Micro Focus Fortify Software v20.1.0

Release Notes
Document Release Date: July28, 2020
Software Release Date: May 2020

IN THIS RELEASE

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 20.1.0 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 20.1.0, which is downloadable from the Micro Focus Product Documentation website:

https://www.microfocus.com/support-and-services/documentation.

FORTIFY DOCUMENTATION UPDATES

The *Micro Focus Fortify Plugins for IntelliJ, WebStorm, and Android Studio User Guide* has been renamed *Micro Focus Fortify Plugins for JetBrains IDEs User Guide.*

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-and-services/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.softwaregrp.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

- Kotlin programming language support - Fortify Static Code Analyzer support for scanning Kotlin is available as a Technical Preview. However, use of this feature requires the June 2020 security content (or later) and installation of the Fortify Static Code Analyzer 20.1.2 patch release. You can find vulnerabilities in your Kotlin applications after these requirements are met.
- 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.
- Java results – Some Java projects may show an increase in issue counts. We have improved our Java frontend in this release and the new design causes an increase in issues found in certain cases.
- Due to limitations in the .NET translator design, we are currently unable to track dataflows through callback arguments of .NET API calls that are specified as delegate objects or function names (aka method group expressions). This issue does not occur if callback arguments are passed in the form of lambda expressions or anonymous methods. We will improve the translator design in a future release to enable dataflow tracking through these arguments for all possible forms in which they can appear in the source code.
- Go:
    - Package “reflect” is not supported. See https://golang.org/pkg/reflect/.
    - Complex numbers are not supported. See https://golang.org/ref/spec#Numeric_types and https://golang.org/ref/spec#Complex_numbers.
    - Compiler directives are ignored. See https://golang.org/cmd/compile/, paragraph “Compiler Directives”.

Fortify Software Security Center (SSC)

- HTTP Basic authentication was deprecated for all REST API endpoints except for `/api/v1/tokens/*`, `/api/v1/auth/*` and `/api/v1/license`.
- The JDBC driver for MSSQL database server is now distributed with SSC.
- REST API endpoint `/api/v1/localUsers/{id}` change: `LocalUser` object has new integer value field - `objectVersion`. `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 consistence. `POST` and `DELETE` requests are not affected by the change.
- The CAS SSO “Fortify Software Security Center Location” (`cas.f360.server.location`) configuration option was removed from ADMINISTRATION. A value of the “Host URL” (`host.url`) property is now used. If `cas.f360.server.location` was different from `host.url`, make sure that you update your CAS authentication server settings.
- To improve application security: If X.509 or Kerberos/SPNEGO SSO authentication is enabled, SSC disallows local logins (using username and password) by default. This affects both LDAP and local users and applies to form UI login, REST API basic authentication and SOAP username/password

authentication. SSC can be accessed only via configured SSO method or API token. The behavior is configured with `sso.localAuthenticationEnabled` property in the `app.properties` file. The `sso.localAuthenticationEnabled` property fully replaces previously available `x509.localUserAuthenticationEnabled` property. A manual migration is required if `x509.localUserAuthenticationEnabled` is set to true. Enabling local login via the `-=aforementioned` property is necessary when you use integration with any product or tool that does not support configured SSO method or token-based authentication (e.g. some Fortify IDE plugins, Fortify WebInspect Enterprise).

- SSC may truncate HTTP response data in issues during FPR processing. In 20.1.0, if the HTTP response for an issue consists of more than 100,000 characters, SSC will truncate the response.
- Premium reports based on SSC 18.20 and later versions that are downloaded from the Customer Portal, are not compatible with versions prior to SSC 18.20.
- 18.10 and later versions contain performance fixes that require longer migration. Migration of databases with over 1 TB of data might take 5 or more hours.
- To prevent potential conflicts, do not run the Fortify ScanCentral Controller on the same Tomcat instance as Fortify Software Security Center.

Fortify WebInspect

- Not all builds of Windows 10 support .NET Framework 4.8. Refer to Microsoft's website to identify Windows 10 builds that support .NET Framework 4.8.
- The Windows 8 operating system is no longer supported.
- The `-engine` option was removed from the MacroGenServer.exe application in the 20.1.0 release. Attempting to use this option will result in the following error: `"Unable to parse command line at argument -engine."` The Micro Focus Fortify WebInspect 20.1.0 User Guide and help still describe this option. Ignore this option description in the documentation; it is no longer valid.

NOTICES OF PLANNED CHANGES

For notification of technologies that will not be supported in the next release, please see the "Technologies and Features to Lose Support in the Next Release" topic in the "Fortify Software System Requirements".

TECHNOLOGIES NOT SUPPORTED IN THIS RELEASE

For a list of technologies that are no longer supported in this release, please see the "Technologies and Features no Longer Supported in this Release" topic in the "Fortify Software System Requirements".

KNOWN ISSUES

The following are known problems and limitations in Fortify Software 20.1.0. The problems are grouped according to the product area affected.

Fortify Software Security Center

This release has the following issues:

- Occasionally, after you delete an application version and are redirected to the APPLICATIONS view, the deleted application remains visible. To solve this, refresh the APPLICATIONS view.
- If Fortify Software Security Center is installed on a Linux system, and you are running OpenJDK, you must install DejaVu Sans fonts and DejaVu Serif fonts on the server to enable users to successfully generate reports. Otherwise, report generation will fail. You can download these fonts from https://github.com/dejavu-fonts/dejavu-fonts.
- If you receive an auto-prediction failure with Audit Assistant, make sure primary tag values are assigned to 'True Issue'. This setting is required in version 19.2.0 and later.
- Occasionally you cannot download reports in MS Word format (DOC).
- You cannot enable "Enhanced security, security manager" for BIRT reports if you use MySQL Connector/J version 5.1.41 or later.

Fortify Static Code Analyzer

This release has the following issues:

- When translating .NET with a project configuration file (using the MSBuild /p:Configuration flag), make sure that there are no spaces in the project configuration file name. Otherwise, the translation will fail.
- Modular scanning: This release includes performance improvements that interfere with the accuracy of modular `'-with-includes'` scans. These scans have been temporarily disabled.

Fortify Audit Workbench, Secure Coding Plugins and Extensions

This release has the following issues:

- Legacy reports were temporarily disabled in the Fortify Visual Studio extension. The action is going to be restored in the next release but lose RTF format support. Use Fortify Audit Workbench or ReportGenerator command-line utility to generate legacy reports. You can still generate BIRT reports from Visual Studio.
- 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. It will pop up a dialog providing three options, one of which is Open. It allows you to run it even in the absence of notarization. More details are available in this 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.
- If you switch between TFS and Jira 7 bug trackers, you must restart Fortify Audit Workbench/Eclipse or you will get an internal error while validating credentials.
- On MacOS Catalina (10.15), the installer requires that the `fortify.license` file is not placed on the Desktop. If you point the installer to a Desktop location, it will fail to copy it. Put the `fortify.license` file in a folder to which the application has permissions, such as your user Home folder.
- The Audit Workbench launch screen is missing the "Start New Project" label used to combine the following commands: Scan Java Project, Visual Studio Build Integration, and Advanced Scan. The user guide refers to this label. This grouping label will be restored in the next release.

Fortify WebInspect

This release has the following issues:

- You may encounter the following known issues while using the Web Macro Recorder with Macro Engine 5.0:
  - Does not open after selecting it from the Tools menu or after clicking Record in the scan wizards.
  - Crashes on macro playback with an error in the log similar to "WebInspectWCFService.TCContainer Failed calling Navigate."

    For these issues, Windows may have prevented a ZIP file from being extracted in the C: Program Files directory.

    As a workaround, navigate to "C:\Program Files\Fortify\Fortify WebInspect" and manually extract all files from "dat59.zip" into "C:\Program Files\Fortify\Fortify WebInspect\dat59".

- In the Help, the Rendering Engine drop-down list in the Basic Scan Wizard and in Guided Scan lists Firefox and Internet Explorer as options. In the product, Firefox has been replaced with Macro Engine 5.0 (recommended) and Internet Explorer has been replaced with Session-based.
- The Review Vulnerability feature was removed when the new Retest feature was implemented. However, in the Help that is included with the WebInspect download, this feature is still listed in the Navigation Pane and Comparing Scans topics. The latest version of WebInspect documentation, which is available at https://www.microfocus.com/en-us/support/documentation, does not include this error.

Fortify WebInspect Enterprise

This release has the following issues:

- The following changes have been made to the WebInspect Enterprise server software requirements.
  - IIS 10 is now the recommended Web server. IIS 7.5, 8.0, and 8.5 are still supported.
  - Mozilla Firefox 75 or later is now the recommended browser. Internet Explorer 11 is still supported.

    The initial release of the System Requirements doc does not include this information.

- The Web Macro Recorder and Rendering Engine drop-down list issues listed under Fortify WebInspect also apply to Fortify WebInspect Enterprise.

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://softwaresupport.softwaregrp.com.

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.