Code Insight 2022 R1 Release Notes

February 2022

Introduction

These Release Notes provide the following information about the Code Insight 2022 R1 release:

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

About Code Insight

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

Revenera Resources

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

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

  https://community.revenera.com

New Features and Enhancements

The Code Insight 2022 R1 release provides new features and enhancements in the following areas:

- Application Life Cycle Management (ALM) Support
- Export and Import of Project Data
- Global Component & License Lookup
- Installation, Upgrades, and Configuration
- Project Inventory
- Project Management
- Project Reporting
- Scanning and Automated Discovery
- Source Code Management (SCM) Support
- REST API Enhancements

Application Life Cycle Management (ALM) Support

This release provides the following enhancement to the ALM functionality that manages external work items to remediate inventory in Code Insight.

Security Token Support for Using Jira in the Cloud

The new **Jira Password/API Token** field in the UI for a Jira instance (replacing the previous **Jira Password** field) gives you the option to enter a valid user password to connect to a non-Cloud Jira server *or* a valid API user token to connect (using HTTPS) to a Jira server residing in the Atlassian Cloud.

Export and Import of Project Data

This release provides the following enhancement to the Code Insight functionality that exports and imports project data.

Support for Custom Fields

Code Insight now supports the export and import of custom field values for projects and inventory. For details, see “Exporting and Importing Project Data” in the *Code Insight User Guide*.

Global Component & License Lookup

Previously, users could search components and look up license details as found in the Code Insight data library only when they created and edited inventory within a project. This release introduces the Global Component & License Lookup feature, which enables users to explore components and licenses in the data library outside the context of project inventory.

This type of exploration might be useful, for example, when a current inventory component is associated with security vulnerabilities. Users can perform a global search on the data library to look for components and their versions associated with less severe vulnerabilities (or no vulnerabilities). The results of such a search can help the user to decide whether to replace the current inventory component with another more secure one.

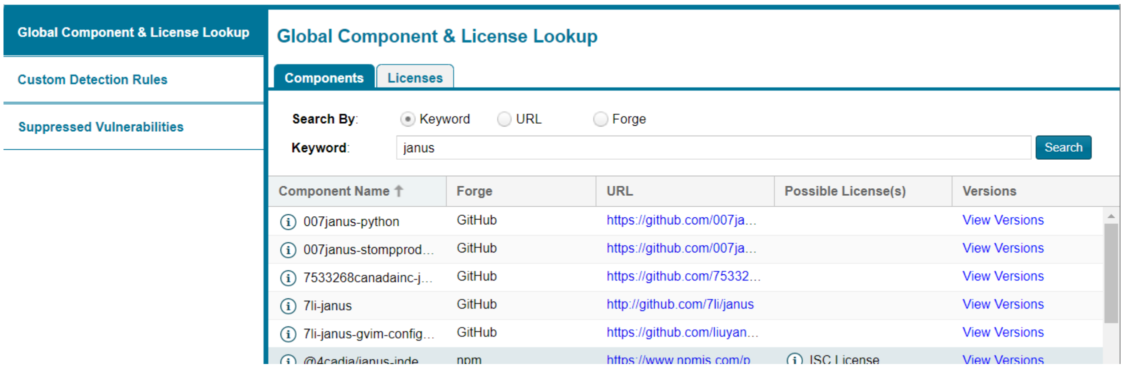
To access this feature, go the Code Insight main menu (☰) and navigate to the **DATA LIBRARY** > **Global Component & License Lookup** tab.

The following sections provide an overview of Global Component & License feature:

- Exploring Components
- Exploring Licenses

Exploring Components

From the **Global Component & License Lookup** > **Components** tab, you can search components by component name, forge URL, or forge and repository name. The list of search results provides several way to explore individual components.

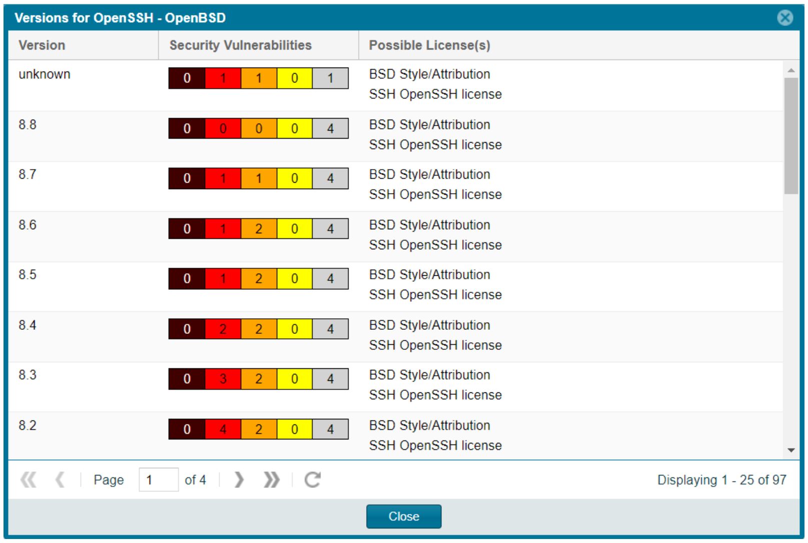

Global Component & License Lookup
Custom Detection Rules
Suppressed Vulnerabilities
Global Component & License Lookup
Components
Licenses
Search

Search By: ● Keyword ○ URL ○ Forge

Keyword: janus

Component Name	Forge	URL	Possible License(s)	Versions
007janus-python	GitHub	https://github.com/007ja...		View Versions
007janus-stompprod...	GitHub	https://github.com/007ja...		View Versions
7533268canadainc-j...	GitHub	https://github.com/75332...		View Versions
7li-janus	GitHub	http://github.com/7li/janus		View Versions
7li-janus-gvim-config...	GitHub	https://github.com/liuyan...		View Versions
@4cadia/janus-inde	npm	https://www.npmjs.com/p	ISC License	View Versions

For example, you can look up details about a component, view information about a component's licenses, and access the third-party web page of a component's project or repository within its forge. You can also open a separate **Versions for** <component> window that lets you research the security vulnerabilities associated with each version of a given component.

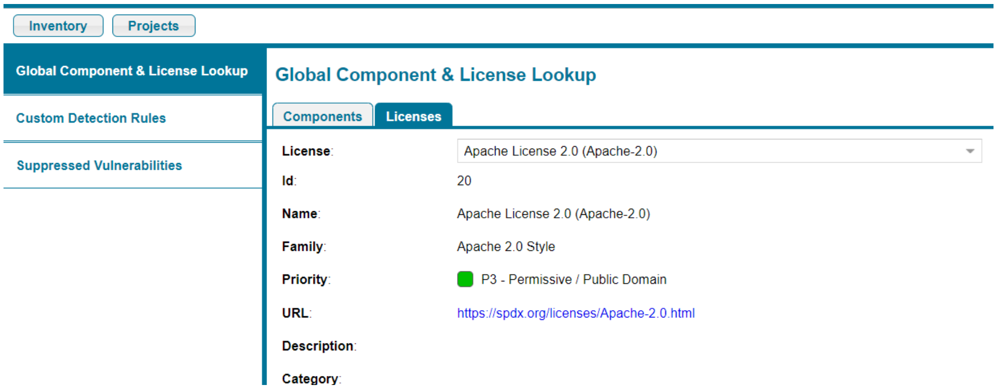


Version	Security Vulnerabilities	Possible License(s)
unknown	0 1 1 0 1	BSD Style/Attribution SSH OpenSSH license
8.8	0 0 0 0 4	BSD Style/Attribution SSH OpenSSH license
8.7	0 1 1 0 4	BSD Style/Attribution SSH OpenSSH license
8.6	0 1 2 0 4	BSD Style/Attribution SSH OpenSSH license
8.5	0 1 2 0 4	BSD Style/Attribution SSH OpenSSH license
8.4	0 2 2 0 4	BSD Style/Attribution SSH OpenSSH license
8.3	0 3 2 0 4	BSD Style/Attribution SSH OpenSSH license
8.2	0 4 2 0 4	BSD Style/Attribution SSH OpenSSH license

On the **Versions for** <component> window, an interactive bar graph for a given version provides vulnerability totals by severity. When the graph is clicked, another window is opened, providing details about each vulnerability associated with the component version and giving you the option to suppress any of these vulnerabilities for the version if necessary.

Exploring Licenses

The **Global Component & License Lookup** > **Licenses** tab enables users to search the Code Insight data library for a specific OSS or third-party license by name. The **Licenses** tab is populated with attributes describing the selected license.


Inventory
Projects
Global Component & License Lookup
Custom Detection Rules
Suppressed Vulnerabilities
Global Component & License Lookup
Components
Licenses

License:	Apache License 2.0 (Apache-2.0)
Id:	20
Name:	Apache License 2.0 (Apache-2.0)
Family:	Apache 2.0 Style
Priority:	🟩 P3 - Permissive / Public Domain
URL:	https://spdx.org/licenses/Apache-2.0.html
Description:	
Category:	

Installation, Upgrades, and Configuration

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

Additional Platform Support

Code Insight is now supported on the following additional platforms:

- CentOS 8.*x*

- RHEL 8.*x*
- Ubuntu 20.04 LTS
- Windows Server 2022

Support for Java Runtime Edition (JRE) 8u301 and 8u311

Code Insight now officially supports Oracle JRE 8u301 and 8u311 (in addition to existing official support for 8u192). Currently, Oracle JRE 8u192 is installed as part of the Code Insight installation. If you want to upgrade the Oracle JRE version currently installed with Code Insight, you must perform additional steps once the Code Insight installation is complete. For more information, see “Upgrading the JRE” in the *Code Insight Installation & Configuration Guide*.

Note ▪ *All other versions under 8u311 are supported, but unofficially.*

Project Inventory

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

- Updates to Task Notifications
- REST Support for Updating Custom Field Values for Inventory

REST Support for Updating Custom Field Values for Inventory

Project analysts can now use the **Update Inventory** and **Create Inventory** REST APIs to update the custom-field values for an inventory item. Previously, users could only view custom field values (using the **Get Project Inventory** or **Get details of an inventory** REST APIs).

Updates to Task Notifications

The following describes changes made to the behavior and content of email notifications triggered by task-management activities during the review of project inventory:

- Previously when a task of any type was closed through the Web UI or the REST interface, an email notification was automatically sent to the task owner only. Now a notification is also sent to the task creator. (Note that project contacts currently do not receive this automatic notification.)
- The content of the email notification sent when a task is closed now includes two new attributes **Closed By** and **Resolution**. The Resolution attribute shows **Approved** or **Rejected** for a **Manual Review Inventory** task or **Closed** for a **Remediate Inventory** or `Miscellaneous` task.
- When a task is reopened or reassigned, an email notification is now automatically sent to the task owner (assignee).

Project Management

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

Custom Fields for Projects

The standard fields used to describe projects in Code Insight might not provide all the detail that your site requires to manage projects. To address this need for additional detail, Code Insight enables the System Administrator to create and manage custom fields that are made available for all projects in your Code Insight system. Project administrators then update the values for these fields as needed within a given project.

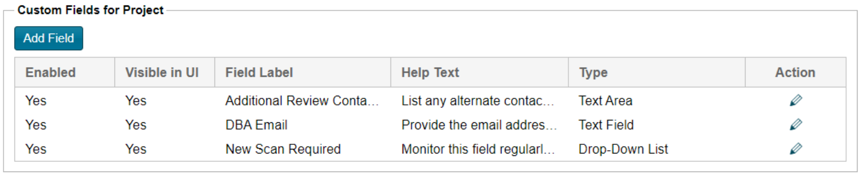
Depending on its configuration, a custom project field can be made available in both the Code Insight Web UI (that is, on a project's **Summary** tab and its **Summary** > **Manage Project** > **Edit Project** > **Custom Fields** tab) and through the Code Insight REST interface. Alternatively, the field can be configured for availability through the REST interface only.

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

- Creating and Managing Custom Fields for Projects
- Updating Custom Field Values for a Project in the Web UI
- Updating Custom Field Values for a Project through REST APIs

Creating and Managing Custom Fields for Projects

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



Enabled	Visible in UI	Field Label	Help Text	Type	Action
Yes	Yes	Additional Review Conta...	List any alternate contac...	Text Area	✎
Yes	Yes	DBA Email	Provide the email addres...	Text Field	✎
Yes	Yes	New Scan Required	Monitor this field regularl...	Drop-Down List	✎

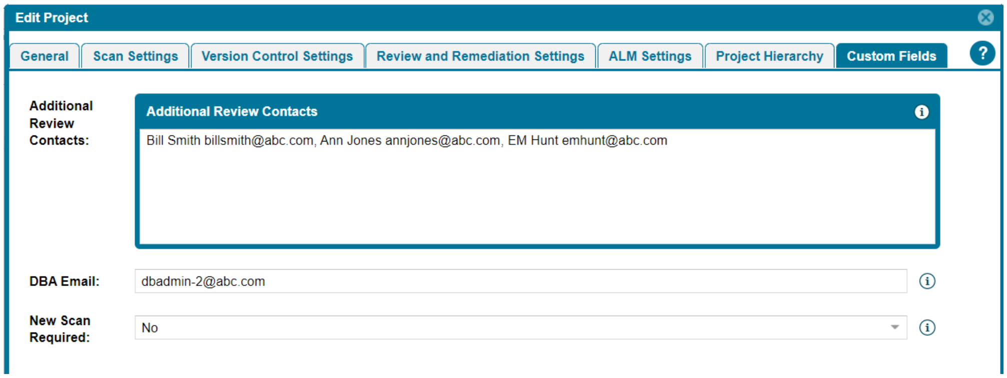
Currently, a maximum of 30 custom project fields can be created.

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 project fields, see the "Configuring Code Insight" chapter in the *Code Insight Installation & Configuration Guide*.

Updating Custom Field Values for a Project in the Web UI

Values for custom fields can be updated for a given project on the **Manage Project** > **Edit Project** > **Custom Fields** tab (accessed from the project's **Summary** tab), as shown in this example. Clicking the ⓘicon in the upper right corner of a field provides guidance for completing the field.

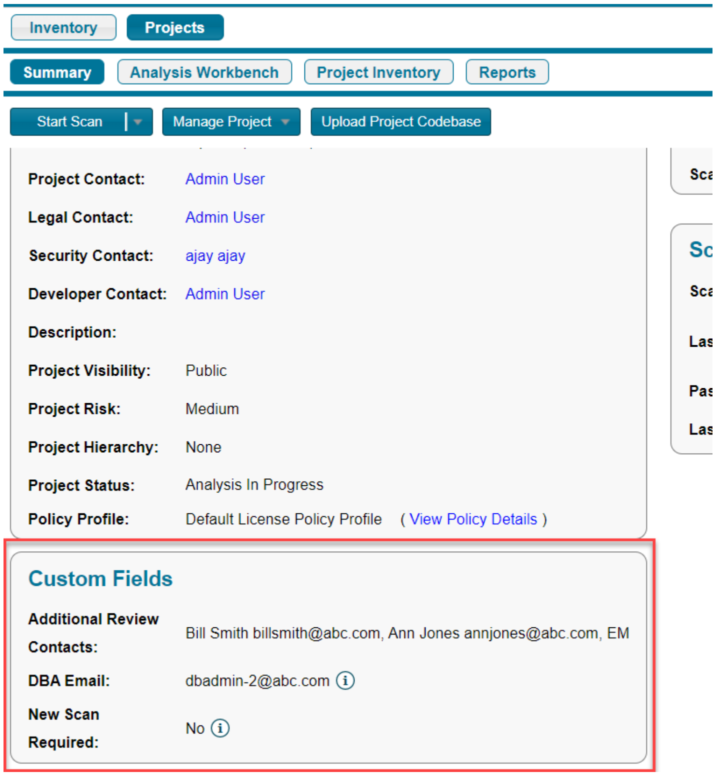


Additional Review Contacts: Bill Smith billsmith@abc.com, Ann Jones annjones@abc.com, EM Hunt emhunt@abc.com

DBA Email: dbadmin-2@abc.com

New Scan Required: No

The custom fields and their values are displayed on the project's **Summary** tab as well. This display is for informational purposes only; the field values are editable only on the **Custom Fields** tab (described previously).



Project Contact: Admin User

Legal Contact: Admin User

Security Contact: ajay ajay

Developer Contact: Admin User

Description:

Project Visibility: Public

Project Risk: Medium

Project Hierarchy: None

Project Status: Analysis In Progress

Policy Profile: Default License Policy Profile (View Policy Details)

Custom Fields

Additional Review Contacts: Bill Smith billsmith@abc.com, Ann Jones annjones@abc.com, EM

DBA Email: dbadmin-2@abc.com

New Scan Required: No

Updating Custom Field Values for a Project through REST APIs

Users can execute the **Get Project Information** REST API to view values for custom fields for a given project. Project administrators can also use the **Update Project** and **Create Project** REST APIs to update values for the custom fields in a specific project.

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

Project Reporting

This release includes the following enhancement to project reporting.

Installer for Example Custom Reports

Code Insight now provides an installer that automatically registers Code Insight's example customer reports on your Code Insight instance. An associated Readme provides complete instructions on how to run the installer. You can access the installer and its Readme here.

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.

Detection of Top-level Inventory and Direct Dependencies in .csproj Files

For `.csproj` files in .NET projects that were created using .NET Core, Code Insight is now able to report top-level inventory items and their direct dependencies even though no information about any top-level items is available in these files. To report a top-level item and its dependencies in such a file, Code Insight assigns the `.csproj` filename as the top-level inventory name and then determines its direct dependencies within the file.

Source Code Management (SCM) Support

This release includes the following enhancement to the Source Code Management (SCM) facility, used to synchronize remote codebases to Code Insight.

New REST Support for SCM

This release includes a new REST interface to create, edit, and view SCM instances. See New APIs for details.

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
CodebaseFolder	**Mark folder as reviewed/ unreviewed** `/codebaseFolder/{folderId}/review`	PUT	Marks all codebase files in the specified folder as reviewed or unreviewed.
Files	**Mark file reviewed/ unreviewed** `/files/{fileId}/review`	PUT	Marks the specified codebase file as reviewed or unreviewed.
sourceCode Management	**scmInstances** `/scmInstances`	GET	Retrieves details for the currently defined SCM instances in the project. You can view all defined instances, all defined instances of a specific type (Git, Perforce, Subversion, or TFS), or a specific defined instance. (In the details for a given instance, the **password** value used to connect to the SCM repository is masked with asterisks.)
		POST	For a specific SCM instance in a given project, tests the connection between the instance and the actual remote repository that is synchronized to the instance.
		DELETE	Deletes a specific SCM instance in a given project.
	[Git| Perforce | Subversion | TFS] scmInstances `/scmInstances/[Git|Perforce|Subversion|TFS]`	POST	Creates a new SCM instance of the specified type (Git, Perforce, Subversion, or TFS) for a given project. ***Note*** ▪ *The instance ID for the first SCM instance of a given type in a project starts with 0 and increments with each added instance of that type (or is renumbered when an instance is deleted). This ID-numbering system is not in sync with the system used in the Code Insight Web UI. When managing instances through the REST interface, always use the IDs generated by the APIs.*
		PUT	Updates property values in an SCM instance definition.

Updates to Existing APIs

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

CWE Information Added

For APIs that retrieve security vulnerability information, the property **vulnerabilityCWE** has been added to the list of properties for each vulnerability to identify the vulnerability's CWE (Common Weakness Enumeration). The property value includes both the category ID (**name** field) of the CWE and the category label (**title** field). The value contains empty brackets if the CWE is not available.

Other API Enhancements

The following lists other changes to existing APIs in this release.

Table 2 ▪ Updates to Existing APIs

Resource	API Name/Endpoint	Method	Function Description
Files	**Get details of a file by Id** `/files/{fileId}`	GET	Retrieves the following additional information for each file in the results: ● **sourceMatchCount**—Total number of source-code snippets found in the file that match other source-code snippets stored in the Code Insight data library. ● **exactFileMatchCount**—The number of files in the Compliance Library that identically match the given file. Previously, the results simply indicated (with a **true** or **false** for **sourceMatches** and **exactFileMatches**) whether matching code snippets and other exact-match files existed in the libraries.
Inventory	**Create inventory** `/inventories`	POST	Enables project analysts to update custom-field values for the inventory item. (The IDs for the custom inventory fields can be obtained through the **Get details of inventory** or **Get Project Inventory** API.)
	Update inventory `/inventories/{inventoryId}`	PUT	

Table 2 ▪ Updates to Existing APIs (cont.)

Resource	API Name/Endpoint	Method	Function Description
Project	**Get Project Information** /project/inventory/{projectId}	GET	In the results for the given project, shows the project's current values (including **null**) for the custom project fields. Only enabled custom fields are listed. If all custom fields are disabled or no custom fields have been configured for projects, an empty array is displayed in the **customFields** section.
	Create Project	POST	Enables project administrators to update custom-field values in the project. (The IDs for the custom project fields can be obtained through the **Get Project Information** API.)
	Update Project	PUT	
	Fetch Evidences for a project /project/{projectId}		For every codebase file in a given project, retrieves the following additional information in the results: ● **sourceMatchCount**—Total number of source-code snippets in the file that match source-code snippets stored in the Code Insight data library. ● **exactFileMatchCount**—The number of files in the Compliance Library that identically match the given file. Previously, the results simply indicated (with a **true** or **false** for **sourceMatches** and **exactFileMatches**) whether matching code snippets and other exact-match files existed in the libraries.
	Export Project Data /project/exportProjectData	GET	Supports the export of all custom fields for the project and its inventory.
	Import Project Data /project/{projectId}/import	POST	Supports the import of custom fields according to the specific rules explained in "Exporting and Importing Project Data" in the *Code Insight User Guide*.

Resolved Issues

The following issues are resolved in this release.

Table 3 ▪ Resolved Issues

Issue	Resolution Notes
SCA-31347	Performance has improved when using the **/projects** API to retrieve a large number of projects. Pagination has been added to the API response as one way of handling a large volume of results.
SCA-31503	Error messaging has improved for SSO sign-in errors. Instead of a default 405 Tomcat error, the message now direct users to a contact for assistance.
SCA-32039	Attempts to drag-and-drop a group of files to associate them with inventory in **Analysis Workbench** was resulting in an error and causing subsequent file operations to hang. The error occurred especially after using the **Filter to Selected Files** option to filter to desired files. This issue is now resolved.
SCA-33194	Line breaks are now retained in the Project and Audit reports.
SCA-37067	The **/project/inventory** REST API no longer fails with an “Unable to parse unicode value” message when attempting to retrieve **Notices** or **As-Found License** text for inventory.
SCA-37099	The project page is now properly refreshed once the project-branching process has completed.
SCA-37384	All project inventory is now imported during the branch process. Previously, unpublished inventory was overwriting published inventory. The order in which published/unpublished inventory is imported has been modified to help address this issue.
SCA-37668 **SCA-38964**	The missing proxy property (**http.nonProxyHosts**) is now available in proxy configuration to identify those hosts that the Scan Server should access directly—that is, *not* through the proxy.
SCA-37879	Issues that caused discrepancies between the number of security vulnerabilities recorded in remote scan-agent logs and the number shown in the Web UI have been resolved.
SCA-38007	The Gradle File Analyzer is now properly handling proprietary code, creating it as a Work in Progress inventory item and giving it the name of the rootProject or the project root folder.
SCA-38770	Gradle dependencies from the `buildscript` tag are no longer detected.
SCA-38771	The false positive reporting of `androidx.annotation` as inventory is now resolved.

Table 3 ▪ Resolved Issues (cont.)

Issue	Resolution Notes
SCA-39010	Previously, in the **Analysis Workbench**, inventory was not properly filtered if a user first filtered files by right-clicking inventory and selecting **Show Inventory Files** *and* then attempted to filter inventory by right-clicking a file in the **File Search Results** pane and selecting **Show file inventory**. This issue has been resolved.
SCA-39013	The right-click option in **File Search Results** to mark a file as reviewed or not reviewed is now working properly.
SCA-39081	The right-click option **Show file evidence** in the **File Search Results** pane is now working properly.
SCA-39284	The dependency `jsch` is now reported with the correct forge.
SCA-39336	Issues with loading projects after upgrading to 2021 R3 have been resolved.
SCA-39352	The Tomcat version installed with Code Insight 2022 R1 resolves the Tomcat vulnerability issues.
SCA-39372	Previously, the **Show file inventory** right-click option for files was not filtering inventory properly unless you performed the right-click operation from the **File Search Results** pane only. This issue is now resolved. Inventory is properly filtered when you select **Show file inventory** from either the **Codebase Files** pane or the **File Search Results** pane.
SCA-39480	The log4j vulnerability issues have been resolved with an upgrade of log4j to the latest version.

Special Notes

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

Support for the JFrog Artifactory Plugin Temporarily Removed

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

GitHub.com Change in Authentication Requirements for Git URLs

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

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

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

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

Known Issues

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

- All-Project Inventory View
- Application Life Cycle Management (ALM) Support
- Automated Workflow for Inventory Review/Publication
- Electronic Updates
- Export and Import
- Installation, Upgrades, and Configuration
- Inventory History
- Manual Codebase Analysis
- Performance
- Project Inventory
- Project Management
- Project Reporting
- REST APIs
- Scan Agent Plugins
- Scanning and Automated Discovery
- Source Code Management (SCM) Support
- Vulnerability Suppression/Unsuppression
- Web UI

All-Project Inventory View

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

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

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

Workaround: None exists.

Application Life Cycle Management (ALM) Support

The following are known issues with Code Insight ALM support.

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

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

Workaround: None exists.

Automated Workflow for Inventory Review/ Publication

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

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

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

Workaround: None exists.

Electronic Updates

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

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

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

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

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

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

```
jquery (MIT)
```

Two possible workarounds are available.

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

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

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

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

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

The following inventory mapping existed in inventory:

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

This component was mapped with License id 744.

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

The inventory item was remapped as follows:

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

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

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

Workaround: Follow these steps:

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

Export and Import

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

SCA-3222: Import overrides inventory details

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

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

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

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

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

Installation, Upgrades, and Configuration

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

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

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

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

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

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

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

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

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

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

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

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

Inventory History

The following are known issues with the Inventory History feature.

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

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

Workaround: None exists.

Manual Codebase Analysis

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

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

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

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

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

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

Workaround: None exists.

SCA-22398: Licenses not highlighted even though evidence exists

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

Workaround: None exists.

SCA-22308: “Email/URLs” evidence truncated

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

Workaround: None exists.

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

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

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

Performance

The following are known issues with Code Insight performance.

Performance slower with MySQL 8 than with MySQL 7

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

Project Inventory

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

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

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

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

Project Management

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

SCA-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 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-38346: NVD calls are not going through proxy for plugin scans

When a proxy is enabled for the generic scan-agent plugin or the Jenkins plugin, NVD calls bypass the proxy during scans.

Workaround: None exists.

SCA-40626: I/O exception during Jenkins plugin scan after deletion of “.codeinsight” folder from Jenkins agent

Users can delete the `.codeinsight` folder from the Jenkins agent if needed. However, once the folder is deleted, scans scheduled for the Jenkins plugin might fail with an I/O exception.

For your reference, this folder is identified as `$user_dir.codeinsight`, where `$user_dir` is as follows:

- `/home/<user>/` on Linux
- `C:/Users/<user>/` on Windows

Workaround: Restart the Jenkins server.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Workaround: None exists.

Scanning and Automated Discovery

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

SCA-33465: Scan agent inventory results impacted when CODEINSIGHT_ROOT variable set to wrong path

A scan agent can produce different inventory count results when the CODEINSIGHT_ROOT variable is set as environment variable and defined with an incorrect path compared to when the variable is set to the correct path or simply not used as an environment variable. (The scan agent does not require CODEINSIGHT_ROOT to be set as an environment variable.)

Workaround: If you are running the scan agent on the same machine as Code Insight Core Server, determine whether CODEINSIGHT_ROOT has been set as environment variable. If it has, ensure that it points to the correct path. Otherwise, do not set CODEINSIGHT_ROOT as an environment variable.

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

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

Workaround: None exists.

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

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

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

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

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

Workaround: None exists.

Inventory automatically published during previous scan now unpublished after rescan

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

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

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

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

Workaround: None exists.

SCA-7820: Some NPM version patterns are not supported

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

Workaround: None exists.

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

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

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

Source Code Management (SCM) Support

The following are known issues with Code Insight SCM support.

SCA-40070: Masked password value returned for SCM instances when user credentials not configured

The response for the **GET SCM Instance** API for an SCM instance shows the masked value **'******'** for the user password even though user credentials for the instance have not been defined.

Workaround: None exists.

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

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

Workaround: None exists

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

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

Workaround: None exists.

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

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

The following issue has been logged with TFS:

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

Workaround: None exists.

Vulnerability Suppression/Unsuppression

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

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

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

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

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

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

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

Workaround: Manually refresh the browser screen.

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

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

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

Workaround: Manually refresh the browser screen.

Web UI

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

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

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

SCA-20683: Project details not automatically updating after scan

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

Workaround: Refresh the screen.

Legal Information

Copyright Notice

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

Intellectual Property

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

Restricted Rights Legend

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