Micro Focus Fortify Software v19.2.0 Release Notes

Document Release Date: November 21, 2019
Software Release Date: November 21, 2019

IN THIS RELEASE

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 19.2.0 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 19.2.0, which is downloadable from the Micro Focus Product Documentation website:

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

FORTIFY DOCUMENTATION

The Fortify Software documentation set contains installation, user, and deployment guides. In addition, you may 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 can be found on the Micro Focus Community (formerly Protect724) website: https://community.softwaregrp.com/t5/Fortify-Product-Documentation/ct-p/fortify-product-documentation.

GitHub Repository

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.

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

Fortify Static Code Analyzer

- Go programming language support - Fortify Static Code Analyzer support for scanning Go is included in this release. However, security content for this feature will be released on December 15, 2019. You can find vulnerabilities in your Go applications only after the security content is available.
- 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.
- Fortify Static Code Analyzer does not support scanning .NET solutions built with Visual Studio 2019 or MSBuild 15.9 or later.

Fortify Static Code Analyzer Tools

- The Fortify extension for Visual Studio 2019 is available in this release but there is limited Fortify SCA support with regards to .NET Core (2.2, 3.0, & 3.1 are currently unsupported by SCA) and to .NET solutions created after 15.9. See Fortify SCA system requirements

Fortify Software Security Center

- Premium reports based on SSC 18.20 and later versions, 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 hours or more.
- In order to prevent potential conflicts, the Fortify CloudScan Controller should not be run on the same Tomcat instance as Fortify Software Security Center.

Fortify WebInspect

- The following text from “Troubleshooting the Postman Scan” in the Fortify WebInspect documentation is incorrect:

  Check the API server logs for more detailed information about which requests executed and which ones failed. You can view the API server logs in the active `WIRCServer.exe` window.

  The text should read as follows:

  Check the API server logs for more detailed information about which requests executed and which ones failed. You can view the API log files using the Windows Event Viewer. The log files are located under **Applications and Services Logs > WebInspect API**.

NOTICES OF PLANNED CHANGES

This list serves as notification of technologies that will not be supported in our 20.1.0 release. This list is not exhaustive and is subject to change without notice. It is based on information known at the time of the 19.2.0 release.

Fortify Software Security Center

- HTTP Basic authentication is scheduled for deprecation for all REST API endpoints except for `/api/v1/tokens/* and /api/v1/license`.

Fortify Static Code Analyzer Tools

- Legacy reports will no longer be available in RTF format. Reports generated using the ReportGenerator command-line utility or the Legacy Reports command in SCA Tools will only support XML and PDF formats.

Fortify WebInspect

No planned changes in WebInspect 20.1.0.

TECHNOLOGIES NOT SUPPORTED IN THIS RELEASE

Fortify Static Code Analyzer

The following technology is not supported in this release:

- AngularJS 1.x

Fortify Static Code Analyzer Tools

The following technologies are not supported in this release:

- Visual Studio 2013
- Eclipse 4.8, 2018-09 (4.9)
- Android Studio 3.0
- Team Foundation Server (TFS) 2013

Fortify WebInspect

The following technology is not supported in this release:

- Windows Server 2012 and 2012 R2

KNOWN ISSUES

The following are known problems and limitations in Fortify Software 19.2.0. The problems are grouped according to the product area affected.

Fortify Software Security Center

This release has the following known issues:

- If Fortify Software Security Center is integrated with Audit Assistant, and you have configured a default value for an application version's primary custom tag, Audit Assistant training does not behave as designed. To optimize Audit Assistant training results, remove the value set as the default for primary custom tags.
  Note: The Analysis tag has no default value unless a user has assigned one.
- On auto-prediction failure with Audit Assistant, please check if primary tag has values assigned to 'True Issue'. This setting is required starting 19.2.0.
- It is not currently possible for a user belonging to an LDAP group to create new application versions in SSC. For example, if an LDAP group has the "Security Lead" role and a member of it logs in to SSC, the application wizard is enabled in the UI. However, if the user attempts to create an application version, it will result in errors when the "Finish" button is pressed in the

Application creation wizard. (Local users and directly registered LDAP users can create application versions if they have the "Security Lead" role.)
Workaround: Customers who want to allow members of an LDAP group to create application versions must assign the "Administrator" role to that group.

- Occasionally you can't download reports in MS Word format (DOC).
- "Enhanced security, security manager" for BIRT Reports can't be enabled if MySQL Connector/J 5.1.41 or newer is used.

Fortify Static Code Analyzer

This release has the following known issues:

- Swift: Null Pointer Exception during High Order Analysis (in StackCESKMachinery.java) of Swift App. There is a known issue with Fortify Static Code Analyzer that causes NPE during scanning Swift apps. The issue occurs when the name of a variable or constant inside a computed property is identical to the property name. Use different names for the computed property and variable or constant inside it to work around this issue.
- Swift: Error opening input file (No such file or directory) [ERROR 1103] Translator execution failed. There is a known issue with Fortify Static Code Analyzer where it throws "error opening input file /<path>/R.swift (no such file or directory)" while translating the R.Swift library. As a workaround, remove the following line from the file: ~/.fortify/sca18.2/build/<build_id>/swift-filelist.txt. Do not issue a sourceanalyzer clean (sourceanalyzer -b <build-id> -clean) command; instead, redo the translation with xcodebuild clean build.
- Due to limitations of the .NET translator design, we're 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.
- Python: When scanning large Python projects on machines with less than 64 GB memory, you may receive an "Out of Memory" warning. To address this, do one of the following:
    - Increase the amount of memory on the machine.
    - Use the previous HOA algorithm by adding the following command line switch: Dcom.fortify.sca.Phase0HigherOrder.AnalysisType=pushdown.
- 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.
    - In function literals, referring variables defined in a surrounding function is not supported. See https://golang.org/ref/spec#Function_literals.
    - Composite literal elements of composite literals are not supported. See https://golang.org/ref/spec#Composite_literals.
    - Arrays and slices of function elements are not supported. See https://golang.org/ref/spec#Array_types, https://golang.org/ref/spec#Slice_types, and https://golang.org/ref/spec#Function_types.
    - Compiler directives are ignored. See https://golang.org/cmd/compile/, paragraph "Compiler Directives".
    - In package blocks, so-called "init" functions are not supported. See https://golang.org/ref/spec#Package_initialization.

Fortify Audit Workbench, Secure Coding Plugins and Extensions

This release has the following known issues:

- Visual Studio extension generates new tokens for each operation with SSC so you may reach the maximum day limit if you do too many uploads from the extension. If it happens, you will see the error "(400) Bad Request" in Visual Studio upon uploading to SSC. To work around this, you can either increase the maximum number on SSC by editing "token.management.user.sessionless.tokens.max" property in ssc.properties on the SSC server or remove the tokens generated by the plugin from the SSC web UI.
- Analyze Project action in IntelliJ Analysis plugin can't analyze java projects with Java 10, 11 or 12 JDK configured. `Fortify -> Analyze Project` displays an error "`Invalid parameter 0.0 for command line argument -source`". If you see that message, use Advanced Analysis action instead.
- 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. Please, 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 3 options, one of which is Open. It allows you to run it regardless of the absence of notarization. Please, find more details in this article: https://support.apple.com/en-us/HT202491
- Security Assistant for Eclipse requires an internet connection for the first run. If you don’t 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 needs the fortify.license file not to be placed on the desktop. If you point the installer to Desktop location, it will fail to copy it. Please, put the fortify.license file in the folder the application has permissions, like your user Home folder.

Fortify WebInspect

- Windows may fail to apply the C++ 2015 runtime redistributable package provided by Microsoft. If you encounter an issue with scans having errors related to loading SPI.Parsers.Script, you must manually install the C++ runtime redistributable package before continuing.

Fortify WebInspect Enterprise

- When you launch the Guided Scan and Reporting help from the WebInspect Enterprise Desktop Application using Chrome or Firefox, the stylesheet and images are blocked by these browsers. This action causes missing images and incorrect fonts in the displayed help. A workaround for this issue is to open the Guided Scan.chm file directly from the installation directory in Windows Explorer.

SUPPORT

If you have questions or comments about using this product, contact Micro Focus Fortify Customer Support using one of the following options.
To Manage Your Support Cases, Acquire Licenses, and Manage Your Account: https://softwaresupport.softwaregrp.com.