Micro Focus Fortify Software v19.1.0
Release Notes

Document Release Date: July 31, 2019
Software Release Date: May and June 2019

Updated: August 26, 2019

IN THIS RELEASE

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 19.1.0 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 19.1.0, which is downloadable from the Micro Focus Product Documentation website:

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

FORTIFY DOCUMENTATION UPDATES

The contents of the Micro Focus Fortify Static Code Analyzer Installation Guide, the Micro Focus Fortify Static Code Analyzer Performance Guide, and the Micro Focus Fortify Static Code Analyzer User Guide have been combined into a single document. We now publish only the Micro Focus Fortify Static Code Analyzer 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 can be found on the Micro Focus Community (formerly Protect724) website: https://community.softwaregrp.com/t5/Fortify-Product-Documentation/ct-p/fortify-product-documentation.

FORTIFY PRODUCT VERSION NUMBERING

Beginning with this release, we have slightly altered our version numbering scheme. The first two digits represent the year of release. This is followed by a single digit to identify the release sequence within the year, and a final digit to identify the patch number. So the first release of 2019 is 19.1.0. If a patch is released, the third digit changes to 1. A release number of 19.2.1 would identify the release as the first patch release to the second release of 2019.

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 new 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.
- 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 Tools

- Support for Kerberos SSO in Audit Workbench and the secure coding plugins for Eclipse and Visual Studio is limited to the Windows platform.
- The Fortify Jenkins Plugin is no longer included with the Fortify_SCA_and_Apps package. This plugin is now available on the Jenkins Plugins Index and you can download and install this plugin directly from Jenkins. Go to Manage Plugins, click the Available tab, and then select the "Fortify" plugin.
- Scan Wizard is no longer shipped as a standalone application, but it is still included in the Fortify_SCA_and_Apps installer. You can request a standalone version from Fortify Customer Support.
- 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 Software Security Center

- To use x.509 authentication in Software Security Center, the Unlimited Cryptography Strength Jurisdiction Policy is required. This is included by default with Oracle JDK version 1.8.161+ and OpenJDK 1.8.161+. You may also need to install a certificate for Software Security Center to the same runtime environment if a self-signed certificate is used for an HTTPS connection.
- 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. You must install a trusted CA certificate on the Java Runtime environment on both the Fortify Software Security Center and Fortify WebInspect servers to view Fortify WebInspect scan results within Fortify Software Security Center.
- JavaScript Sandbox Project (https://fortify.github.io/ssc-js-sandbox-docs/) -- A utility designed to showcase customer requested scenarios leveraging the Fortify Software Security Center RESTful API. The code is available as well as the tutorial style documentation.

Fortify WebInspect

- The new login and workflow macro recorder in Fortify WebInspect provides improved scan speeds as well as better support for modern single-page applications. However, it also requires more resources. If you elect to use this upgraded tool, then Micro Focus suggests that you use it with the recommended hardware requirements of 4 CPU cores and 16 GB of RAM or greater.

- Windows Server 2012 R2 is currently included as a supported Operating System, however our real-world experience has shown this OS version to have major reliability problems related to SSL and TLS. We will drop support for this operating system in our next release, and we urge customers to upgrade their operating systems as soon as possible.

NOTICES OF PLANNED CHANGES

This list serves as notification of technologies that will not be supported in our 19.2.0 release. This list is not exhaustive and is subject to change without notice. It is based on information known at the time of the 19.1.0 release.

Fortify Software Security Center

No planned changes in SSC 19.1.0.

Fortify Static Code Analyzer Tools

After this release, we will no longer support:

- Android Studio 3.0
- Eclipse 4.8, 4.9
- Visual Studio 2013

Fortify WebInspect

After this release, we will no longer support:

- Windows Server 2012 and Windows Server 2012 R2

TECHNOLOGIES NOT SUPPORTED IN THIS RELEASE

Fortify Software Security Center

The following technologies are not supported in this release:

- SQL Server 2014
- Internet Explorer 11
- Service Integrations: Jira 7.4

Fortify Static Code Analyzer

The following technologies are not supported in this release:

- Xcodebuild 9.x
- Apple LLVM (clang) 5.x
- Swift 4.1.x

Fortify Static Code Analyzer Tools

The following technologies are not supported in this release:

- IntelliJ 2017.x
- WebStorm 2017.x
- Eclipse 4.6, 4.7
- Android Studio 2.3.x
- Standalone Scan Wizard distribution

KNOWN ISSUES

The following are known problems and limitations in Fortify Software 19.1.0. The problems are

grouped according to the product area affected.

Fortify Software Security Center

This release has the following issues:

- If you have permission to comment on issues, but do not have permission to edit custom tag values, then if you add a comment from the issue details section of the AUDIT page, your first attempt to save the comment will fail. To work around this issue, click SAVE a second time. The second save attempt will succeed.
- The first page (Start page) of the Fortify Software Security Center Setup wizard contains a link to the Release Notes for the 18.20 version of the software. The correct link is: https://www.microfocus.com/documentation/fortify-software-security-center/1910/19.1.0%20Release%20Notes.htm
- 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 _are_ able to 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.
- If Tomcat is installed in a path containing white spaces, there might be problems displaying issues under the Audit tab for an Application Version. For example, the following installation path examples include one or more spaces and should be avoided:

  C:\parent dir with spaces\child_dir_no_spaces\tomcat_install_dir\

  C:\parent_dir_no_spaces\child dir with spaces\tomcat_install_dir\

  C:\parent_dir_no_spaces\child_dir_no_spaces\tomcat install dir with spaces\

- 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 Software Security Center must be deployed as a single instance and not behind a load balancer.
- Your LDAP server (single or multiple) should not be configured behind a load balancer.

Fortify Static Code Analyzer

This release has the following 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.
- .NET: There is a known issue in .Net binary translation which may not work correctly if multiple binaries are translated with separate Fortify Static Code Analyzer invocations where the same build ID is used across all invocations. This scenario is supposed to be used to enable scanning the entire set of translation results by a single Fortify Static Code Analyzer invocation. The issue is manifested by numerous translation and scan errors. As a workaround, use MSBuild integration or the Fortify Extension for Visual Studio for translation of .Net projects if this issue is observed.

- Java results – Some Java project scans may produce an increased number of issues. We have improved our Java frontend in this release and the new design may result in an increase in the number of issues found.
- 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.
- Scan Wizard does not support scanning Apex and Visualforce code in this release.

Fortify Audit Workbench, Secure Coding Plugins and Extensions

This release has the following issues:

- Fortify Complete plugin for Eclipse 4.7+ - the progress dialog is not displayed by default when you do things like open an FPR or start a scan. Instead, there is a progress indicator at the bottom right corner of the window that you can click to see how things are progressing. If you like to see the dialog, you can configure it in Window > Preferences > General > remove the "Always run in background" check.
- Fortify Audit Workbench - Issues you suppress might still appear in the issues list; if this occurs, choose Options > Show Suppressed Issues and disable the Show Suppressed Issues function.
- 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.
- Fortify Remediation plugin for Eclipse displays an error if the Fortify Complete plugin for Eclipse is also installed. Please uninstall the Fortify Complete plugin to work with the Fortify Remediation plugin. You can contact customer support to get an updated version of Fortify Remediation plugin for Eclipse.

Fortify WebInspect

- Any supported Windows operating system 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.
- The topics "Converting Recorded Steps to Code" and "Using the Event Handler Editor" in the help for the Web Macro Recorder tool Technology Preview describe features that are not available in the tool. Ignore these topics.

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.

To Call Support
844.260.7219

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.