opentext™

Fortify Software

Document Release Date: December 2023

What's New in Fortify Software 23.2.0

December 2023

This release of Fortify Software includes the following new functions and features.

Fortify Software Security Center

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

Fortify Audit Assistant Gen 2

Audit Assistant is an optional tool that you can use to help determine whether or not the issues returned from your scans represent true vulnerabilities. Generation 2, or Gen 2, of Audit assistant is now available. Using advanced AI and machine learning, Gen 2 provides improved accuracy, training based on the decisions your auditors have made, and greater speed.

When upgrading Fortify Software to version 23.2.0, you must also upgrade Audit Assistant to use the new Gen 2 version of Audit Assistant.

BIGINT Data Type Replaces INT in scan_issue(ID) and issue(ID) Fields

This change affects the scan_issue table in both MSSQL and MySQL databases. During database migration, the data type for scan_issue(ID) and issue(ID) will be changed to BIGINT if it has not already been done. For information on how this impacts your database migration, see "Preparing to Upgrade the Fortify Software Security Center Database" in the *OpenText™ Fortify Software Security Center User Guide*.

Debricked SBOM Support

You can now download Debricked Software Bill Of Materials and view information on the third-party components in your application.

Base URL Attribute

You can now assign a base URL attribute via the SCANCENTRAL DAST ATTRIBUTES page.

New Automation Token

Fortify Software Security Center now has a new SSC API Token type: the AutomationToken. This token type is a duplicate of the UnifiedLoginToken type. It provides access to most of the REST API and is intended for use in long-running automations and can be configured to last up to a year.

Preserve Issue Detected on Date Across Versions

Now, when creating a new application version based on a previous version, the **Detected on** date will be carried over to the new version. Previously, the **Detected on** date was set to the current date when basing a new application version on a previous one.

Change User Assigned to an Issue

You can now change the user assigned to an issue.

Custom Banner

An administrator can create an informational banner that persists until removed or changed.

New Reports

The premium report bundle now includes two new issue reports:

- OWASP API Top 10 (2023)
- CWE Top 25 (2023)

The following report versions are no longer available in this release:

- SANS 2009/2010
- STIG 4.10, 4.9 and below
- OWASP < 2013
- CWE Top 25 2019/2020
- WASC 24 + 2

REST Fortify Client

The REST fortifyclient replaces the SOAP fortifyclient and is now the default.

Additions to the System Requirements

Fortify Software Security Center Database

- SQL Server 2022

Service Integrations

- Jira 9.10

Software Requirements

- Red Hat Enterprise Linux 9 (RHEL 9) support
- Kubernetes 1.27 and 1.28 support
- Helm 3.12 support

BIRT Reporting

- BIRT Report Designer 4.13.0

Fortify ScanCentral SAST

The following features have been added to Fortify ScanCentral SAST.

- Support for ScanCentral SAST .NET scanning and packaging on Linux systems
- Support for remote translation and scan of COBOL projects
- ScanCentral SAST will now retry any failed uploads to Fortify Software Security Center. Use the new upload command to resend an FPR file to Fortify Software Security Center after a previous upload attempt failed.
- REST API documentation for the Fortify ScanCentral SAST Controller is available with Swagger UI
- You can now package the debug logs from clients, sensors, and Fortify Static Code Analyzer into a ZIP archive using the start command option `-diagnosis`.
- Offload translation and scan support with Gradle versions 7.4-8.3 and MSBuild versions 17.4 - 17.8

Fortify Static Code Analyzer

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

Build tools

- Ant 1.10.14
- Gradle 8.1 and 8.3
- Maven 3.9.4
- MSBuild 17.6 - 17.8
- xcodebuild 15 and 15.0.1

Languages

- Angular 15.1, 15.2, 16.0
- Apex 58
- Bicep v0.12.x → current
  - 0.12.1 → 0.14.85 (supporting .NET 6)
  - 0.15.31 → current (supporting .NET 7)
- C# 12
- C17
- Dart 3.0
- ECMAScript 2023
- Go 1.20
- Kotlin 1.8
- .NET 8.0
- Python 3.12
  - Django up to 4.2
- React 18.0
- Solidity 0.4.12-0.8.21
- Swift 5.9
- TypeScript 5.0

Compilers

- Clang 15.0.0
- Swiftc 5.9

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.

Fortify Audit Workbench

- Syntax source code highlighting for Terraform, Dart, Bicep, and Solidity.
- Installation automatically detects the Fortify Static Code Analyzer versions installed in a default location.
- By default, Fortify Audit Workbench does not display binary source code

Secure Coding Plugins

• Fortify Plugin for Eclipse adds support for 2023-06 and 2023.06

• Fortify Analysis Plugin for IntelliJ IDEA and Android Studio adds support for IntelliJ IDEA 2023.2 and Android Studio 2022.2 and 2022.3

New Report Versions

OWASP MASVS 2.0

CWE Top 25 2023

OWASP API Top 10 2023

Fortify ScanCentral DAST

The following features have been added to ScanCentral DAST

Fortify Connect

The new Fortify Connect feature enables you to perform scans of private applications from the cloud without exposing the application through your firewall.

Event-based Logout Conditions

The Event-based Web Macro Recorder now supports the use of JavaScript during execution to detect and notify the Fortify WebInspect sensor of logout.

Event Handlers

The Event-based Web Macro Recorder now supports event handlers that react to unpredictable events, such as dialogs opening and popup DOM elements that steal focus.

Web Storage Keys

The Event-based Web Macro Recorder now supports the use of web storage keys that enable the application to determine and maintain state.

Support for IMAP in Two-factor Authentication Scans

Two-factor authentication scanning now supports IMAP email servers.

Fortify WebInspect

The following features have been added to Fortify WebInspect.

Fortify License and Infrastructure Manager

Linux Version

A Linux version of the Fortify License and Infrastructure Manager (LIM) is now available for download from the Fortify Docker repository.

Event-based Logout Conditions

The Event-based Web Macro Recorder now supports the use of JavaScript during execution to detect and notify the Fortify WebInspect sensor of logout.

Event Handlers

The Event-based Web Macro Recorder now supports event handlers that react to unpredictable events, such as dialogs opening and popup DOM elements that steal focus.

Web Storage Keys

The Event-based Web Macro Recorder now supports the use of web storage keys that enable the application to determine and maintain state.

Web Socket Events

WebInspect now includes a Capture Web Socket Events setting in the JavaScript dialog under Scan Settings.

Support for IMAP in Two-factor Authentication Scans

Two-factor authentication scanning now supports IMAP email servers.

Contacting Customer Support

Visit the Support website to:

- Manage licenses and entitlements
- Create and manage technical assistance requests
- Browse documentation and knowledge articles
- Download software
- Explore the Community

https://www.microfocus.com/support

We Welcome Your Feedback

If you have comments or suggestions about the documentation, you can send these to the documentation team at fortifydocteam@opentext.com. Please use the subject line “Feedback on <Document_Title> <Product_Version>.” We appreciate your feedback!

What’s New in Fortify Software 23.1.0

May 2023

This release of Fortify Software includes the following new functions and features.

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-new-rest/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 low-priority 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
- MSBuild 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. Once configured, there is no need for user interaction.

SQLite SecureBase

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

What's New in Micro Focus Fortify Software 22.2.0

November 2022

This release of Micro Focus Fortify Software includes the following new functions and features.

Micro Focus Fortify Software Security Center

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

Priority Override Capability

Administrators can now enable users to change, or override the priority values assigned to issues. With the introduction of priority override capability, the **Engine Priority** option was added to the **Group by** menu. This grouping selection returns issues based on the original priority value assigned by the engine that identified the issue.

Prioritizing ScanCentral SAST Jobs

In this release, you can move a pending scan request to the first position in the jobs queue from the SCANCENTRAL SAST tab. For details, see "Prioritizing a ScanCentral SAST Scan Request" in the user guide.

Support for Tomcat Access log Pattern for Kubernetes Deployments

Fortify Software Security Center now supports changing the Tomcat access log pattern for a Kubernetes deployment. For details, see "Configuring the Apache Tomcat Access Logs for Additional Fields on the Docker Image" in the user guide.

ScanCentral SAST Tab Enhancements

The following changes were made to the SAST tab in the SCANCENTRAL view:

- The **Status** column is now the **State** column, which now displays symbols to indicate the current scan state.
- The Scan Requests table now includes the **Priority** column, which shows the order in which pending scan requests jobs are to be run. You can sort the listed jobs by selecting the

Priority heading. The details for an expanded scan request now include the **PRIORITIZE SCAN** button, which you can select to move the scan request to the top of the job queue for the pool. You can also click the arrow icon in the Scan Requests table to move the request to the top of the queue. For details, see "Prioritizing a ScanCentral SAST Scan Request" in the user guide.

Viewing and Auditing Debricked Vulnerability Results

You can now view and audit Debricked scan results for applications in Fortify Software Security Center so that, in addition to seeing vulnerabilities in the source code, you can also view the open-source vulnerabilities from third-party libraries. For details, see "Viewing Open Source Data" in the user guide.

Creating Clickable Links in Bug Tracking Templates

As of release 22.1.1, you can use the new `HtmlUtil` class in the velocity templates for bug trackers to create a link to a specific issue in Fortify Software Security Center. For information about how to use this class, select the **Editing tips** link in the EDIT TEMPLATE dialog box (see "Customizing Velocity Templates for Bug Tracker Plugins" in the user guide).

Changes to the About Fortify Software Security Center Box

The **Configuration** section of the ADMINISTRATION view now includes the About page, from which you configure the SUPPORT link in the About box. For information about how to change the SUPPORT link, see "Customizing the Fortify Software Security Center About Box" in the user guide.

Changes to SAML SSO Configuration

The procedure used to configure Fortify Software Security Center to work with SAML SSO has changed (see "Configuring Fortify Software Security Center to Work with SAML 2.0-Compliant Single Sign-On Solutions" in the user guide)

Preventing LDAP Refresh on Startup / Enabling Persisted Cached LDAP Data

Previously, the LDAP data resided in in-memory cache and was lost at server shutdown. Now, you can enable the cached data to persist after shutdown, so that restarting Fortify Software Security Center is much faster, especially for large LDAP environments. For more information, see "Enabling Persistence of the LDAP Cache" in the user guide.

Updated Kubernetes Support

- Support for Kubernetes 1.23 and 1.24
- Support for Helm 3.9

Micro Focus Fortify ScanCentral SAST

The following features have been added to Fortify ScanCentral SAST.

Support for Packaging Java 8 Projects

If you have a Java 8 project that fails to build because ScanCentral SAST requires Java 11 to run, you can set the new `SCANCENTRAL_JAVA_HOME` environment variable to point Java 11. After you do, ScanCentral SAST runs correctly, and the build runs successfully with `JAVA_HOME` set to `Java 8` for the project build.

Upgrade of the Internal H2 Database Engine

The internal H2 database for Fortify ScanCentral SAST was upgraded. As a result, you must run an associated migration script. For details, see "Upgrading the ScanCentral SAST Controller" in the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

Improved Method for Excluding Files From Scans When Using ScanCentral SAST to Package Projects

Previously, Gradle, Maven, and MSBuild integration relied on internal build procedure logic to collect files. The only way to exclude files was either to exclude them from the build file, or use an additional translation argument (`-targs"-exclude...,"`), which required that you knew where the file was to be saved in the ScanCentral SAST working directory.

You can now use the `-exclude` option directly from the ScanCentral SAST command line to exclude some files from scans for the Maven, Gradle, MSBuild build tools, and for `-bt none`. For details see "Package Command" in the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

Configuring the Name of FPR Files Uploaded to *Fortify Software Security Center*

The FPR files uploaded to Fortify Software Security Center are named scan.fpr. You can now use the -fprssc option specify the name to use for generated FPR files uploaded to Fortify Software Security Center. For details, see "Submitting Scan Requests and Uploading Results to Fortify Software Security Center" in the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

Packaging Projects with File Paths that Contain an Umlaut

Previously, packaging failed if a file name or file path for a project included an umlaut character. Now, you can prevent such failures by adding a new property to the fortify-sca.properties file. For details, see the cautionary note in "Package Command" in the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

Configuring a Proxy for ScanCentral SAST Clients

If your outbound traffic must go through a proxy, you can now add a proxy configuration for that purpose. For details, see "Configuring Proxies for Fortify ScanCentral SAST Clients " in the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

(Fortify on Demand only) New Option for Packaging Files for Debricked

The new -oss packaging option enables you to package additional files that Debricked requires for its scans. See "Package Command" in the *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.

Micro Focus Fortify Static Code Analyzer

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

Operating System Updates

Fortify added support for the following operating systems and versions:

- macOS 12 Apple silicon
- Ubuntu 22.04.1 LTS

Compiler Updates

Fortify added support for the following compiler versions:

- Clang 14.0.0
- Swiftc 5.7

Build Tool Updates

Fortify added support for the following build tool versions:

- Xcodebuild 14 and 14.0.1

Language and Framework Updates

- COBOL
  IBM Enterprise COBOL for zOS 6.2 and 6.3
  Micro Focus Visual COBOL 7.0 and 8.0
- Apex 55
- Kotlin 1.6
- PHP 8.1
- TypeScript / JavaScript
  React 17.0
  React Native .68
  Vue 2

Note: Rules for Vue 2 will be part of the Fortify Software Security Content 2022 R4 release.

Micro Focus Fortify Static Code Analyzer Tools

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

Fortify Analysis Plugin for IntelliJ and Android Studio

The Fortify Analysis Plugin for IntelliJ IDEA and Android Studio now supports:

- IntelliJ 2022.2
- Android Studio 2021.3

Eclipse Support

The Fortify Eclipse Complete Plugin now supports Eclipse 2022-06 and 2022-09.

Updated CWE Top 2022 Report

Updated to incorporate content from the Fortify Software Security Content 2022 Update 3.

Updated Custom Rules Editor

Includes the following generic and category-specific templates for generating custom Configuration, Regex, and Infrastructure as Code (IaC) rules:

- `Configuration Rule for PropertyMatch`
- `Configuration Rule for XPathMatch`
- `Docker Bad Practices: Untrusted Base Image in Use`
- `Credential Management: Hardcoded API Credential`

- Regex Rule for ContentRegex
- Regex Rule for FileNameRegex
- Regex Rule for FileNameRegex and ContentRegex
- Structural Rule for Cloud Configuration in Nested Objects
- Structural Rule for Cloud Configuration in Single Object
- Structural Rule for Terraform Configuration in Nested Blocks
- Structural Rule for Terraform Configuration in Single Block
- Terraform Bad Practices: Untrusted Module in Use

Additional language support:

- Apex
- Go
- HCL
- JavaScript/TypeScript
- JSON
- Kotlin
- PHP
- Python
- YAML

Additional configuration file type support:

- configuration
- docker
- xml

Micro Focus Fortify ScanCentral DAST

The following features have been added to Fortify ScanCentral DAST

GraphQL Native Support

ScanCentral DAST now supports scanning GraphQL natively. A Postman collection or workflow is no longer required to get a comprehensive GraphQL scan.

gRPC Scanning

ScanCentral DAST has added support for gRPC scanning. This popular server-to-server framework can now be scanned for security vulnerabilities.

SOAP Service Scanning

ScanCentral DAST now supports scanning SOAP services.

Engine 7.1 Updates

Fortify continues to enhance its engines to improve scan coverage and performance. ScanCentral DAST 22.2.0 provides a faster crawl and audit and better application support from the Web Macro Recorder with Macro Engine 7.1.

Linux Version

The ScanCentral DAST core components and sensor are now available on a lightweight Linux container. This new Linux option provides enhanced support for automation and sensor auto scaling.

Sensor Auto Scaling

ScanCentral DAST provides optional sensor auto scaling in Kubernetes that automatically starts the sensor container, runs the scan, and shuts down the container upon completion.

Micro Focus Fortify WebInspect

The following features have been added to Fortify WebInspect.

GraphQL Native Support

WebInspect now supports scanning GraphQL natively. A Postman collection or workflow is no longer required to get a comprehensive GraphQL scan.

gRPC Scanning

WebInspect has added support for gRPC scanning. This popular server-to-server framework can now be scanned for security vulnerabilities.

Engine 7.1 Updates

Fortify continues to enhance its engines to improve scan coverage and performance. WebInspect 22.2.0 provides a faster crawl and audit, and better application support from the Web Macro Recorder with Macro Engine 7.1.

Linux Version

WebInspect is now available on a lightweight Linux container. This containerized version of WebInspect is a great option for automation scenarios when WebInspect is used through its API.

Updated SOAP Scanning

WebInspect will be deprecating its older SOAP scanning option through the Web Service Test Designer tool. In preparation, a new mechanism to scan SOAP applications is available through the API scanning option.

opentext™

What's New in Micro Focus Fortify Software 22.1.0

June 2022

This release of Micro Focus Fortify Software includes the following new functions and features.

Micro Focus Fortify Software Security Center

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

Issue Correlation Details

If you have correlated issues in an application version, you can use the heading for the correlated issues icon (⇄) to sort listed issues based on whether or not they are correlated with other issues (see "Viewing Correlated Issues on the AUDIT Page" in the *Fortify Software Security Center User Guide*). You can also selectively list the issues with which a given issue is correlated (see "Auditing Correlated Issues" in the *Fortify Software Security Center User Guide*).

Targeted Rulepack Downloads

Previously, Fortify Software Security Center ignored the clientType parameter in Rulepack update requests. As a result, Rulepack clients received all Rulepacks available (both Fortify Static Code Analyzer and Fortify Security Assistant Rulepacks). Now, Fortify Software Security Center takes the clientType parameter into account for Rulepack update requests. For details, see "Updating Rulepacks from the Micro Focus Fortify Update Server" in the *Fortify Software Security Center User Guide*.

Updated Processing Rule: Ignore SCA Scans Performed in Quick Scan Mode

The processing rule for ignoring Fortify Static Code Analyzer scans performed in quick scan mode now also prevents the upload of Fortify Static Code Analyzer speed dial results performed with a setting of less than four. For details, see "Setting Analysis Results Processing Rules for Application Versions" in the *Fortify Software Security Center User Guide*.

Report Maintenance: New "Days to Preserve" Option

On the Scheduler page, the **Days to preserve** option was added in a new **Reports maintenance** section. This option enables you to specify the number of days Fortify Software Security Center retains generated reports. For more information, see "Configuring Job Scheduler Settings in the *Fortify Software Security Center User Guide*.

Pausing Job Execution

You can now control job execution by pausing (and then resuming) it using the **Pause job execution** option located on the Maintenance page (**ADMINISTRATION > Maintenance**). After you pause job execution, jobs (artifact processing, report generation, data export requests, and so on) that are currently running continue to completion. Any new jobs submitted are queued for processing once the **Pause job execution** check box is cleared and normal processing resumes. For more detail, see "Pausing and Resuming Job Execution" in the *Fortify Software Security Center User Guide*.

Requiring Comments for Specific Custom Tag Values

Administrators can now require comments for custom tags. When the "Require Comments" setting is checked, any changes to the custom tag will cause an additional comment box to appear for the custom tag and the Save button will be disabled until a comment is entered. For details, see "Adding Custom Tags to the System" in the *Fortify Software Security Center User Guide*.

Expanded Issue Counts

Previously, you could display 20, 50, or 100 issues at a time on the AUDIT page. Now, you can display up to 150 or 200 issues per page.

Kubernetes Updates

- Added support for Kubernetes 1.22
- Added support for Helm 3.8

Micro Focus Fortify ScanCentral SAST

The following features have been added to Fortify ScanCentral SAST.

Kotlin for Android Support

You can now use the ScanCentral Client to package Kotlin for Android projects for remote translation using Gradle integration (`-bt gradle`).

New Command to Update ScanCentral Client

Using the new `update` command, you can update ScanCentral Client to the latest version on the ScanCentral Controller.

Get SSC Artifact Processing State Using Job Token

Using the `status` command, ScanCentral Client can retrieve the processing state of a job that uploaded the FPR to SSC.

Build Tool Updates

• Gradle 7.3

• MSBuild 14.0, 17.0, 17.1, and 17.2

Support for Multiple Client Versions on the Controller for Auto-Update

The Auto-Update feature now supports multiple versions of clients. Sensors and embedded clients will be updated by the versions available in the Controller, rather than the version of the Controller.

Micro Focus Fortify Static Code Analyzer

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

Operating System Updates

Fortify added support for the following operating systems and versions:

- macOS 12
- Windows 11

Compiler Updates

Fortify added support for the following compiler versions:

- Clang 13.1.6

- OpenJDK javac 17
- Swiftc 5.6
- cl (MSVC) 2015 and 2022

Build Tool Updates

Fortify added support for the following build tool versions:

- Gradle 7.4.x
- MSBuild 14.0, 17.0, 17.1 and 17.2
- Xcodebuild 13.3 and 13.3.1

Language and Framework Updates

- C# 10
- .NET 6.0
- C/C++ 20
- HCL 2.0
- Java 17
- TypeScript 4.4 and 4.5

Note: Rules for Terraform and Google Cloud Platform will be part of the Fortify Software Security Content 2022 R2 release.

Micro Focus Fortify Static Code Analyzer Tools

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

Visual Studio 2022 Support

The Fortify Extension for Visual Studio now supports Visual Studio 2022.

IntelliJ 2021.x Support

The Fortify Analysis Plugin for IntelliJ now supports IntelliJ 2021.x to 2021.3.

Import Standard Fortify Rulepacks from Filesystem

Use the **Options** menu in Fortify Audit Workbench, Fortify Eclipse Complete Plugin, and Fortify Extension for Visual Studio to import Fortify Rulepacks downloaded from the Customer Portal.

Compare LOC of Scanned Files Between Two FPRs

View LOC counts of analyzed files in an FPR (`-loc`) or compare LOC counts between two FPRs using FPRUtility (`-loc, -compareTo`).

Configurable Timeout for fortifyupdate

Configure the socket timeout for fortifyupdate using the `rulepackupdate.SocketReadTimeoutSeconds` property in the `server.properties` file. The default value is `180`.

New Search Modifier: shortfilename

In Fortify Audit Workbench and the Fortify Plugins for Eclipse, you can use `shortfilename` as a search modifier in Issue Templates to filter or hide issues that match the file name. For full path matches, continue to use the `file` search modifier.

New OWASP Top 10 2021 Report

Generate new OWASP Top 10 Report (2021) from the following tools:

- Fortify Audit Workbench
- Fortify Extension for Visual Studio
- Fortify Remediation Plugin for Eclipse
- BIRTReportGenerator

Micro Focus Fortify ScanCentral DAST

The following features have been added to Fortify ScanCentral DAST

User Configuration Restrictions

- New permissions allow you to bar scanning of specific domains or IP addresses.
- New Modify User permission required to allow user to modify a scan. A user who does not have this permission can only configure a scan URL, login macro, workflow macros, and network credentials. With this limited role, users can start scans, create scans from base settings, and view settings but not change them.

PostgresSQL Support

- Support for use of a PostgresSQL database.

Scan Import

- Import Scans into ScanCentral PostgresSQL database from Fortify WebInspect or Fortify WebInspect Enterprise.

Automated Deployment (Infrastructure as Code)

- Support for the fully automated deployment of ScanCentral DAST.

Rescan Button

- The Rescan button allows you to rescan and existing scan.

Micro Focus Fortify WebInspect

The following features have been added to Fortify WebInspect.

Support for HAR Files

Scanning with workflow macros ensures that important content is covered in a scan. WebInspect can now use HAR files for workflow scanning.

Out-of-Band Testing

WebInspect can now test for a new class of vulnerabilities called Out-of-Band or OAST vulnerabilities. Using the public Fortify OAST server, WebInspect can detect OAST vulnerabilities such as Log4Shell.

Engine 7.0 Updates

Fortify continues to enhance its engines to improve scan coverage and performance. WebInspect 22.1.0 provides a faster crawl and audit, and better application support from the Web Macro Recorder with Macro Engine 7.0.

MS SQL AD Authentication Support

WebInspect 22.1.0 can now use a MS SQL Database using AD Authentication.

Windows 11 Support

WebInspect 22.1.0 is now supported on the Windows 11 operating system.

Azure SQL Database Support

WebInspect 22.1.0 can now use an Azure SQL Database for storing scan data.

Sensor Support for Fortify WebInspect Enterprise 21.2.0

WebInspect 22.1.0 can be configured as a sensor for Fortify WebInspect 21.2.0.