Micro Focus Fortify Software v20.2.0

Release Notes

Document Release Date: November 2020 (updated 3/2/2021)
Software Release Date: November 2020

IN THIS RELEASE

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 20.2.0 of the Fortify product suite.

This information is not available elsewhere in the product documentation. For information on new features in this release, see What's New in Micro Focus Fortify Software 20.2.0, which is downloadable from the Micro Focus Product Documentation website:

https://www.microfocus.com/support/documentation.

FORTIFY DOCUMENTATION UPDATES3/2

- The *Micro Focus Fortify ScanCentral Installation, Configuration, and Usage Guide* has been renamed *Micro Focus Fortify ScanCentral SAST Installation, Configuration, and Usage Guide*.
- The *Micro Focus Fortify Plugins for JetBrains IDEs User Guide* has been renamed *Micro Focus Fortify Plugins for JetBrains IDEs and Android Studio User Guide*.
- A new guide, the *Micro Focus Fortify ScanCentral DAST Configuration and Usage Guide* is now available.
- The *Micro Focus Fortify Static Code Analyzer User Guide* requires the following changes to Chapter 14: Translating COBOL Code:
    - In the "Preparing COBOL Source and Copybook Files for Translation" section, the following sentences should be deleted: Fortify Static Code Analyzer processes only top-level COBOL sources. Do not include copybook files in the directory or the subdirectory where the COBOL sources reside.
    - In the "Translating COBOL Source Files Without File Extensions" section, the property name is incorrect. The correct option in the example should be: -Dcom.fortify.sca.fileextensions.xyz=COBOL

Accessing Fortify Documentation

The Fortify Software documentation set contains installation, user, and deployment guides. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest HTML or PDF versions of these documents from the Micro Focus Product Documentation website:

https://www.microfocus.com/support/documentation.

If you have trouble accessing our documentation, please contact Fortify Customer Support.

Note: Documentation prior to the 18.10 release is available on the Micro Focus Community (formerly Protect724) website: https://community.microfocus.com/t5/Fortify-Product-Documentation/ct-p/fortify-product-documentation.

INSTALLATION AND UPGRADE NOTES

Complete instructions for installing Fortify Software products are provided in the documentation for each product.

Updating Security Content after a Fortify Software Security Center Upgrade

If you have upgraded your Fortify Software Security Center instance but you do not have the latest security content (Rulepacks and external metadata), some generated reports (related to 2011 CWE) might fail to produce accurate results. To solve this issue, update the security content. For instructions, see the *Micro Focus Fortify Software Security Center User Guide*.

USAGE NOTES FOR THIS RELEASE

There is a landing page (https://fortify.github.io/) for our consolidated (Fortify on Demand + Fortify On-Premise) GitHub repository. It contains links to engineering documentation and the code to several projects, including a parser sample, our plugin framework, and our JavaScript Sandbox Project.

Fortify Static Code Analyzer

- Structural results - Most structural issues will show new instance IDs. The algorithm that computes instance IDs for structural issues now produces more variance than previous IDs that often differed only in the final digit.
- COBOL: If you plan to scan COBOL on a Windows system via automation, update the group policy so that Error Reporting does not require user intervention when an error occurs.
    - Click the Windows **Start** button.

    - Type `gpedit.msc`
    - Navigate to `Computer Configuration->Administrative Templates->Windows Components->Windows Error Reporting`
    - In the right pane, click on `Prevent display of the user interface for critical errors` and set it to **Enabled**.
- ABAP
    - The ABAP Extractor includes a new option to export SAP standard code in addition to custom code. The Micro Focus Fortify Static Code Analyzer User Guide will be updated to include this information in a future update.
    - If you have an issue installing the ABAP Extractor, contact Customer Support and request a newer version.
- Kotlin
    - If you have Java code in your project that references Kotlin source, Kotlin functions called in Java are only resolved if the parameters and return types are built-in types or types defined in the same file as the called function definition.

Fortify Software Security Center

- REST API endpoint `/api/v1/localUsers/{id}` change: PUT method must contain up to date `objectVersion` value retrieved by a preceding GET request to the endpoint. An outdated, missing, or incorrect `objectVersion` value will cause a failure of the PUT request to protect `LocalUser` object consistency. POST and DELETE requests are not affected by the change. Note: This was incorrectly included in the *Micro Focus Fortify Software Release Notes v20.1.0*.
- The MariaDB JDBC driver, which is now used as the JDBC driver for MySQL database server, is bundled with the `ssc.war` file (`<ssc.war>/WEB-INF/libs`). In some cases the MariaDB driver uses different JDBC URL parameters.

  Note: Fortify Software Security Center does not support MariaDB as a backend database. The `connectionCollation=<collation_name>` parameter must be replaced with `sessionVariables=collation_connection=<collation_name>`. The `rewriteBatchedStatements=true` parameter is still supported. Any additional custom JDBC URL parameters must use syntax compatible with the MariaDB driver. If you are automating an SSC deployment and configuration, please be sure to update your auto-configuration file. Use the correct syntax to specify the jdbc.url property as described above and set the value of the `db.driver.class` property to `org.mariadb.jdbc.Driver`.

- HTTP Basic authentication is deprecated for all REST API endpoints except for `/api/v1/tokens/*, /api/v1/auth/*` and `/api/v1/license`.
- Token-related REST endpoints (`/api/v1/tokens/*`) are only available via HTTP Basic Authentication and disallowed when using Token authentication. Analogously, access to the legacy SOAP `InvalidateTokenRequest` and `GetAuthenticationTokenRequest` has been removed from all the default token

types. Although these requests can still be granted in a custom token definition, such use is deprecated and access via token authentication will be explicitly denied in the future. Token creation/deletion functionality is only available when authenticated to SSC via HTTP Basic Authentication or the SSC Admin UI.
- When integrating WebInspect Enterprise / ScanCentral DAST / AWB or other Fortify Tools to work with SSC, clock skew must be minimized between the different communicating machines (suggested: less than 5 minutes, compared on UTC basis). Requests to SSC can fail if there is excessive clock skew.
- Since 20.1.0, the unused `copyCurrentStateFpr` flag has been removed from the payloads of `/projectVersions/action/copyFromPartial` and `/projectVersions/action/copyCurrentState` endpoints. The flag caused confusion since it was ignored in the former endpoint and redundant in the latter. We recommend that you remove this flag from any scripts calling these endpoints.
- Use the new `ScanCentralCtrlToken` token type instead of `CloudCtrlToken`. The `CloudCtrlToken` token type will be removed in the next release.
- Due to a limitation in the way the ScanCentral SAST client currently collects files for remote translation of ASP.NET code, Fortify recommends that you run local translations and remote scans via ScanCentral SAST for ASP.NET projects.

Fortify WebInspect

- **ScanCentral DAST**: When running a Fortify ScanCentral DAST sensor outside of a container, such as a sensor service on the same machine as a Fortify WebInspect installation, you must install the ASP.NET Core Runtime 3.1.x (Hosting Bundle) as a prerequisite.
- **LIM on Docker Requirements**: The LIM on Docker container runs on and works with the following software packages:
    - Windows 10 Pro
    - Windows Server 2019
    - Docker 18.09 or later

KNOWN ISSUES

The following are known problems and limitations in Fortify Software 20.2.0. The problems are grouped according to the product area affected.

Fortify Software Security Center

This release has the following issues:

- When servlet session persistence is enabled in Tomcat, a "class invalid for deserialization" exception may be thrown during Tomcat startup. It is caused by

significant changes in the classes where instances can be stored in HTTP sessions. This exception can be ignored.
- When servlet session persistence is enabled in Tomcat and SSC is started in maintenance mode, the seeding step may fail with "Unable to load seed context" error. To recover from the error, SSC must be restarted.
- You cannot enable "Enhanced security, security manager" for BIRT reports if your Fortify Software Security Center is installed on a Windows system.
- In the ScanCentral SAST CLI, use the '/switch' form instead of '-switch' for the '-bc (--build-command)' option when using 'msbuild' for the '-bt (--build-tool)' option.

Fortify Static Code Analyzer

This release has the following issues:

- Due to major improvements in our scanning capabilities for Go, Kotlin and Python, some issues will be assigned a new Instance ID and marked as New. The previous finding will be marked as removed.
- Visual Studio 2019 update 16.7 and later brings .NET Core SDK 3.1.403, which is not yet supported by Fortify Static Code Analyzer and can result in translation issues. As a workaround, Fortify recommends you downgrade the .NET Core SDK to version 3.1.109 (the latest version that Fortify Static Code Analyzer currently supports).
- There might be issues in picking up dockerfiles that are named dockerfile. As a workaround, specifically mention them in the translation command. This issue will be fixed in an upcoming patch

Fortify Audit Workbench, Secure Code Plugins, and Extensions

This release has the following issues:

- To launch the installer on MacOS Catalina (10.15), open the location in Finder and Control+click the app to invoke a context shortcut menu and select Open. A dialog appears providing three options, one of which is Open. You can run it even in the absence of notarization. More details are available in this support article: https://support.apple.com/en-us/HT202491
- Security Assistant for Eclipse requires an Internet connection for the first use. If you do not have an Internet connection, you will get an "Updating Security Content" error unless you copied the rules manually.
- On MacOS Catalina (10.15), if you point the installer to a copy of the `fortify.license` on the desktop, it will fail to copy it. Put the `fortify.license` file in a folder that the application has permissions, such as your user Home folder.
- ScanWizard generates incorrect command line options for ScanCentral invocation when upload to SSC is enabled. The generated script contains `-project` and `-versionname` options instead of `-application` and `-version` respectively. To

make ScanCentral upload results correctly to the Application Version, you need to replace following line

```
%SCANCENTRAL_CLI% -sscurl %SSCURL% -ssctoken %SSCTOKEN%
start -upload  -uptoken %SSCTOKEN% -project %SSCPROJECT% -
versionname %SSCVERSION% -b %BUILDID% -scan
```

with

```
%SCANCENTRAL_CLI% -sscurl %SSCURL% -ssctoken %SSCTOKEN%
start -upload  -uptoken %SSCTOKEN% -
application %SSCPROJECT% -version %SSCVERSION% -b %BUILDID%
-scan
```

- On MacOS, there is a known issue when running the BIRTReportGenerator from the console. Please use AuditWorkbench to generate reports.

NOTICES OF PLANNED CHANGES

Fortify Static Code Analyzer

- Support for running FindBugs from Fortify Static Code Analyzer will be removed in the next release.

Note: For a list of technologies that will not be supported in the next release, please see the "Technologies to Lose Support in the Next Release" topic in the *Micro Focus Fortify Software System Requirements* document.

FEATURES NOT SUPPORTED IN THIS RELEASE

- Incremental Analysis in Fortify Static Code Analyzer is no longer supported.
- The following reports have been removed in Fortify Software Security Center: DISA STIG 3.x, SSA Application, and SSA Portfolio.
- DISA STIG 3.x mappings have been removed. This means the attributes associated with DISA STIG 3.x are no longer displayed in the Group By and Filter By lists on the Audit page in Fortify Software Security Center.

WebInspect

Support for Selenium IDE has been deprecated in WebInspect. However, Selenium WebDriver is still supported. Ignore content related to Selenium IDE in the WebInspect documentation.

WebInspect Enterprise

Support for Selenium IDE has been deprecated in WebInspect Enterprise. Ignore content related to Selenium IDE in the WebInspect Enterprise documentation.

Note: For a list of technologies that are no longer supported in this release, please see the "Technologies no Longer Supported in this Release" topic in the *Micro Focus Fortify Software System Requirements* document.

SUPPORT

If you have questions or comments about using this product, contact Micro Focus Fortify Customer Support using the following option.

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account: https://www.microfocus.com/support.

LEGAL NOTICES

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.