Micro Focus Fortify Software, Version 22.1.0
Release Notes
Document Release Date: June 7, 2022, updated 12/14/2022

IN THIS RELEASE

This document provides installation and upgrade notes, known issues, and workarounds that apply to release 22.1.0 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 22.1.0*, which is available on the Micro Focus Product Documentation website:

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

FORTIFY DOCUMENTATION UPDATES

Accessing 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 forthcoming 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.

- The *Micro Focus Fortify Plugins for Eclipse User Guide* and the *Micro Focus Fortify Plugins for JetBrains IDEs and Android Studio User Guide* do not include the complete updates for the remediation plugins. These two guides will be updated when the plugins are released in an upcoming patch release. For more information, see NOTICES OF PLANNED CHANGES for Secure Code Plugins in this document.

INSTALLATION AND UPGRADE NOTES

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

Fortify Static Code Analyzer

Migrating from a Patched Release of Fortify Static Code Analyzer: If your Fortify Static Code Analyzer installation has been patched, the last digit in the version number will be greater than zero. For instance, release 21.2.0 has a zero as the last digit which identifies it as a major release that has not been patched. Versions 20.1.6, 20.2.4, 21.1.4, and 21.2.3 are examples of patched releases. When upgrading from a patched Fortify Static Code Analyzer release, your configuration files and properties (`sca.properties`) may not carry over to

the new installation. If you would like to migrate your configuration and properties settings to the new installation, please contact Customer Support for assistance.

Fortify ScanCentral SAST

The ScanCentral SAST client must be installed on a machine with a Java 11 runtime.

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

- PHP: There is a new preview PHP translator that you can enable with the -Dcom.fortify.sca.PHPv2 option on the command-line. The translator is still in development and not complete but fixes problems in the production translator and in some cases can produce better results.

Fortify Software Security Center

- Fortify Software Security Center can now identify Security Assistant Rulepacks on import and correctly distribute them to Rulepack update clients. This identification only happens when Rulepacks are imported into Fortify Software Security Center. For Fortify Software Security Center to identify Security Assistant Rulepacks that already exist in Fortify Software Security Center, you will need to remove them from Fortify Software Security Center and re-import them.
- When a third-party scan is uploaded to Fortify Software Security Center, the Plugin Framework now validates that the `engineType` of the submitted vulnerabilities is coherent with `engineType` provided in the plugin metadata. Incorrectly implemented parser plugins will fail to submit vulnerabilities. Fortify recommends fixing such plugins at your earliest convenience. In the meantime, the validation can be suppressed by setting a system environment variable `FORTIFY_PLUGINS_PARSER_VULN_ENGINETYPECHECK` or JVM system property `fortify.plugins.parser.vuln.engineTypeCheck` to `false`. Starting from 23.1 release, it will no longer be possible to suppress this validation.
- When aggregating by an attribute of date type, REST API endpoint `/api/v1/dashboardVersions` now returns date in `YYYY-MM-DD` format instead of `YYYY-MM-DD 00:00:00.00` on Oracle and MSSQL databases. The format can be changed to the original one for backward compatibility by adding dashboard.aggregation.dateFormatBackwardCompatibility=true property to app.properties.
- A request to generate report will fail if the requestor does not have `Generate reports` permission. Previously, a POST to `/api/v1/reports` endpoint succeeded, but the underlying job of report generation failed.
- For security reasons, validation of allowed characters was tightened up for the fields of these entities:

    - Local User: First Name, Last Name, Username, Email
    - Role: Name, Description
    - Application: Name
    - Application Version: Name

  Added restrictions: value must not start with = (equals to) + (plus) - (minus) or @ (at) character and must not contain control characters (with exception of a newline in Role's Description field). Validation is applied in both REST API and UI. This affects creating a new entity as well as updating an existing one. Affected REST API endpoints: `/api/v1/localUsers`, `/api/v1/roles`, `/api/v1/projects`, `/api/v1/projectVersions`

  Thanks to GovTech (Thomas Lim and Yu Pengfei) for discovering the need for this validation.

- It is no longer possible to submit a DELETE request to the `/api/v1/authEntities/{parentId}/projectVersions` endpoint with an empty list of IDs to delete. This resulted in removing access to all applications versions the auth entity had access to. Now the list of IDs to delete is required and it is no longer possible to submit a `DELETE` request with empty list.
- The maximum allowed size for JSON requests to SCIM API (`/api/scim/v2/`) was limited to 10 MB. The maximum size of the request can be customized by adding following property to `app.properties`: `scim.request.maxJsonSize=X`, where X is the desired maximum size in bytes.
- In previous releases, Fortify Software Security Center did not perform validation to prevent loading of project templates containing custom tags with negative lookup indices - even though this was never the intended usage and could result in mutated indices being stored in Fortify Software Security Center. Validation has now been added to enforce the intended behavior and Fortify Software Security Center will only allow loading new project templates containing custom tags with non-negative lookup indexes. Consider the following cases involving legacy project template files (containing negative lookup indexes for one or more custom tags)
    - Older Fortify Software Security Center instance with template already loaded:
        - If the template is not currently assigned to any applications, delete the template and the custom tag from the system.
        - If the template is assigned to applications and users have already used the tag in issue audits, leave it as is.
    - Attempting to load the legacy template into a new SSC instance:
        - We strongly recommend that you not use such a template. Instead, edit the template (xml file) to use non-negative indices before you load it into a new Fortify Software Security Center instance.
        - If the template cannot be modified, you can use a fallback to allow the deprecated legacy behavior. The `custom.tag.values.lookupindices.handling.legacy` Fortify Software Security Center property must be set to true before you attempt to load the template into a new SSC instance.

KNOWN ISSUES

The following are known problems and limitations in Fortify Software 22.1.0. The problems are grouped according to the product area affected.

Fortify Software Security Center

- Enabling the "Enhanced Security" option for BIRT reports will break report generation if Fortify Software Security Center is installed on a Windows system.
- For successful integration with Fortify WebInspect Enterprise, Fortify Software Security Center must be deployed to /ssc context. In particular, the context must be changed for Fortify Software Security Center Kubernetes deployment, which uses root context by default.
- If there are errors on the Application Version Overview page when selecting group by & filter by options, please clear all the filters and retry prior to refresh.
- Fortify Software Security Center 21.2.0 introduced faulty migration for newly introduced `Use data exports` permission. Instead of executing only once, the migration was executed every time seeding was performed in Fortify Software Security Center 21.2.0 in maintenance mode. To resolve the issue, the migration will run one last time during migration to 22.1.0.

  The migration in question adds the new `Use data exports` permission to any existing role that also contains a `View Application Versions` permission. In case any custom non-system defined roles were affected and the change was not desired, please update these roles manually after migration to 22.1.0.

- Fortify Software Security Center API Swagger spec contains two definitions that differ only in case:
  - `Custom Tag` used for assigning custom tag values to issues in an application version
  - `Custom tag` used for managing custom tags

  Please pay attention when using tools to auto-generate API clients from Swagger spec. This might cause conflicts due to case insensitive process, and the generated client might need manual modification.

Fortify ScanCentral SAST

- In the Fortify ScanCentral SAST CLI, the `-targs` and `-sargs` options do not handle paths with spaces correctly. To resolve this issue, all paths that include spaces should be enclosed in quotes as in the following examples:

  ```
  -targs "-exclude 'C:\My Project\src\Project1.java'"
  ```

Fortify Static Code Analyzer

- While scanning JSP projects, you might notice a considerable increase in vulnerability counts in JSP-related categories (e.g. cross-site scripting) compared to earlier versions of Fortify Static Code Analyzer. To remove these spurious findings, specify the `-legacy-jsp-dataflow` option on the Fortify Static Code Analyzer command line during the analysis phase.

- In some circumstances the custom settings in the `fortify-sca.properties` configuration file may not get migrated. As a workaround, copy the custom settings from the `fortify-sca.properties` configuration file in the old installation location into the new one.

Fortify Audit Workbench, Secure Code Plugins, and Tools

- If you are not connected to the internet, you will get an `Updating Security Content` error when you first start Fortify Security Assistant for Eclipse. After importing the rules, you will no longer get this error upon startup.

Fortify ScanCentral DAST

- When importing an HTTP archive (.har) file to use as a workflow macro, the file size is limited to 4 MB. To increase the file size limit to 30MB, run the following SQL command:

```
IF NOT EXISTS (SELECT Id FROM ConfigurationSetting WHERE SettingName =
'UtilityWorkerServiceSettings.MaxReceiveMessageSize')

    INSERT INTO ConfigurationSetting (SettingName, SettingValue,
    IsEncrypted)

    VALUES ('UtilityWorkerServiceSettings.MaxReceiveMessageSize',
    '31457280', 0)

GO
```

- Global Restrictions and Application Settings Domain Restrictions are applied only for Standard Scans or API scans that use a start URL.

NOTICES OF PLANNED CHANGES

This section includes product features that will be removed from a future release of the software. In some cases, the feature will be removed in the very next release. Features that are identified as deprecated represent features that are no longer recommended for use. In most cases, deprecated features will be completely removed from the product in a future release. Fortify recommends that you remove deprecated features from your workflow at your earliest convenience.

Note: For a list of **technologies** that will lose support 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.

Fortify Static Code Analyzer

- Support for the GOPATH will be removed in a future release to align with changes in the Go language.

Fortify Software Security Center

- REST API token endpoint `/api/v1/auth/token` will be removed in the next release. The endpoint has been disabled by default since the 21.1.0 release. Please use the `/api/v1/tokens` endpoint instead.
- SOAP API is deprecated and is scheduled for removal, together with `fortifyclient` and the `wsclient` library.
    - Please use REST API (`/api/v1/*, /download/*` and `/transfer/*`) endpoints instead of SOAP API (`/fm-ws/*`) endpoints
    - A new sample command-line based Fortify Software Security Center client (`ssc-client`) using REST API is included in the Fortify Software Security Center distribution. The `ssc-client` sample serves as a starting point for using a REST API-based client as a replacement for the SOAP API-based `fortifyclient`.
- The Velocity template engine library will be upgraded in the next release. This might affect custom bugtracker filling templates, which might need to be manually updated to be compatible with new syntax.
- A major upgrade of libraries providing functionality for SAML Single Sign On and Single Logout solution will be in the next release. Although Fortify will look into making the transition as smooth as possible, extra steps may be part of the upgrade process for Fortify Software Security Center with SAML enabled. This includes updating the Identity Provider service configuration.

Fortify ScanCentral SAST

- The `allow_insecure_clients_with_empty_token` property, used to configure the Controller, will be removed from the `config.properties` file in 22.2.0.

Fortify Audit Workbench, Secure Code Plugins, and Tools

- Eclipse Remediation Plugin is not included in the Fortify_SCA_and_Apps_<version>_<OS>.zip in this release. It will be available in a patch release and for download from the Eclipse Marketplace. Starting from the next release, it will only be available from the marketplace.
- IntelliJ Remediation Plugin is not included in the Fortify_SCA_and_Apps_<version>_<OS>.zip in this release. It will be available in a patch release and for download from the JetBrains Marketplace. Starting from the next release, it will only be available from the marketplace.
- Security Assistant for Eclipse will not be included in the Fortify_SCA_and_Apps_<version>_<OS>.zip in the next release. It will be available for download from the Eclipse Marketplace.

FEATURES NOT SUPPORTED IN THIS RELEASE

The following features are no longer supported. Fortify Static Code Analyzer no longer supports Visual Studio Web Site projects. You must convert your Web Site projects to Web Application projects to ensure that Fortify Static Code Analyzer can scan them.

- The Seven Pernicious Kingdoms report is longer supported. It was deprecated and is not recommended for use.
- Fortify WebInspect no longer supports Flash parsing

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. This list only includes **features** that have lost support in this release.

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.