opentext™ | Cybersecurity

Article

Fortify's Latest and Greatest

What's New in Fortify 23.1.0

May 2023

What's New in Fortify 23.1.0

General Availability—Fortify 23.1 Release

At Fortify by OpenText™, we believe great code is secure code and helping customers achieve it runs through everything we do. Fortify continues to cover the most critical use cases common to today's software landscape. From DevSecOps, Cloud Transformation, and Securing the Software Supply Chain, Fortify is the only AppSec solution recognized as a market leader by Gartner, Forrester, IDC and G2.

We are excited to announce the general availability of our Fortify 23.1.0 release! With enhanced offerings to increase speed, accuracy, scalability, and ease of use, this marks another important chapter in Fortify's elevation of code security. This release contains updates to Fortify Static Code Analyzer, Fortify WebInspect, Fortify Software Security Center, and Fortify Software Composition Analysis.

Some of the highlights of this release include:

- **.NET 7 and .NET 7 on Linux**—along with continued expansion of other languages and framework support.
- **Scan Policies**—Identify the most serious vulnerabilities at the most appropriate times with three policies to choose from: classic, security and devops.
- **Priority Override**—We now give customers the ability to modify the Fortify issue severity for more flexibility and customization.
- **Report Enhancements**—Implementation of high-demand report enhancements for better application security risk assessment.
- **ScanCentral SAST Improvements**—We have added numerous improvements for usability and functionality to ScanCentral SAST.
- **Automated 2FA with Authenticator Apps**—Have the ability to continue to scan, even in 2FA environments with WebInspect.
- **Client-Side Software Composition Analysis**—CVEs of client-side libraries, health data of open source projects and exportable CycloneDX SBOM are now available
- and so much more!

Fortify Software Security Center

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

FIPS-Inside Technology Preview

With this release, you can run Fortify Software Security Center functions in RHEL 8.5 and 9.0 FIPS-only-enabled environments. However, Kerberos SSO authentication is not supported. The support is subject to limitations of Red Hat OpenJDK 11 on the RHEL OS in FIPS mode. Since this has been released as a Technology Preview, please report any omissions, issues, or gaps in functionality so that we can address them prior to the next release.

Priority Override Signifiers in Reports

Changes to Fortify priority values (using the priority override feature) are now reflected in issue reports. For details, see "Viewing Priority Overrides Information in Issue Reports" in the Fortify Software Security Center User Guide, 23.1.0.

Fortify Insight

If you have purchased Fortify Insight, you can link your Fortify Software Security Center to your Fortify Insight dashboard by adding a Fortify Insight link to your SSC Dashboard.

Extended Search Capability for X.509 SSO Implementation

Previously, for an X.509 SSO implementation, Fortify Software Security Center searched the Subject field of the client certificate to retrieve the username for certificate authentication. The search now extends to include the Subject Alternative Name field.

Replacing SOAP fortifyclient with REST fortifyclient

In an effort to further secure your Fortify Software Security Center deployment, Fortify is phasing out SOAP fortifyclient and replacing it with REST fortifyclient. In this release, SOAP fortifyclient remains the default, but REST fortifyclient is available to you.

The file names for both utilities are the same, but the files are in different directories. The SOAP fortifyclient files are in <ssc_install_dir>/Tools/fortifyclient/bin and the REST fortifyclient files are in <ssc_install_dir>/Tools/fortifyclient-newrest/bin.

To improve security and prepare for the eventual deprecation of SOAP-based fortifyclient, Fortify strongly recommends disabling SOAP and testing the REST version of fortifyclient in your testing environment. Report any lack of parity or functionality as soon as possible.

For more information, see the Fortify Software Release Notes 23.1.0.

Job Queue Redesign
A new job execution strategy named "Flexible (technical preview)" is introduced in this release. Based on the conservative strategy, the flexible strategy makes more efficient use of job queue sensors. Users can switch between the new strategy and previous strategies, as needed.

Improved Event Log Filtering
Two new options enable you to refine the data displayed on the Event Logs page. You can now specify a username and / or an event type to filter the events that you view and export. To remove specified filters, click CLEAR.

Cloud Database Support
Fortify Software Security Center now supports SQL Server in both Azure and AWS cloud database services.

Windows Server 2022 Support
Fortify Software Security Center now supports running on the Windows Server 2022 operating system.

Kubernetes Support
- Support added for Kubernetes versions 1.25 and 1.26
- Support added for Kubernetes Persistent Volumes with optional support for Pod Security Context fsGroup option (fsGroup support is required for using a non-default container user ID)
- Support added for kubectl command-line tool version 1.24, 1.25, and 1.26. Fortify recommends the use of the same version of kubectl command-line tool as the Kubernetes cluster version
- Support added for version 3.10 and 3.11 of the Helm command-line tool

Fortify ScanCentral SAST

The following features have been added to Fortify ScanCentral SAST.

Specifying Fortify Static Code Analyzer Options and Properties as -targs and –sargs Arguments
ScanCentral now supports the options specified in -targs and -sargs that Fortify Static Code Analyzer allows, and ignores or blocks those that are not allowed.

Clients now accept rules, filters, and project templates—not only through the designated ScanCentral options, but also from the scan arguments parameter (-sargs). Previously, if specified, these options were ignored. For more information, see Appendix A: Fortify ScanCentral SAST Command-Line Options in the Fortify ScanCentral SAST Installation, Configuration, and Usage Guide.

New Status Command Option: --block-until
Previously, a ScanCentral client had no way to let you know if an FPR that you uploaded to Fortify Software Security Center was processed completely. Now, you can use the --block-until option to block additional actions from being performed until processing is complete, so that the merged results you later download include all of the audits, comments, suppressed issues, and history from the previous scans.

The new --block-until option for the STATUS command polls Fortify Software Security Center for the scan merge status, and then returns the following information:
- Job status
- SSC upload status
- SSC application version ID
- SSC application name
- SSC application version name
- SSC artifact ID
- SSC artifact status

Build Tools
- Added support for Maven version 3.9.x

Auto Detection of Build Tool for Remote Translation
Previously, to perform a remote translation, you had to supply the -bt (--build-tool) option with a value that specified the build tool. Now, Fortify ScanCentral SAST detects the build tool automatically based on the project files being scanned. For example, if Fortify ScanCentral SAST detects a pom.xml file, it automatically sets -bt to mvn. If it detects a build.gradle file, it sets -bt to gradle. If Fortify ScanCentral SAST detects a *.sln file, it sets -bt to msbuild and sets -bf to the xxx.sln file.

If ScanCentral detects multiple file types (for example, pom.xml and build.gradle), it prioritizes the build tool selection as follows: Maven > Gradle > MSBuild and prints a message to indicate which build tool type was selected based on the multiple file types found.

Note: If you specify the build tool manually, auto-detection is overridden.

Configurable Location for the worker-persist.properties File
For containerized deployments it is useful to determine where certain files are generated so that you can customize persistence. For example, the worker-persist.properties file and the job files are stored in the same folder (sensor working directory). Now, you can use two new properties to specify where the worker-persist.properties file is generated and where the job files are generated. This enables you to persist the worker-persist.properties file, which is needed to maintain sensor pool assignments, without having to keep all of the old Job files.

Fortify ScanCentral Controller and Sensor Docker Images and Helm Chart
ScanCentral Controller and Sensor Docker images are now available on Docker Hub. You must be a member of the fortifydocker organization to download the images. A Helm Chart is available at **https://github.com/fortify/helm3-charts**.

Windows Server 2022 Support
Fortify ScanCentral SAST now runs on the Windows Server 2022 operating system.

Fortify Static Code Analyzer

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

Features

- The Fortify Static Code Analyzer installation program no longer includes the Fortify Static Code Analyzer applications and tools. A separate installer is provided to install the Fortify Static Code Analyzer applications and tools.
- **Scan Policy**
  You can set a scan policy to identify the most serious vulnerabilities. There are three policies to choose from: classic, security, or devops. The classic scan policy is the default; it does not prioritize analysis results. The security scan policy is used to exclude issues related to code quality from the results. Use this policy to focus on remediation. The devops scan policy excludes issues that are also excluded by the security policy and reduces the number of lowpriority issues. Use this policy when speed is a priority and developers want to review results directly (without intermediate auditing).
- **Filter Files**
  You can now set an exclusion threshold value to a filter file by adding one of the following exclusion types: priority, impact, likelihood, confidence, probability, and accuracy.
- .NET analysis on Linux. You can now translate .NET code on Linux installations of Fortify Static Code Analyzer.

Platforms

- Red Hat Enterprise Linux 9.x
- macOS 13 on Intel and Apple Silicon (compatibility mode)

Compilers

- Clang 14.0.3
- gcc 11
- g++ 11
- swiftc 5.8

Build Tools

- Ant 1.10.13
- Gradle 8.0.2
- Maven 3.9.1
- SBuild 17.5 (Windows)
- Xcodebuild 14.2 and 14.3

Languages

- .NET 7
- Apex 56 and 57
- ASP.NET Core 7
- C# 11
- Dart 2.12–2.18 / Flutter 2.0–3.3. Rules for Dart/Flutter will be released in Q2 2023.
- ECMAScript 2022
- Go 1.18 and 1.19
- Kotlin 1.7
- PHP 8.2
- Python 3.10, 3.11
- TypeScript 4.6–4.9

Fortify Static Code Analyzer Tools

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

The Fortify Static Code Analyzer installer no longer includes the Fortify Static Code Analyzer applications and tools. A separate installer is included for installing the Fortify Static Code Analyzer applications and tools.

Platforms and Architectures

- Windows 11
- macOS 13. All tools run in compatibility mode on Apple M1 and M2 processors

Secure Code Plugins

Added support for updated versions of the following IDEs:

- Eclipse 2023-03
- IntelliJ IDEA 2023.1
- Android Studio 2022.1
- Visual Studio 2022, version 17.5

Fortify Extension for Visual Studio

The remediation phase now supports custom tags that require comments and the priority override tag.

New Report Template Versions

- PCI DSS 4.0
- PCI SSF 1.2
- DISA STIG 5.2

Fortify ScanCentral DAST

The following features have been added to ScanCentral DAST.

Client-Side Library Analysis

The hacker-level insights check has been enhanced to include information from the National Vulnerability Database (NVD) and Debricked health metrics when configured with a Debricked access token.

Key Stores

ScanCentral DAST now provides key stores as a way to create variables that you can use in scan settings, base settings, and macro parameters. When a scan is run, these variables are replaced with the latest values from the key store.

Artifacts Repositories

ScanCentral DAST now supports using artifacts repositories where scan artifacts reside. When a scan is run that references an artifact in a repository, either a tagged version or the latest copy of the artifact is pulled and used to configure and run the scan.

Private Data Settings

You can now configure private data settings that remove personally identifiable information from the scan and log data upon scan completion.

Scan Visualization Enhancements for API Scans

The site tree in scan visualization now includes icons for operations and parameters in API scans.

Postman Scan Enhancements

You can now import global variables files to use in Postman scans. There are also changes to validation and the ability to edit the sessions contained in collection files after validation.

Fortify WebInspect

The following features have been added to Fortify WebInspect.

Client-Side Library Analysis

The hacker-level insights check has been enhanced to include information from the National Vulnerability Database (NVD) and Debricked health metrics when configured with a Debricked access token.

Two-Factor Authentication

WebInspect has added the ability to automate Two-factor Authentication scans of sites using Authenticator Apps. This is in addition to our SMS- and email-based two-factor scanning. Onceconfigured, there is no need for user interaction.

SQLite SecureBase

WebInspect now uses a SQLite database for SecureBase. The file extension is nowSecureBase.db.

Support for Postman Global Variables

You can now import global variables files to use in Postman scans.

WebInspect REST API v2

The WebInspect REST API now includes a version 2, which includes asynchronous versions of endpoints that take a long time to complete. These endpoints generate a job token that you can use with the v2 Job endpoints to get the status and results from the job.

Enhanced Support of Localized SecureBase Content

A new Application Setting for SmartUpdate allows you to select a language to localize the security and report content in SecureBase.

Enhancements to False Positives
False Positives and ignored items have been renamed as Suppressed Findings in the UI. You can now export and import suppressed findings as JSON files.

Enhanced Support for Client Certificates
WebInspect now supports client certificates with strong private key (password) protection in Guided Scans, Basic Scans, and Interactive Scans.

Improved Scan Coverage and Performance
Fortify continues to enhance its engines to improve scan coverage and performance. WebInspect 23.1.0 provides a faster crawl and audit, and better application support with the Event-based Web Macro Recorder (formerly called Web Macro Recorder with Macro Engine 23.1.0).

WebInspect Software Requirements
Added support for Windows Server 2022, SQL Server 2022, and SQL Server Express 2022.

Contact Fortify by OpenText's Customer Support

If you have questions or comments about using this product, contact Fortify by OpenText's Customer Support using one of the following options.

To manage your support cases, acquire licenses, and manage your account: **www.microfocus.com/support**

For More Information
For more information about Fortify software products: **www.microfocus.com/solutions/application-security**

Connect with Us

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.