import data from inventory-only export performed in Code Insight 2020 R2 or earlier.
SCA-26668	Missing vulnerability information for Jenkins PRQA Plugin 3.1.0 and Jenkins XL TestView Plugin 1.2.0
SCA-27363	Code Insight not detecting the Curl license as a possible license for appropriate components.
SCA-27426	Vulnerability falsely associated with SmallRye Mutiny component.
SCA-27646	Unable to disable Secunia vulnerabilities on Linux due to case issue in the internal query controlling this task.
SCA-27659	A “save confirmation” dialog erroneously appearing during attempt to delete an inventory item.
SCA-27660	Project deletion successful but process throws SQL exception in the logs while deleting unused data however project gets deleted
SCA-29019	Project Report significantly larger than in previous releases (even though the codebase size has remained the same).
SCA-29488	Unresponsive Code Insight Web UI when attempting to run reports and scans in parallel.
SCA-25636, SCA-28802, SCA-29873	Scan failures after Code Insight upgrade.
SCA-29976	Analysis Workbench: The file right-click Copy File Path option not working for files listed on the Associated Files tab.

Known Issues in this Release

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

- [Automated Workflow for Inventory Review/Publication](#)
- [Export and Import](#)
- [Installation and Configuration](#)
- [Manual Codebase Analysis](#)
- [Project Administration](#)

- [Project Inventory](#)
- [Reporting](#)
- [REST APIs](#)
- [Scan Agent Plugins](#)
- [Scanning and Automated Discovery](#)
- [Source Control Management \(SCM\) Support](#)
- [Web UI](#)

Automated Workflow for Inventory Review/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.

Export and Import

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 and Configuration

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 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: <https://community.reverera.com>.)

Manual Codebase Analysis

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.

Project Administration

SCA-30486: My Projects filter not showing those projects for which the user has only Project Administrator role

When a user has only a Project Administrator role for a given project, that project is not visible in the **Projects** list when the **My Projects** filter is enabled.

Workaround: Disable the **My Projects** filter to view all projects.

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

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.

Reporting

SCA-22054: Project Report not showing vulnerabilities

Reports are not showing 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

SCA-22413: Get All Scanned Files API not returning all scanned files in an inventory-only project

When a scan agent scans a codebase for an inventory-only project, it sends the results to the Code Insight server. These results include information for only those files that are associated with inventory. Consequently, when the `allscannedfiles` REST API retrieves the file information from the Code Insight server, the response shows only files associated with inventory, not an entire list of scanned files.

Workaround: None exists.

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

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

Workaround: None exists.

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

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

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

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-27787: Scan failure when scanning large codebases on Azure DevOps hosted agent

Scan failure can occur when scanning codebases that contain more than 5000 files on an Azure DevOps hosted agent.

Workaround: Scan the codebase on a Azure DevOps private agent.

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

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.

SCA-30420: A complete rescan triggered on all project codebases (on the Scan Server) after an NG-bridge data update

A complete rescan of all project codebases loaded on the Scan Server is triggered whenever an NG-bridge data update is performed. The rescans detect any new exact-file matches based on the latest digest information provided in the data update. However, running a full rescan for each new data update consumes time.

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

SCA-30039: Transitive-level inventories not reported for “optional” dependencies in Maven POM.xml

When a Maven POM.xml file contains dependencies for which “Optional” is set to **true**, no transitive dependencies are being reported for the optional dependencies when the file is scanned.

Workaround: None exists.

SCA-26934: 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: * version containing hyphen as 3.1.9-1 (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

SCA-30568: Significant space consumed by Perforce synchronization logs in Code Insight

When a user synchronizes a Code Insight project with a Perforce codebase 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 codebase 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.

Web UI

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

SCA-21917: Last Server Scan field on dashboard showing date of report generation

The **Last Server Scan** value on the **Project Dashboard** should show the date of the last scan. However, when a report is generated, this date changes to the report-generation date.

Workaround: Obtain the last scan date from the scan history link (in the **Past Server Scans** field) on the project **Summary** tab.

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 © 2020 Flexera Software

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

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

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

Intellectual Property

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

Restricted Rights Legend

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