Micro Focus Fortify Product Announcement: SCA, SSC, WI & WIE 20.2.0

Micro Focus Fortify Product Announcement
Date: November 17, 2020
Version 20.2.0

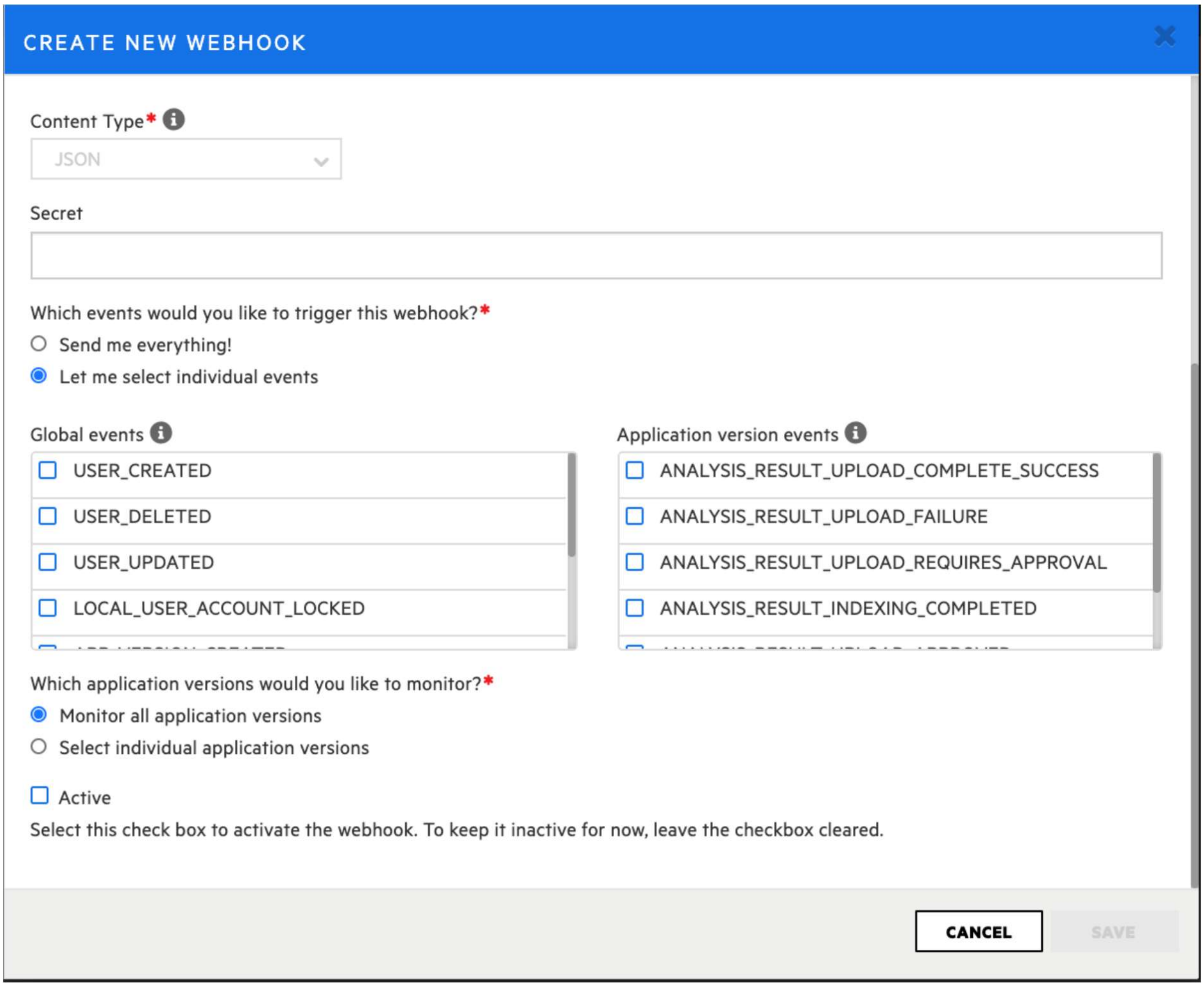
Micro Focus Fortify is pleased to announce the availability on 11/17/20 of version 20.2.0 of Fortify Software Security Center (SSC), Fortify Static Code Analyzer (SCA), WebInspect, and WebInspect Enterprise. The Fortify 20.2.0 on-premises release continues to advance the strategic initiatives of the product suite by adding accelerated language support, providing end users with actionable results, expanding our open source solution with Sonatype, offering hybrid delivery methods, and shifting application security left.

Micro Focus Fortify Software Security Center

The following features have been added to Fortify Software Security Center.

Webhooks

The latest version of Fortify Software Security Center includes a new Webhook feature in the Administrative section. Use it to create hooks for system and application version events directly in the UI or API. When available, Webhooks can be helpful in updating external pipelines with Fortify Software Security Center data. This feature will drive our next generation of build failure workflows in the continuous integration plugins that we currently offer.



CREATE NEW WEBHOOK

Content Type*

JSON

Secret

Which events would you like to trigger this webhook?*

○ Send me everything!

● Let me select individual events

Global events

□ USER_CREATED

□ USER_DELETED

□ USER_UPDATED

□ LOCAL_USER_ACCOUNT_LOCKED

Application version events

□ ANALYSIS_RESULT_UPLOAD_COMPLETE_SUCCESS

□ ANALYSIS_RESULT_UPLOAD_FAILURE

□ ANALYSIS_RESULT_UPLOAD_REQUIRES_APPROVAL

□ ANALYSIS_RESULT_INDEXING_COMPLETED

Which application versions would you like to monitor?*

● Monitor all application versions

○ Select individual application versions

□ Active

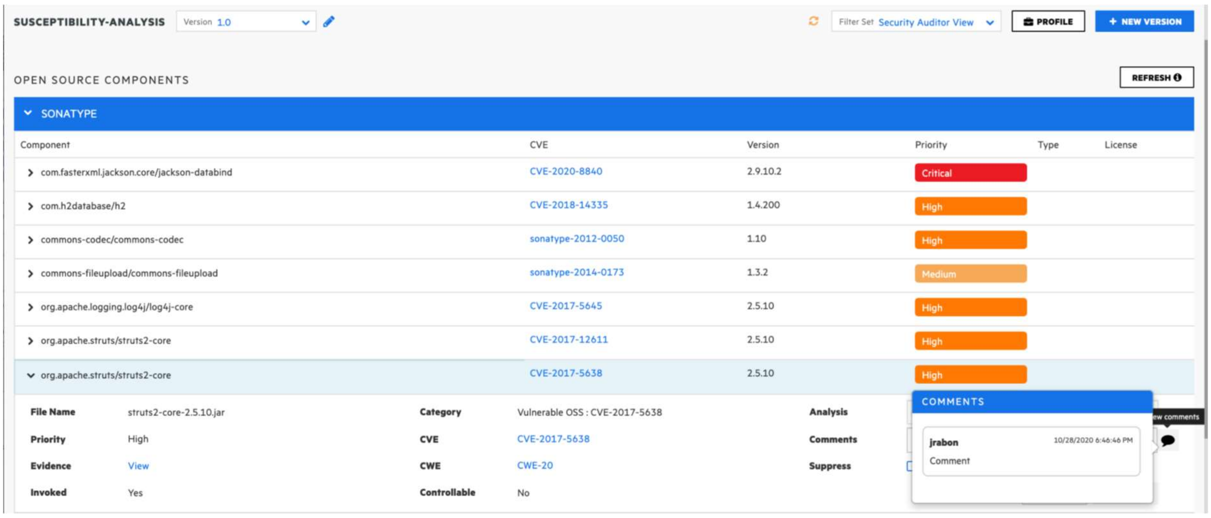
Select this check box to activate the webhook. To keep it inactive for now, leave the checkbox cleared.

General Performance Improvements

- Ahead-of-time compilation reduces the time needed to download the JavaScript for our user interface. Our testing indicates a 40% reduction in the overall package size.
- The Issue endpoint has been refactored for better direct API performance.

Open Source Components View

A new Open Source Components view appears on the Open Source tab of the Issues page. This view displays Sonatype open source issues. The user can audit these issues directly in the view. This view also includes two new fields: Invoked and Controllable. These fields indicate whether the Sonatype-identified method or function(s) were called or user-controlled input reached this function/method in your custom code.



Component	CVE	Version	Priority	Type	License
com.fasterxml.jackson.core/jackson-databind	CVE-2020-8840	2.9.10.2	Critical		
com.h2database/h2	CVE-2018-14335	1.4.200	High		
commons-codec/commons-codec	sonatype-2012-0050	1.10	High		
commons-fileupload/commons-fileupload	sonatype-2014-0173	1.3.2	Medium		
org.apache.logging.log4j/log4j-core	CVE-2017-5645	2.5.10	High		
org.apache.struts/struts2-core	CVE-2017-12611	2.5.10	High		
org.apache.struts/struts2-core	CVE-2017-5638	2.5.10	High		

File Name	struts2-core-2.5.10.jar	Category	Vulnerable OSS : CVE-2017-5638	Analysis	
Priority	High	CVE	CVE-2017-5638	Comments	
Evidence	View	CWE	CWE-20	Suppress	
Invoked	Yes	Controllable	No		

OWASP ASVS v4.0 Report

The OWASP ASVS v4.0 report provides an easy way to consolidate the list of requirements for secure software development as defined by this standard.

ScanCentral DAST

ScanCentral DAST joins the family! The ScanCentral tab in Fortify Software Security Center now has both SAST and DAST options. WebInspect customers can now orchestrate dynamic testing and automation from within Fortify Software Security Center.

Java 11 Support

Support for Java 11 in combination with Tomcat 9. See the *Micro Focus Software System Requirements* document for more information.

Fortify ScanCentral SAST

Product Name Change

With the introduction of Fortify ScanCentral DAST (for dynamic scans), Fortify ScanCentral was re-named ScanCentral SAST. For information about Fortify ScanCentral DAST, see the *Micro Focus Fortify ScanCentral DAST Configuration and Usage Guide*.

JavaScript Packaging Improvement

There is a new parameter available in the ScanCentral SAST client to include npm dependencies, when they are not present in the current working directory. Users can add –scan-nodemodules to ScanCentral SAST client command. ScanCentral SAST will download the node modules and include them for translation and analysis. If this flag is not present, even if the node modules are there, we exclude them by default.

Quality Improvements

- ScanCentral SAST has improved support for multiple versions of Fortify Static Code Analyzer. When scanning resources are unavailable for a particular client version, more informative error messages will be issued.
- The auto upgrade feature now patches all connected ScanCentral SAST clients, avoiding the need to manually install the patches multiple times.

- ScanCentral SAST standalone clients receive both patch upgrades and major version upgrades (controller is upgraded).
- Embedded ScanCentral SAST clients from Fortify Static Code Analyzer will not automatically upgrade to the new version, but do receive patches.
- Custom build parameters that are required for software compilation are now included and invoked by ScanCentral SAST clients. Previously, the default build invocation parameters for supported build tools was used.

Micro Focus Fortify Static Code Analyzer

The following features have been added to Fortify Static Code Analyzer.

Java

- Support added for Java 14
- Native support for Lombok added. It is not necessary to use “delombok” anymore
- Support added for Kotlin interoperability

If your project contains Java code that refers to Kotlin code, include all the source directories in the translation command so that the Kotlin function calls are correctly resolved.

.NET

- Now uses MSBuild 16.6
- Added Generics Type support

Swift/Obj C

- Added support for XCode up to version 11.7
- JavaScript

JavaScript

- Support added for TypeScript 3.3- 4.0
- Support added for ECMAScript 2019 and 2020

Kotlin

- Added full support for Kotlin 1.3.50
- Kotlin support is no longer a Technology Preview
- Added Kotlin Java Interoperability

If your project contains Kotlin and Java source code, you can use the Java source to resolve any Kotlin types that refer to Java files

- Added Kotlin for Android support

Go

- Added support for Go Modules
- Refactoring of Go translation which allows easier translation and takes away the need to have Go installed on the translation machine

COBOL

- Added support for IBM Enterprise COBOL up to version 6.1

Python

- Added support for Python 3.8
- Improved imports support for Python

Docker

- Added support for running Fortify Static Code Analyzer in a Docker container
- Added support for scanning Docker configuration files

ABAP Extractor

- Improved performance

- Added option to block the download of SAP standard code

Modular Analysis (Technology Preview)

- Updated to include control flow analysis

Speed Dial (Technology Preview)

The first version of Speed Dial provides a selection of configuration files to select the breadth and depth of the desired Fortify Static Code Analyzer scan.

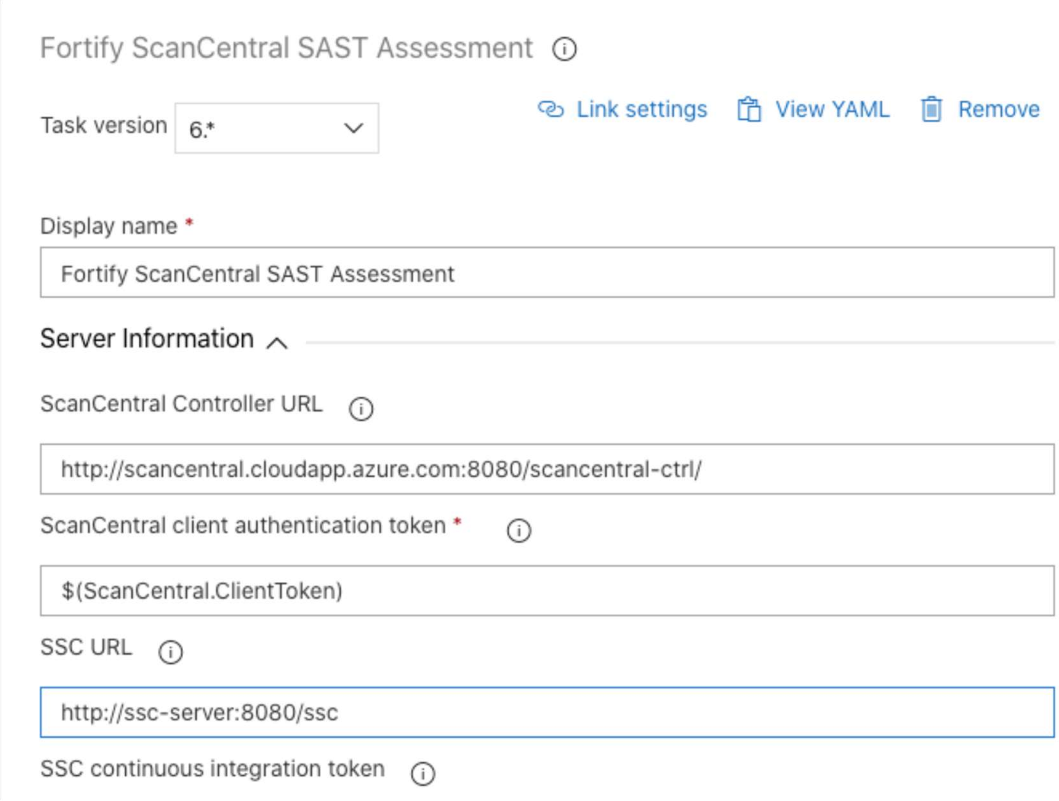
Micro Focus Fortify Static Code Analyzer Tools

The following features have been added to Fortify Static Code Analyzer Tools.

Azure DevOps

- New ScanCentral SAST Task

With the new Azure DevOps task, you can programmatically install the ScanCentral SAST client from the controller to configure and use the ScanCentral SAST client to orchestrate remote scanning from Azure DevOps. This works for both hosted and local build agents.



Fortify ScanCentral SAST Assessment

Task version: 6.*

Display name *: Fortify ScanCentral SAST Assessment

Server Information

ScanCentral Controller URL: http://scancentral.cloudapp.azure.com:8080/scancentral-ctrl/

ScanCentral client authentication token *: $(ScanCentral.ClientToken)

SSC URL: http://ssc-server:8080/ssc

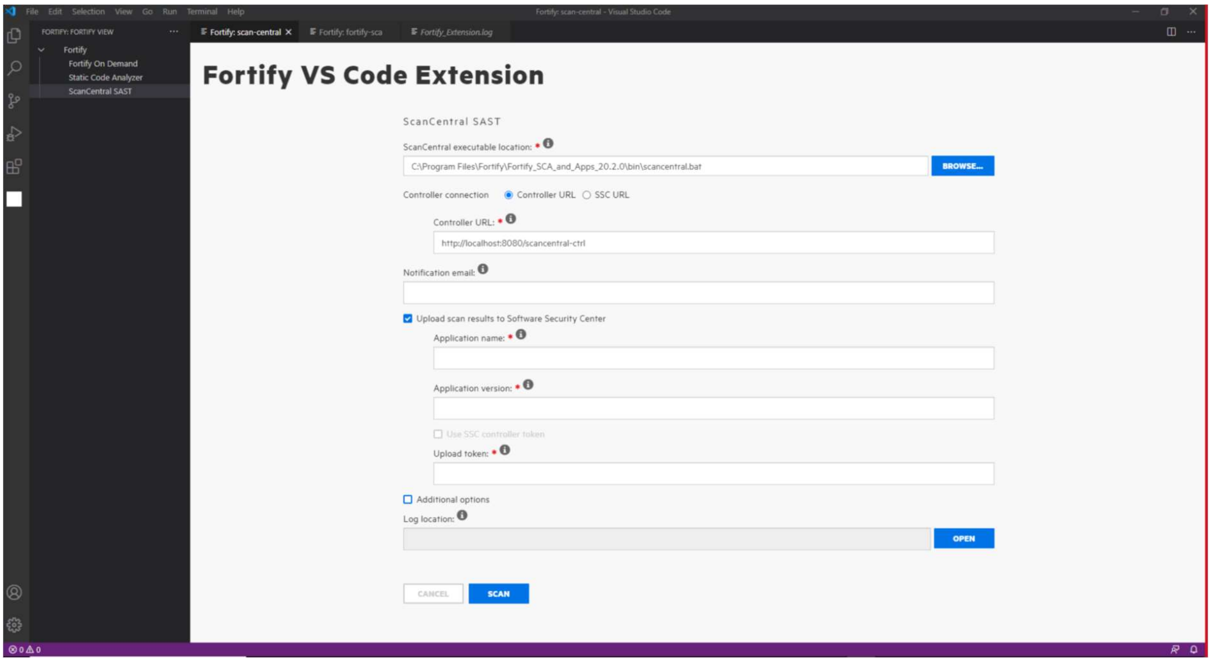
SSC continuous integration token

- New ScanCentral DAST Task

In Azure DevOps, this task allows you to automate and orchestrate remote dynamic (WebInspect) scans from the ScanCentral DAST module inside of Fortify Software Security Center.

Visual Studio Code

Fortify is happy to welcome the Fortify Visual Studio Code Extension to our IDE plugin family. In this first release, local Fortify Static Code Analyzer scans, remote scans via ScanCentral, and remote scans via Fortify on Demand are all supported.



Fortify VS Code Extension

ScanCentral SAST

ScanCentral executable location: *
C:\Program Files\Fortify\Fortify_SCA_and_Apps_20.2.0\bin\scancentral.bat

Controller connection ● Controller URL ○ SSC URL

Controller URL: *
http://localhost:8080/scancentral-ctrl

Notification email:

☑ Upload scan results to Software Security Center

Application name: *

Application version: *

□ Use SSC controller token

Upload token: *

□ Additional options

Log location:

Token Authentication in all the Tools

Fortify has introduced token-based authentication to Fortify Static Code Analyzer from Audit
Workbench and the Visual Studio, Eclipse, and IntelliJ plugins.

Support for OWASP ASVS v4.0 Report

Support has been added for OWASP ASVS v4.0 reports.

Micro Focus Fortify WebInspect

The following features have been added to Fortify WebInspect.

Automatic Detection of Single-page Applications

Fortify continues to improve usability with time-saving features that eliminate manual configuration of scans. WebInspect 20.2.0 detects when applications use modern frameworks such as Angular and React and automatically adjusts its configuration to provide the best coverage.

Redundant Page Detection

Applications with lots of redundant content, such as content management systems and catalog sites, can cause unnecessarily long-running scans. With WebInspect 20.2.0, you can use an advanced redundant page detection algorithm to reduce these scan times.

ADFS CBT Support

Per advice from Microsoft, many organizations are implementing a channel binding token (CBT) to secure Active Directory Federation Services (ADFS) authentication. WebInspect 20.2.0 now supports this extended protection mechanism. Look at Scan Settings under Network Authentication > Method > ADFS CBT to use this new feature, and reference the Help topic for details.

Engine 5.1 Updates

Fortify continues to evolve its engines to improve coverage and performance. WebInspect 20.2.0 provides a faster crawl and audit, and better application support from the web macro recorder. Finally, as a sneak peak of things to come in 2021, the Web Macro Recorder with Macro Engine 5.1 now attempts to detect and display client-side frameworks that are used in the target application. For more information, read the Help.

OpenSSL Technical Preview

WebInspect 20.2.0 introduces a technical preview of our OpenSSL integration. This integration provides support for TLS 1.3, and provides an option for customers whose system administrators may be restricting the Microsoft SCHANNEL stack. The setting may be enabled in the UI at Edit > Application Settings > General.

ScanCentral DAST

Fortify is excited to release a new DAST orchestration and automation platform integrated right into Software Security Center 20.2.0!

Micro Focus Fortify WebInspect Enterprise

The following features have been added to Fortify WebInspect Enterprise.

Automatic Detection of Single-page Applications

Fortify continues to improve usability with time-saving features that eliminate manual configuration of scans. The WebInspect 20.2.0 sensor detects when applications use modern frameworks such as Angular and React, and automatically adjusts its configuration to provide the best coverage.

Redundant Page Detection

Applications with lots of redundant content, such as content management systems and catalog sites, can cause unnecessarily long-running scans. With the WebInspect 20.2.0 sensor, you can use an advanced redundant page detection algorithm to reduce these scan times.

ADFS CBT Support

Per advice from Microsoft, many organizations are implementing a channel binding token(CBT) to secure Active Directory Federation Services (ADFS) authentication. The WebInspect 20.2.0 sensor now supports this extended protection mechanism. For more information, read the Help topic.

Learn More

For more information about the Micro Focus Fortify 20.2 release, visit these links:

- View the Fortify Technical Forum previewing this release.
- Fortify Unplugged YouTube Playlist for 20.2

Join the Fortify Community!

Join the Micro Focus Security community that provides customer-facing forums, educational webinar, product documentation and tutorials. Connect with peers, ask questions, search for solutions, share ideas, and collaborate over best practices in the Fortify Community today. Visit:
https://community.softwaregrp.com/t5/Fortify/ct-p/fortify

Documentation

You can find both html and pdf documentation for Fortify version 20.2.0 software products at:
https://www.microfocus.com/support-and-services/documentation/

Note: Legacy documentation (prior to 18.1) can still be found at:
https://community.softwaregrp.com/t5/Fortify-Product-Documentation/ct-p/fortify-product-documentation

Contact Support

For support, please visit https://softwaresupport.softwaregrp.com/.
Details are available in the attached release letter along with specific feature requirements. We hope that you continue to find out products helpful and we welcome any feedback. If you have any questions, please don’t hesitate to contact us.