

FlexNet Code Insight 2019 R3 Release Notes

October 2019

Introduction	3
About FlexNet Code Insight 2019 R3.....	3
New Features.....	3
Project Administration	4
Enhanced Archive Support for Codebase Uploads	4
Project Risk Value Added to the Export JSON Output.....	4
My Projects Filter Enabled by Default	4
Process Flow.....	5
Ability to Assign Task Owner During Task Creation.....	5
Search Available for String Output in Partial Matches	5
Scanning and Automated Discovery	5
Support for Custom Detection Rules.....	5
Support for git Ecosystems.....	6
Support for Multiple Scan Servers.....	6
Support for CVSS v3.0 Vulnerability Data.....	6
REST APIs	7
Web UI Enhancements	7
Reports	8
New “All Scanned Files” Worksheet in Project Report	8
Notices Text Now Populating As-Found License Text in Project Report	8
Resolved Issues.....	8
Known Issues in this Release	9
Installation / Configuration	9
Scanning and Automated Discovery	10
Export / Import	11
Analysis Workbench	11
Inventory Management.....	12
Data Library.....	12
Project Administration	12
Web UI.....	13

Email Notifications and Reports	13
REST APIs	14
Plugins	14
Archives	15
Legal Information	16

Introduction

These Release Notes provide the following information about the FlexNet Code Insight 2019 R3 release:

- [About FlexNet Code Insight 2019 R3](#)
- [New Features](#)
- [Resolved Issues](#)
- [Known Issues in this Release](#)
- [Legal Information](#)

About FlexNet Code Insight 2019 R3

The FlexNet Code Insight 2019 R3 is the next generation Open Source security and compliance management solution with the following core capabilities:

- **File-based scanner** designed for fast rescans that fit into a continuous scan process.
- **Automated discovery framework** for detection of various package formats, EXE/DLL files, and targeted components, with dependency support for multiple package managers.
- **Scan agent framework** for remote scanning on various engineering applications with scan results sent to Code Insight for review, remediation and alerting.
- **Automated inventory review with remediation** according to legal and security policy.
- **Advanced security vulnerability** detection, reporting, alerting, and search; with access to vulnerability information from multiple sources.
- **Web interface** for configuration, analysis, management and reporting functions.
- **Powerful search** for locating high risk inventory per project or across the organization.
- **Integrations** with various engineering systems for a seamless fit into your enterprise IT environment and DevOps lifecycle.
- **REST APIs** with Swagger documentation for programmatic interaction with Code Insight and development of extensions and integrations.

New Features

The FlexNet Code Insight 2019 R3 provides new features in the following areas:

- [Project Administration](#)
- [Scanning and Automated Discovery](#)
- [Vulnerability Reporting](#)
- [REST APIs](#)

- [Web UI Enhancements](#)
- [Reports](#)

Project Administration

This release includes the following new administrative features to help with the setup and management of Code Insight projects.

Enhanced Archive Support for Codebase Uploads

Archive support for codebase uploads has been enhanced as follows:

- Previously, the FlexNet Code Insight supported uploading a codebase only as a .zip file. Supported archive types to upload the codebase now include .tar, .tar.gz, and .7z files, along with the already supported .zip file.
- Previously, the uploaded archive was expanded, but archives within the codebase were not. Analysts were required to manually expand these archives to examine their contents. The upload process can now be configured to perform first-level only or recursive archive expansion within the codebase. (Additionally, an option to expand only the uploaded archive is available to perform the previous upload behavior.)

See the “Uploading a Project Codebase” section in the *FlexNet Code Insight User Guide* for more information about the new codebase-upload configuration options as well as a list of archive types that can be expanded within the codebase.

Scanning and Automated Discovery

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

- [Support for Custom Detection Rules](#)
- [Support for git Ecosystems](#)
- [Support for Multiple Scan Servers](#)

Support for Custom Detection Rules

During a FlexNet Code Insight project scan, the Automated Analysis component of the Scan Server uses a set of internal detection rules, stored in the Code Insight data library, to automatically generate inventory items. However, in some cases, your manual analysis might find codebase files that are associated with a third-party component but not associated with inventory. Code Insight now enables you to create custom detection rules that convert such findings into future automatically-created inventory items. These rules are saved to the Code Insight data library for global use by Automated Analysis during scans on future projects (or rescans of current projects).

Code Insight provides two methods for creating custom rules:

- In **Analysis Workbench**, within the context of an inventory item that you have manually updated or created to add codebase files. This method pre-populates much of the information needed to create the rule, including the MD5 value for each file associated with the inventory item.
- From the new **Custom Data | Custom Detection Rules** tab on the Code Insight main menu. From here you can create custom rules from scratch, as long you know the MD5 values for the files on which you are basing the rule.

Additionally, the new **Custom Detection Rules** tab provides a single location for managing custom rules, enabling you not only to create rules, but also to view and edit any custom detection rule in your system.

For more information about custom detection rules, see “Managing Custom Detection Rules” in the *FlexNet Code Insight User Guide*.

Support for git Ecosystems

FlexNet Code Insight now scans configuration files inside the `.git` folders encountered in a project codebase and uses the detected evidence to automatically create inventory items.

Support for Multiple Scan Servers

Previously, FlexNet Code Insight supported one Scan Server to handle the codebase scans for all projects. Code Insight now supports multiple Scan Servers, thus providing the means for users to distribute codebase scans among servers.

The FlexNet Code Installer, while maintaining the option to install the Core Server and Scan Server on the same instance, now offers an option to install only a Scan Server on a given instance, thus allowing for various deployment configurations. Once a Scan Server is installed, the Administrator then “adds” the Scan Server to the Code Insight system—that is, identifies the server to the Core Server to make it available for scanning. The administrator can also view the status of each Scan Server and enable or disable a server to control its availability in Scan Server lists.

The codebase for a given project can be assigned to only one Scan Server (but multiple project codebases can be assigned to different Scan Servers). All codebases assigned to a given Scan Server are stored on that server in a location that specified when the server is added to the system.

For more information about multiple Scan Servers, see the “Installing FlexNet Code Insight” and “Configuring FlexNet Code Insight” in the *FlexNet Code Insight Installation Guide*.

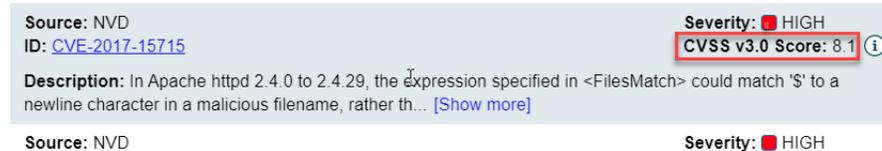
Vulnerability Reporting

This release provides the following vulnerability-reporting features and enhancements.

Support for Common Vulnerability Scoring System (CVSS) v3.0

FlexNet Code Insight now supports CVSS v3.0 (in addition to its previous support of CVSS v2) for displaying the scores and severities of security vulnerabilities associated with inventory components. The Administrator uses the new **System Settings** tab on the **Administration** page to configure Code Insight to use either CVSS v2 or CVSS v3.0.

When users view details about vulnerabilities associated with inventory in the **Security Vulnerabilities** dialog, they can easily see which CVSS standard is being used in their Code Insight system. They can also view both scores for a given vulnerability by clicking the  button next to the displayed score.



The screenshot shows a vulnerability detail card with the following information:

- Source:** NVD
- ID:** [CVE-2017-15715](#)
- Description:** In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '\$' to a newline character in a malicious filename, rather th... [\[Show more\]](#)
- Severity:**  HIGH
- CVSS v3.0 Score:** 8.1 

Note that switching between CVSS versions will affect CVSS scores and severity values for vulnerabilities, as displayed in the Web UI and reports. The change also has an impact on policies based on CVSS scores and vulnerability severities. However, the existing inventory priorities of an already scanned project will not change.

For more information, see the “Security Vulnerabilities Associated with Inventory” section in the *FlexNet Code Insight User Guide* and the “Setting the Common Vulnerability Scoring System (CVSS) Version” section in the *FlexNet Code Insight Installation and Configuration Guide*.

REST APIs

The following are new or updated FlexNet Code Insight REST APIs:

- Updates to Inventory API to include Auditor Notes and Notices Text when creating or updating inventory.
- New Inventory API to create inventory.
- New Component and License API to create custom components, versions, and licenses.
- New Component API to retrieve component details by component ID
- New Rules API to create and manage custom detection rules.
- New Project API to retrieve files containing third-party evidence
- New Task APIs to create, update, retrieve (by project or inventory), reassign ownership of, and close tasks.
- Update to the Create Project API to include a new `scanServerAlias` property for specifying a Scan Server with which to associate the project.

Web UI Enhancements

This release includes the following enhancements to the Web UI:

- [Ability to Assign Task Owner During Task Creation](#)
- [Search Available for String Output in Partial Matches](#)

- “My Projects” Filter Enabled by Default

Ability to Assign Task Owner During Task Creation

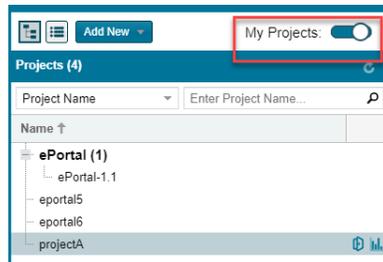
Previously, when users created tasks, the task was automatically assigned to the default task owner. This assignment could be changed only by saving and reopening the task to edit the value. Now when creating a task, users can assign the task to a different user.

Search Available for String Output in Partial Matches

The **String Output** list in the **Partial Matches** view now provides a search field to help users more easily locate specific strings, especially when the list is extensive.

“My Projects” Filter Enabled by Default

The **My Projects** toggle above the **Projects** list is now turned on whenever you log into FlexNet Code Insight, saving you the effort of changing this filter to locate your projects each time you open Code Insight. You can always turn the toggle off to view all projects during your current Code Insight session.



Reports

This release includes the following enhancements to FlexNet Code Insight reports.

New “All Scanned Files” Worksheet in Project Report

A new **All Scanned Files** worksheet is available on the Excel version of the Project report. This worksheet lists all scanned files and, for each file, any license, copyright, email, URL, or search-term evidence found in that file. In cases where no scan evidence is found for a file, these cell values will be empty. This information is not available in the JSON version of the Project report.

Notices Text Now Populating As-Found License Text in Project Report

If a project inventory item contains **Notices Text** content, it is now shown in the **As-Found License Text** column in the Project report. However, if the inventory item has no **Notices Text** content, the item’s **As-Found License Text** content populates the **As-Found License Text** column in the report. In either case, depending on the amount of content, a link to the license content might be provided instead of the actual content.

Note that, if the inventory item has no **Notices Text** or **As-Found License Text** content, the **As-Found License Text** column in the report is blank.

Resolved Issues

The following issues are resolved in this release.

Table 1 • Resolved Issues

Issue	Description
SCA-5063	Browser search not showing strings outside of scrolling pane.
SCA-17746	Scans failing with TFS plugin failing with “Batch update returned unexpected row count...” error.
SCA-18349	Incorrect versions available for the “golang” component.
SCA-18379	Notices report not picking up contents from As-Found License Text when previous Notices Text contents are cleared.
SCA-18481	Global defaults overriding project-level configuration.
SCA-18827	Plexus license being detected when no explicit evidence is found.
SCA-19134	Incorrect BSD license detection

Known Issues in this Release

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

- [Installation / Configuration](#)
- [Scanning and Automated Discovery](#)
- [Export / Import](#)
- [Analysis Workbench](#)
- [Inventory Management](#)
- [Data Library](#)
- [Project Administration](#)
- [Web UI](#)
- [Email Notifications and Reports](#)
- [REST APIs](#)
- [Plugins](#)

- [Archives](#)

Installation / 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 result in an error.

Scanning and Automated Discovery

SCA-17065: As-Found License text not migrated

As-Found License text detected during a project 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-7759: Rescan does not process some Scan Profile changes

There are cases when a rescan does not reflect the current state of the codebase and project settings. For example, scanning with transitive dependencies on, followed by a rescan of top-level dependencies only, will not delete inventory generated for the transitive dependencies. Similarly, rescanning a project after changing the codebase files does not delete inventory generated by the original scan.

Workaround: Scan the materials in a new project or manually clean up the outdated inventory using bulk delete functionality in **Analysis Workbench** (multi-select the inventory and right-click to select delete).

SCA-3296 / SCA-2587: Duplicate Inventory for some CocoaPods and Bower projects

When a CocoaPods project has both a `.podspec` file and a `podfile.lock` file, duplicate inventory is created in Code Insight. Likewise, inventory that contains both a `bower.json` and `composer.json` file, can result in duplicate inventory.

Workaround: Review and remove duplicate inventory after scan completion; you can select multiple items for deletion using multi-select functionality.

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.

SCA-17968: As-Found License Text field is not being populated in certain cases

In this release, when a specific rule is triggered, the **As-Found License Text** field is not being populated in a few cases.

Workaround: None exists.

SCA-20008: Unable to use REST API to upload codebases to a remote Scan Server

When a Scan Server is installed on an instance separate from the one on which the Core Server is installed, users cannot use REST API to upload codebases to that Scan Server.

Workaround: If possible, use the FlexNet Code Insight Web UI to upload codebases to a remote Scan Server.

Export / Import

SCA-7794: Export via Web UI is not available for Inventory projects

The **Export Project Data** option is available on the **Manage Projects** dropdown for only projects of type “Standard”. Projects of type “Inventory-Only”, such as those created for plugin use, do not show the export option.

Workaround: Use the Export Project REST API to perform export of inventory-only projects.

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”.

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.

Analysis Workbench

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.

SCA-7896: Remote File search shows wrong file count for empty result set

In **Analysis Workbench > Partial Matches**, searching for a license that is not valid can show a file count result of -1 when the result should be zero.

Workaround: None exists.

SCA-17523: Invalid search strings for projects still showing results

(SQL Server on Windows only) When you use the **Project Inventory** filter to search projects in the **Projects** list, invalid search strings such as `[a-z]` and `[0-9]` are producing results.

SCA-16952: Search strings with underscores showing no results

(SQL Server on Windows only) When you use the **Project Name** filter to search for projects in the **Projects** list whose names contain an underscore (`_`), no results are generated if the search string you provide includes an underscore (`_`).

Workaround: Search for projects whose names contain underscores as long as you do not include an underscore in the search string.

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.

Data Library

SCA-17766: “Search By Keywords” string with underscores not working for custom components

(SQL Server on Windows only) The **Search By Keywords** option on the **Lookup Component** window provides a means to search for existing components by their name or a partial string in the name. However, this option does not locate custom components when the search value you enter contains an underscore (_).

Workaround: Search for custom components by their forge or forge URL.

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.

Web UI

SCA-2290: Refresh required to update filtered search results in Web UI

Search results are not automatically refreshed when the contained data is edited (for example, editing an inventory item does not automatically update the search result set to reflect the change).

Workaround: Use F5 to refresh the page.

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-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.

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-19331: Inventory priority set to P3 for inventory created using Create Inventory REST API

When inventory is created using the Create Inventory REST API, by default the inventory priority is set to 3 regardless of the license priority.

Workaround: None exists.

Plugins

SCA-11736: Eclipse Plugin

At this time, the Eclipse plugin is only supported with Java projects and not with General projects.

Workaround: None exists.

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-20065: Top-level *.tar.gz file not deleted after full recursive expansion of uploaded codebase

The top-level *.tar.gz file is not deleted when you upload a codebase using the **Uploaded file and all contained archives file** expansion option on the **File Upload** dialog.

Workaround: Search those inventory items whose name includes “Found inside *archiveName.tar.gz*”, and manually delete the ones that are redundant with other inventory items based on the extracted files.

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

Copyright © 2019 Flexera

This publication contains proprietary and confidential information and creative works owned by Flexera 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 is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

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

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.