FlexNet Code Insight 2020 R1 SP1 Release Notes

April 2020

Introduction

FlexNet 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.

These Release Notes provide the following information about the current release of FlexNet Code Insight:

- Changes in FlexNet Code Insight R1 SP1
- New Features
- Resolved Issues
- Known Issues in this Release
- Legal Information

Changes in FlexNet Code Insight R1 SP1

The FlexNet Code Insight 2020 R1 Service Pack (SP) 1 release contains the following changes:

- Resolved issues described in Issues Resolved in 2020 R1 SP1.
- A new known issue, described in SCA-24085: Tomcat Vulnerability.

The remaining information in this document, which pertains to the previous FlexNet Code Insight 2020 R1 release, required no additional updates to address this service pack.

New Features

FlexNet Code Insight 2020 R1 introduces new features in the following areas:

- Scanning and Automated Discovery
- Friction-Free Flow
- Manual Analysis
- Reporting
- External Workflow Integration
- Project Export and Import
- External Logging
- Web UI Enhancements
- REST APIs

Scanning and Automated Discovery

This release provides the following Code Insight scan and Automated Discovery enhancements:

- Minimum Threshold for Source Code Matches
- Automated Discovery Support for Python Packages
- NPM Analyzer Enhancements

Minimum Threshold for Source Code Matches

Previously, the codebase scan always reported a codebase file as having source-code matches if the file contained three or more code snippets that matched open-source code snippets found in the Compliance Library. This internal policy could easily result in a large number of files containing evidence for the analyst to review.

Now, a new scan profile setting allows users to set the minimum number of source-code matches that a codebase scan must detect before it reports a file as having a source match. In general, the higher the minimum value, the fewer source-code matches an analyzer has to review.

Automated Discovery Support for Python Packages

FlexNet Code Insight supports the discovery of top-level inventory for pre-build and post-build artifacts of a Python project. These artifacts include source packages such as `tar.gz`, `zip`, and other such files and binary packages such as `.whl` files.

NPM Analyzer Enhancements

Previously, FlexNet Code Insight provided scan support for `package.json`. In this release, FlexNet also scans a `package-lock.json` or `npm-shrinkwrap.json` file if it exists along with `package.json`. (Either of these files helps Code Insight identify the exact dependency versions to pull from `package.json`.)

Friction-Free Flow

The following are the new features and enhancements available for creating a FlexNet Code Insight audit and review experience best suited for your environment:

- Full Rescan Option
- Auto-Publication of Inventory with Undetermined Licenses

Full Rescan Option

Previously, when you rescanned a project codebase, a full scan was run only if your project's scan settings had changed or if you had upgraded Code Insight or the Compliance Library (CL). Otherwise, an incremental scan was performed.

An option to force a full-codebase rescan is now available in the Web UI and API interface. A forced full rescan enables you to scan your entire codebase at any time even if no changes that normally trigger a full scan have occurred. You might need a forced full rescan, for example, to view the latest changes to inventory or to apply any new custom detection rules.

Auto-Publication of Inventory with Undetermined Licenses

A new project scan setting is available that gives users control over whether to publish inventory with undetermined licenses (that is, licenses with a **License** value of **I don't know**). Previously, a codebase scan always published such inventory, giving auditors no opportunity to investigate the license issue and select an appropriate license before publishing the inventory. This new option provides the means to stop the auto-publication of this inventory.

Manual Analysis

The following are the new features and enhancements available for the auditing process in the **Analysis Workbench**:

- Enhanced Copyright Detection
- Enhanced Support for License Highlighting in Partial Matches

Enhanced Copyright Detection

Previously, when a copyright was detected during a codebase scan, its corresponding evidence in the Web UI and on reports displayed as a copyright holder instead of the full copyright text. (A *copyright holder* is an incomplete copyright statement, such as the name of the copyright author only.) Now a full copyright statement, including its author, is displayed.

Enhanced Support for License Highlighting in Partial Matches

The **Partial Matches** tab now accurately highlights (in green) the specific evidence for licenses within the content of codebase files, enabling auditors to easily discern the exact license text.

Reporting

The following are the new features and enhancements available for FlexNet Code Insights reporting in this release.

Support for Custom Reports

FlexNet Code Insight's new Custom Report Framework enables you to build your own reports in the format of your choice, capturing only data that is most relevant to you. The custom reports display as selections, along with the standard FlexNet Code Insight reports, for generation from any project's **Summary** tab.

For complete details about setting up and generating a custom report, refer to the following KB article in the Flexera Community:

https://community.flexera.com/t5/FlexNet-Code-Insight-Customer/Custom-Reports-Framework-in-FlexNet-Code-Insight/ta-p/132702

External Workflow Integration

This release supports the initial phase of external workflow integration. FlexNet Code Insight lets you configure a URL link to the external workflow instance that tracks the open tasks for a given inventory item. (The link displays for the inventory item in the Code Insight Web UI.) In addition, REST API are available to update the inventory item with additional parameters describing the workflow instance—for example, its latest status, the name of the instance reviewer, or any other instance-related parameters used in your workflow system. These parameters, displayed for the inventory item in the Web UI, provide users with a quick overview of pertinent information about the workflow instance without their having to access the workflow system.

Project Export and Import

This release provides the following FlexNet Code Insight project export and import enhancements:

Option to Overwrite or Append Inventory Notes

The FlexNet Code Insight Web UI and REST interface offer a new import option that determines how notes—Notices Text, Audit Notes, Usage Guidance, and Remediation Notes— are handled for an inventory item that is identical in the source and target projects. The user can choose to have the import process overwrite target inventory notes with the notes from the source inventory or append the source inventory notes to existing in notes in the target inventory. By appending note content, the import retains information that might be relevant to the audit or review process of the target inventory.

External Logging

Starting with this release, FlexNet Code Insight can integrate with your Splunk Enterprise setup to monitor Code Insight events. Splunk Enterprise correlates, analyzes, and reports Code Insight log data, enabling users to identify and resolve operational and security issues quickly and efficiently.

For details about how to integrate Code Insight with Splunk Enterprise, refer to the following KB article in the Flexera Community:

https://community.flexera.com/t5/FlexNet-Code-Insight-Customer/FlexNet-Code-Insight-Integration-with-Splunk/ta-p/133655

Web UI Enhancements

This release includes the following enhancements to the Web UI:

- **Improved project inventory search**—You can now search published project inventory by the type and status of tasks associated with inventory.
- **Scrolls bars for lengthy descriptions**—Scroll bars have been added to tabs and dialogs in **Project Inventory** to manage the viewing of lengthy descriptions.

REST APIs

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

New APIs

The following new REST APIs were added in this release:

Resource	API Endpoint	Description
inventoryWorkflow	`/inventories/{inventoryID}/workflows`	(GET method) Retrieves workflow request details for an inventory item.
		(POST method) Creates or updates the workflow request details for an inventory item.
Project	`/projects/{projectId}`	(GET method) Retrieves metadata for a given project.
	`/projects/{projectId}`	(PUT method) Updates the metadata for a given project.
	`/projects/{projectId}/allscannedfiles`	(GET method) Retrieves a list of all scanned files for a project.

Resource	API Endpoint	Description
Reports	`/reports`	(GET method) Retrieves metadata for every standard and registered custom report.
	`/reports`	(POST method) Registers a custom report, making it available for generation from the **Select Report** dropdown on the **Summary** tab for any project.
	`/reports`	(PUT method) Updates the metadata for a given standard or custom report.
	`/reports/{reportId}`	(GET method) Retrieves metadata for a given standard or custom report.
	`/reports/{reportName}`	(DELETE method) Permanently deletes a custom or standard report.

Updated APIs

The following REST APIs were updated in this release.

Resource	API Endpoint	Description
ProjectImporter	`importer/importProjectData`	(POST method) A new parameter, `overwriteInventoryNotes`, added to overwrite existing notes in the target inventory with note content from the import data file (default), or to append note content from the import data file to the existing notes.
Scan	`/scanResource/projectScan/{projectId}`	(POST method) • New parameter, `fullRescan`, added to force a full rescan. • Support for a multiple-scanner environment (no new parameter added).

Resolved Issues

The following issues have been resolved in FlexNet Code Insight 2020 R1 and its associated service packs:

- Issues Resolved in 2020 R1 SP1
- Issues Resolved in 2020 R1

Issues Resolved in 2020 R1 SP1

The following issues are resolved in FlexNet Code Insight 2020 R1 SP1 release.

Table 1 • Resolved Issues

Issue	Description
SCA-22569	Stored XSS (cross-site scripting) issues occurring in certain areas of the Code Insight Web UI.
SCA-22683	No prevention against the acceptance of iframe objects (containing stored XXS) that can be injected through certain Code Insight Web UI elements.
SCA-22686	User-privilege enforcement issues that enable unauthorized users to use Spring MVC calls to access projects for critical business use cases.

Issues Resolved in 2020 R1

The following issues were resolved in FlexNet Code Insight 2020 R1 release.

Table 2 • Resolved Issues

Issue	Description
SCA-7759	Rescans not showing expected results when scan settings change.
SCA-17584	Long component and inventory descriptions truncated in **Project Inventory** (no scroll bar available).
SCA-18676	Failure to identify copyright patterns that do not include a year.
SCA-20008	Unable to use REST API to upload codebases to a remote Scan Server.
SCA-20139	No inventory created if `package.json` contains incorrect versions.
SCA-20358	Failure to detect known vulnerabilities not detected for Jenkins DSL Plugin 1.7.1.
SCA-20772	User unable to select the intended license when manually creating an inventory item.
SCA-21026	Failure of Automated Discovery to work with a proxy server configured with authentication to connect to external URLs during a scan.
SCA-21052	First-level dependencies not being identified in `package.json`.

Known Issues in this Release

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

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 picklists, 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.

Scanning and Automated Discovery

SCA-17065: As-Found License text not migrated

As-Found License text detected during a codebase scan that was performed before a migration no longer displays for the project post-migration.

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 will 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.

Project 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-3123: Inventory Only import does not process custom vulnerabilities

Import does not process custom vulnerabilities and custom vulnerability mappings on import into a project of type “Inventory Only”.

Workaround: Run import into a project of type “Standard”.

Manual Analysis

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.

Inventory Management

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

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

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

Project Administration

SCA-10791: Unable to delete large projects on SQL Server

Attempting to delete a large project (for example, a codebase containing 30K+ files) on a Code Insight instance using the SQL Server database can result in a SQL grammar exception. Smaller projects are not impacted.

Workaround: Delete the project directly from the database.

Security Vulnerabilities

SCA-24085: Tomcat Vulnerability

The Tomcat vulnerability CVE-2020-1938 (with a base score of 9.8, considered “critical”) affects the current Tomcat version installed by FlexNet Code Insight. The vulnerability is the result of the Apache JServ Protocol (AJP) connection, which uses the 8009 port by default. Tomcat treats an AJP connections as having higher trust than HTTP connections. If such connections are available to an attacker, they can be exploited in unexpected and damaging ways.

For more information about this vulnerability (including a list of all affected Tomcat versions), access the following site:

https://nvd.nist.gov/vuln/detail/CVE-2020-1938

Preferred solution: Upgrade the current Tomcat version used by Code Insight from 8.5.41 to 8.5.51.

The bundle version of Apache Tomcat will be upgraded in a future release of FlexNet Code Insight. Meanwhile, since FlexNet Code Insight does not require the APJ connector, it can be disabled by using the instructions described in the first workaround below. Another way to avoid the vulnerability is simply to block the 8009 port, described in **Workaround 2**.

Workaround 1: Disable the APJ connector.

Since Code Insight does not require the APJ connector, it can be disabled. Once the connector is disabled, you can continue to use port 8009.

To disable the APJ connector, follow these steps:

1. Open the appropriate Tomcat configuration file in a text editor:
   - On Windows, open `{CODEINSIGHT_ROOT_DIR}\tomcat\conf\server.xml`.
   - On Linux, open `/etc/tomcat9/server.xml`.
2. Search for the string `8009`, and comment out the line about AJP protocol, as shown in the highlighted text:

   ```
   <!-- Define an AJP 1.3 Connector on port 8009 -->
   <!-- Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /> -->
   ```

3. Save the file.
4. Restart the Apache Tomcat service. (For assistance, see "Starting and Stopping Tomcat" in the *FlexNet Code Insight Installation and Configuration Guide*.)

Workaround 2: Block port 8009 for incoming connections on your firewall.

Use the appropriate method to block the port.

On Windows

A Windows server usually blocks the port by default, but you can create an explicit rule to ensure that port 8009 is blocked on your firewall.

To block the port on Windows, use these steps:

1. Create a rule that blocks all inbound connections on port 8009.
2. To ensure that the port is blocked, run the following command:

   ```
   netstat -ano | findstr 8009
   ```

   If the port is no longer active, you receive negative results.

On Linux

To block the port on Linux, use these steps:

1. Use your security product or the Linux iptables utility to block port 8009.

If you use the iptables utility, use the following command to block the port:

```
iptables -A INPUT -j DROP --destination-port 8009
```

2. To ensure that the port is blocked, run the following command:

   ```
   ss -a | grep 8009
   ```

   If the port is no longer active, you receive negative results.

SCA-22557: Vulnerabilities not reported for certain components

Post-scan, FlexNet Code Insight is not reporting security vulnerabilities for the component `activemq-client-5.15.0`.

Workaround: None exists.

SCA-22383: RustSec advisory links invalid

The URL that FlexNet Code Insight is currently providing for any RustSec security vulnerability uses an invalid path that points to component information, not to the advisory. The link should point to the specific advisory in https://rustsec.org/advisories.

Workaround: In a browser, enter the correct path, replacing the component path with the advisory path. For example, if Code Insight shows the invalid link `https://github.com/RustSec/advisory-db/tree/master/crates/spin-RUSTSEC-2019-0031`, enter the following URL in the browser instead:

https://rustsec.org/advisories/RUSTSEC-2019-0031.html

Reporting

SCA-22054: Project Report not showing latest NVD information

New security vulnerabilities captured in the most recent scan are not displaying on the Project Report.

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

SCA-21549: Error generating the Project Report when data exceeds Excel limit

The generation of a Project Report in Excel format fails when the report entries exceed the Excel entries-per-sheet limit.

Workaround: None exists.

Web UI

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

The **Last 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 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.

SCA-3256: Cases of slow UI performance during scan on systems with hundreds of projects

On systems with more than 500 projects, users can experience a performance lag while a scan is running.

Workaround: Wait for the scan to complete prior to bringing up the Web UI.

Email Notifications and Reports

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.

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 unexpected 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: 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”.

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.

Plugins

SCA-3378: Jenkins Scan 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.

Archives

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.

Legal Information

Copyright Notice

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexera.com/producer/company/about/intellectual-property/. All other brand and product names mentioned in Flexera 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.