MICRO FOCUS

Fortify Software

What’s New in Micro Focus Fortify Software 19.1.0

May - June 2019

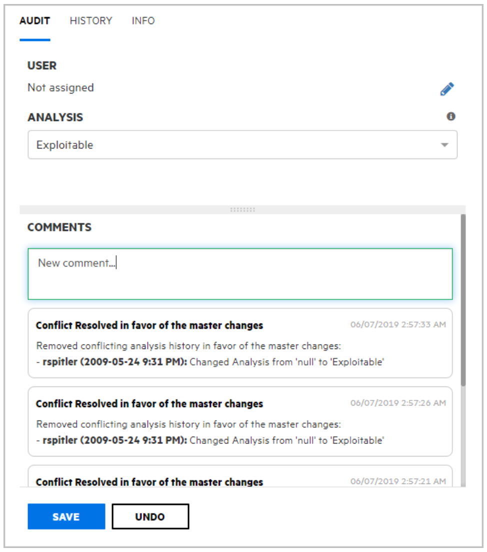
This release of Micro Focus Fortify Software includes the following new functions and features.

Micro Focus Fortify Software Security Center

The following features have been added to Fortify Software Security Center.

UI / Usability Updates

- The COMMENTS section has been moved. Previously, you posted and viewed comments from the COMMENTS & HISTORY tab. Now you can post and view comments on the AUDIT tab in the right panel of the issue details section.



USER

Not assigned

ANALYSIS

Exploitable

COMMENTS

New comment...

Conflict Resolved in favor of the master changes 06/07/2019 2:57:33 AM

Removed conflicting analysis history in favor of the master changes:
- **rspitler (2009-05-24 9:31 PM):** Changed Analysis from 'null' to 'Exploitable'

Conflict Resolved in favor of the master changes 06/07/2019 2:57:26 AM

Removed conflicting analysis history in favor of the master changes:
- **rspitler (2009-05-24 9:31 PM):** Changed Analysis from 'null' to 'Exploitable'

Conflict Resolved in favor of the master changes 06/07/2019 2:57:21 AM

- Audit Page: Rulepack content is now divided into separate sections. Details / Recommendations / Metadata / References / etc are now found in the Info tab.
- The new version selector has a three-column layout for selecting application versions. It was designed to accommodate thousands of application versions.

Micro Focus Fortify Static Code Analyzer

The following features have been added to Fortify Static Code Analyzer.

TypeScript

TypeScript language support now includes:

- Higher Order Analysis (HOA) performance improvements
- Support for TypeScript 3.0, 3.1 and 3.2

Python

Python language support now includes:

- Support for Python 3.7
- Support for Django 2.x
- Performance improvements

Gradle

Gradle support now includes Gradle 4.x.

Angular

Angular support now includes Angular 7.

Java

Java support now includes Java 10 and Java 11.

ECMAScript

Fortify Static Code Analyzer now supports ECMAScript 2018.

Higher Order Analyzer

Higher Order Analyzer is on by default for JavaScript and TypeScript applications. When Higher Order Analyzer is enabled, Fortify Static Code Analyzer is able to better track dataflow issues and uncover more vulnerabilities.

Micro Focus Fortify CloudScan

Fortify CloudScan now ships with a utility to package source code, dependencies, and Fortify Static Code Analyzer translation instructions. You no longer have to install Fortify Static Code Analyzer locally or on the build server. The packaging utility allows you to centralize your Fortify infrastructure and create a consistent approach across languages.

- You no longer have to install and run Fortify Static Code Analyzer on the build server for the following languages: Java, JavaScript, Ruby, Python, and PHP.
- The packaging utility packages everything necessary, including dependencies, and sends the package directly to the CloudScan CLI. The CloudScan CLI then sends it on to the sensors, which perform both translation and scanning phases of the analysis.
- The packaging utility intelligently sets what were previously manual translation options. Simply provide the location of the build file (build.gradle / pom.xml). No other configuration options are required for build integration.
- This new Fortify CloudScan utility supports auto packaging using the Gradle or Maven build tools.

Micro Focus Fortify Static Code Analyzer Tools

The following features have been added to Fortify Static Code Analyzer Tools.

Fortify Jenkins Plugin

- Post-build action analyzes the source with Fortify Static Code Analyzer, updates security content, uploads analysis results to Fortify Software Security Center, and fails the build based on uploaded results processed by Fortify Software Security Center.
- Provides native pipeline support for source code analysis with Fortify Static Code Analyzer, security content update, and uploads to Fortify Software Security Center.
- Snippet generator makes it easy to generate the pipeline code necessary to add a Fortify task to a pipeline script.
- Displays Fortify security analysis results for each job that includes a history trend and the latest issues from Fortify Software Security Center. Navigates to individual issues on Fortify Software Security Center for detailed analysis.

Micro Focus Fortify WebInspect

The following features have been added to Fortify WebInspect.

Login Macro Recorder updates

We've upgraded the underlying engine that drives our Login Macro Recorder. You will now experience improved compatibility with recording macros on applications built in modern frameworks.

Automatic Macro Creation

We're eliminating some of the manual touchpoints traditionally required by dynamic scanning. WebInspect can now automatically create a login macro with just a URL, username, and password. However, you can still use our familiar Login Macro Recorder to record a macro manually.

Automatic Macro Validation

Ease of use is important to us. With our new Macro Validation feature, WebInspect can now optionally test macros prior to scanning. This will minimize wasted time spent scanning with macros which may have outdated credentials or steps that are no longer valid.

Swagger (OpenAPI) 3.0 support

We're committed to making API scanning easier. Our WISWAG tool can now consume definitions built in the OpenAPI 3.0 specifications, and convert them to settings for simple API scanning.

Multi-user Login Macro improvements

For single-session restricted applications, WebInspect supports tying a unique user/password combination to each thread. With this release, we've added this feature to the user interface.

New API Endpoints

Our new "data" API endpoint simplifies requesting vulnerability details, scan statistics, and dashboard information.

Directory Hit Count Limiter

Long running scans are a waste of everyone's time. We've introduced a directory hit count limiter that can be used to easily control scans that run long because of wide directory structures.

WebInspect on Docker

For customers using concurrent licenses, we're now providing a containerized version of WebInspect that supports both CLI- and API-driven scanning.

Micro Focus Fortify WebInspect Enterprise

The following feature has been added to Fortify WebInspect Enterprise.

New API Endpoints

New SmartUpdate endpoints provide a way of:

- Getting a list of all SmartUpdate occurrences
- Getting details or status of a specific SmartUpdate
- Starting the SmartUpdate process to download the latest SecureBase changes and sensor versions

Contacting Micro Focus Fortify Customer 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

1.844.260.7219

For More Information

For more information about Fortify software products:
https://software.microfocus.com/solutions/application-security

What’s New in Micro Focus Fortify Software 18.20

November 2018

This release of Micro Focus Fortify Software includes the following new functions and features.

Micro Focus Fortify Software Security Center

The following features have been added to Fortify Software Security Center.

SSC Scalability

- The persistence layer has been optimized to accommodate additional SCA scans
- The format of the issue fields has been made more efficient when storing and retrieving
- Total issue size has been reduced
- Adding new scans is typically 10-30% faster

Audit Page Redesign (Phase 1)

- Fortify Priority Order (Critical / High / Medium / Low) appears on the Audit and Overview screens. Clicking these folders allows you to view the associated issues.
- Issue Details and Recommendations are now accessed from the tabs on the Audit page
- Adding comments to individual issues no longer requires going to the Assign screen; comments can be submitted directly in the Audit page

Audit Assistant Auto-Predict

- You can now set automatic predictions for application versions. You can enable this feature on the **ADMINISTRATION -> Configuration -> Audit Assistant** page by checking the **Enable auto predict** check box in the application version Profile window
- New predictions are automatically requested when new issues are uploaded to an application version

Note: Audit Assistant does not re-predict on issues in application versions when a previous prediction was made. Create a new application version to reset this functionality.

Application Security Training

When viewing security issues, a "Get Training" link will take you to contextual application security training provided by Secure Code Warrior.

- Contextually correct application security training has been designed to integrate with any application security training provider. The current iteration includes integration to Secure Code Warrior.
- A current list of the full mapping between Secure Code Warrior and Fortify Software Security Center is available from customer support

Request Dynamic Scans (Fortify WebInspect Enterprise) Migrated to the Current User Interface

The dynamic scan request feature in the legacy user interface has been migrated to the current user interface

Micro Focus Fortify Static Code Analyzer

The following features have been added to Fortify Static Code Analyzer.

Apple Update

Support for the latest releases of the following components:

- Swift 4.2
- Xcode 10
- Objective-C/C++

TypeScript

Added the ability to scan TypeScript applications. TypeScript is a superset of JavaScript that adds optional static typing to the language.

.NET Update

- MSBuild support has been changed to reflect the direction Microsoft has set for .NET
- MSBuild integration is now the only build integration used to translate .NET applications

- When translation is invoked from the Visual Studio extension or devenv on the command line, MSBuild integration is used
- In addition to translating Visual Studio Solutions, you can now translate individual Visual Studio Projects
- Added support for delegate and function modeling
- Improved support for rules surfaces more vulnerabilities in .NET applications

Python

The new Python translator supports both Python 2 and Python 3 applications. The new Python translator is used by default, but the legacy Python 2.x translator is still available with a command line option.

The new Python translator provides:

- Improved support for Python 3
- Support for Python 2.x applications
- Improved support for Django 1.8

The legacy Python 2 Translator:

Fortify Static Code Analyzer uses the new Python translator by default. To use the legacy translator, specify it on the command line.

Scanning Python 3 Applications:

By default, Fortify Static Code Analyzer assumes you are scanning Python 2.x applications. To scan Python 3 applications, specify the Python version on the command line:

```
-python-version 3
```

Node.js

We added support for scanning Node.js 10.x applications.

Angular

This initial release of Angular support enables scanning Angular 2, 4, 5 and 6 applications.

Java 9

Major defects were fixed in our Java 9 support, resulting in the discovery of more complex vulnerabilities in Java 9 applications.

Logging

With this release, we provide a major update to the logging infrastructure. There are now two different log files:

- Standard log file (sca.log): provides information you can use when troubleshooting
- Fortify Support log (sca_FortifySupport.log): provides information that may be helpful to the customer support or development team

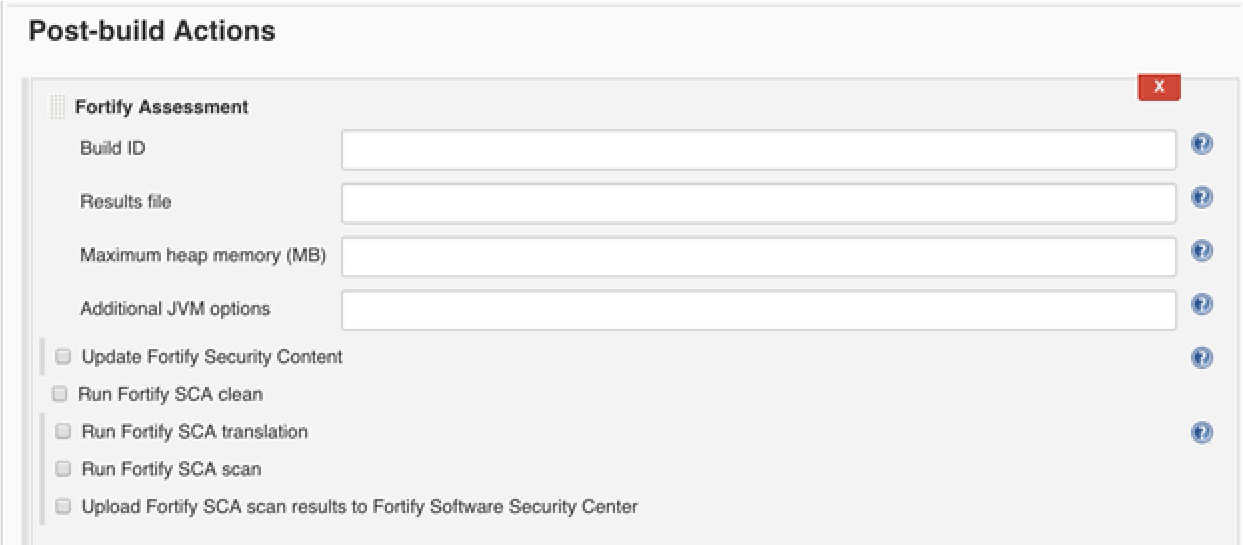
Micro Focus Fortify Static Code Analyzer Tools

The following features have been added to Fortify Static Code Analyzer Tools.

Fortify Jenkins Plugin

An improved version of the Fortify Jenkins Plugin. It includes the following features and capabilities:

- Full translation and analysis capabilities
- Ability to upload your results to Fortify Software Security Center
- Supported application types include:
  - Java
  - Maven
  - Gradle
  - .NET (msbuild / devenv)
  - Other (directly input any Fortify Static Code Analyzer command)
  - Ability to fail or mark builds as unstable using the Fortify Software Security Center search criteria



Post-build Actions

Fortify Assessment

Build ID

Results file

Maximum heap memory (MB)

Additional JVM options

□ Update Fortify Security Content

□ Run Fortify SCA clean

□ Run Fortify SCA translation

□ Run Fortify SCA scan

□ Upload Fortify SCA scan results to Fortify Software Security Center

MSBuild Integration Enhancements

With this new, enhanced version, you can continue to use devenv or msbuild as you always have. The devenv invocations are now converted to msbuild options automatically. In addition, this new version:

- Provides increased consistency in the Fortify Static Code Analyzer translation / analysis phases
- No longer requires the Fortify Extension for Visual Studio or Visual Studio in order to scan .NET solutions (.NET framework is required to be installed). To scan from the Visual Studio IDE, the Fortify Extension for Visual Studio is still required
- No longer requires admin privilege to install Fortify Extension for Visual Studio forVisual Studio 2013

For example, the following command:

```
sourceanalyzer -b test devenv Sample.sln /REBUILD
```

will be converted to:

```
sourceanalyzer -b test msbuild Sample.sln /t:rebuild
```

Micro Focus Fortify WebInspect

The following features have been added to Fortify WebInspect.

Checks over WebSockets

The Fortify WebInspect engines can now examine the data traversing WebSockets. This allows us to detect vulnerabilities in modern applications leveraging WebSockets for advanced communication.

Pause-resume Scan Capability on the Command Line

The command line has been updated to support pause/resume of running scans. When you use the Fortify WebInspect command line interface for automation, you will gain greater flexibility, control, and improved parity withexisting API functionality.

Micro Focus Fortify WebInspect Enterprise

The following features have been added to Fortify WebInspect Enterprise.

Improved Sensor Stability

Improvements to thread management in the Fortify WebInspect Enterprise sensors result in significant improvements to sensor stability, reliability, and greater up time.

API Improvements

The following enhancements have been made to the API:

- Existing scan templates may be overridden with workflow and login macros.
- SSC Project Versions can be assigned to any security group.
- When using the temporary file upload endpoint, Fortify WebInspect Enterprise automatically

creates a file identifier rather than requiring your input.

- Endpoints now list which parameters are required or optional.

SmartUpdate

SmartUpdate just got smarter. Now, instead of downloading the entire package, you select the language and version number you require, reducing the amount of content you need to download.

What’s New in Micro Focus Fortify Software 18.10

May 2018

This release of Micro Focus Fortify Software includes the following new functions and features.

Micro Focus Fortify Software Security Center

The following features have been added to Fortify Software Security Center.

Token Management

This release includes a new user interface for managing tokens. You no longer have to use the CLI to create, extend, or revoke tokens. When a token is about to expire, a notification is sent, making interruptions due to expired tokens less likely.

The token management interface can be accessed from the Administration section under Users.

Oracle Partitioning

A new partitioning script for Oracle can increase FPR processing by up to 20%. This results from an increase in the maximum number of processing threads enabled by the enhanced DB Access concurrency.

The partitioning script for Oracle is located in the Fortify Software Security distribution in the following directory: `/sql/oracle/extra/partitioning.sql`.

Micro Focus Re-branding and User Interface Refresh

The user interface has been re-branded and updated to the more modern Micro Focus look and feel.

Audit Assistant Auto-Apply – Automatically Audit Security Issues

With Audit Assistant you can now automatically apply Audit Assistant predictions to mapped analysis tags. Predictions that fall within the confidence threshold are automatically audited.

To Enable Audit Assistant Auto-apply, navigate to the Administrative section, then Configuration, and then Audit Assistant and choose Enable Audit Assistant auto-apply.

JavaScript "Sandbox" API Utility

A number of new scenarios have been added to the JavaScript Sandbox utility. The scenarios provide examples of how to use the Fortify Software Security Center RESTful API, including:

- Creating Application Versions
- Batching User Assignment
- Batching Request Audit Assistant Predictions and Training
- Generating, tracking, and downloading reports

To help you get started, you can access our code and documentation on our github site.

- Code: `https://github.com/fortify/ssc-js-sandbox`
- Documentation: `https://fortify.github.io/ssc-js-sandbox-docs/`.

Access Swagger-generated API Reference Documentation by browsing to "About ->" and then clicking "API Documentation" from within Fortify Software Security Center.

Improved Password Strength

Fortify Software Security Center now leverages the zxcvbn4j password generator (developed by Dropbox) to check password strength when creating new users or self-service password changes. Rather than the traditional hard-coded rules about password requirements, this library is inspired by password crackers and estimates password strength conservatively through pattern matching and other techniques. It recognizes and weighs:

- 30K common passwords
- Common names and surnames according to US census data
- Popular English words
- Common Dates
- Repeats (aaa)
- Sequences (abcd)
- Keyboard Patterns (qwertyuiop)
- L33t speak

This feature is enabled by default. You can configure minimal password strength in

```
<fortify.home>/<context>/conf/app.properties#password.strength.min.score
```

You can also import additional password dictionaries at

- app.properties# password.strength.dictionary.location

Consolidated Proxy Settings

Fortify Software Security Center now uses a consolidated proxy configuration section that can be re-used throughout the application instead of having to individually configure proxy configurations for things like Audit Assistant, bug trackers, etc.

To enable and configure your organization's proxy settings, browse to **Administration -> Configuration -> Proxy**. After your proxy configuration has been saved, you can browse to other areas of Fortify Software Security Center and check the "Use SSC proxy for <Feature>" option to use the proxy settings you configured.

Bug Tracker Plugin Redesign

The bug tracking plugins have been repackaged to leverage a new plugin framework and an OSGi container that helps Fortify Software Security Center avoid collisions.

The JIRA plugin has been rewritten with better comments in cleaner code.

The included bug trackers can be enabled and configured by browsing to **Administration -> Plugins -> Bug Tracking**.

Micro Focus Fortify Static Code Analyzer

The following features have been added to Fortify Static Code Analyzer.

.NET Enhancements

The following languages and frameworks have been added to our .NET support:

- Support for Android and iOS Applications (including Forms Applications) built on Windows using Xamarin

- Support for Azure Projects

Scala Enhancements*

- Fortify Static Code Analyzer now supports scanning Scala applications up to version 2.13
- Support for applications based on the Play framework

*Scanning Scala source code requires a Lightbend license

JavaScript Support

- Support for applications built using the 2016 and 2017 ECMAScript scripting language specifications
- Improved support for scanning Node.js applications

Apple Support

In this release we have added support for:

- Swift 4 and Xcode 9.2 applications
- The latest Objective-C/C++ compilers

Python Support

The following changes have been made to Python:

- Python 3 applications are supported
- Significant performance improvement when scanning large Python applications

Micro Focus Fortify Static Code Analyzer Tools

The following features have been added to Fortify Static Code Analyzer Tools.

Fortify Plugin for Bamboo

We have released a Fortify Static Code Analyzer extension for the Atlassian Bamboo product. It adds the following functionality to Bamboo:

- Integrates Fortify Static Code Analyzer with Gradle, Maven, MSBuild, and Visual Studio (devenv)
- Uploads results to Fortify Software Security Center
- Fail builds based upon user-selected build fail criteria
- Support for all of the languages supported by Fortify Static Code Analyzer

The Fortify Bamboo extension is available through the Atlassian marketplace. From the marketplace, search for Fortify to locate the software, an overview video, and a link to the documentation.

Fortify Security Assistant Extension for Visual Studio

Fortify Security Assistant Extension for Visual Studio provides real-time security analysis and results. Structural and configuration analyzers are built for speed and efficiency, providing instantaneous security feedback as you type. Find vulnerabilities as you write your code to avoid costly security mistakes. Leveraging Visual Studio's native interface, Security Assistant displays security errors alongside Visual Studio errors and provides details and recommendations from the same rich Fortify ruleset used by Fortify Static Code Analyzer.

The Fortify Security Assistant Extension for Visual Studio is available through the Microsoft Visual Studio marketplace.

Micro Focus Fortify WebInspect

The following features have been added to Fortify WebInspect.

Autopass

Autopass is a new, one-portal process for acquiring licenses for WebInspect named users and concurrent users. In addition, it also provides for offline activation. The process has been designed to decrease the manual effort required to secure a WebInspect license.

Micro Focus Re-branding and User Interface Refresh

The user interface has been rebranded and updated to the more modern Micro Focus look and feel.

Multi-User Login Macro (Technical Preview)

Applications that only allow a single active login session prevent multi-threaded scanning. With multiple logins, the threads invalidate each other's state, resulting in slow scan times.

Our multi-user login solution requires you to create multiple login accounts with the same application privileges. Scan settings are then configured so that each scan thread uses a different username and password, which allows the scan to run across multiple threads. Each thread has a different login session, resulting in faster scan times.

This functionality is currently in preview and is not distributed with the release. If you would like to preview the multi-user login macro, please contact Micro Focus Customer Support.

Micro Focus Fortify WebInspect Enterprise

The following features have been added to Fortify WebInspect Enterprise.

Micro Focus Re-Branding and User Interface Refresh

The user interface has been rebranded and updated to the more modern Micro Focus look and feel.

Standalone Proxy Server

A standalone license-free proxy server with associated REST API is available to download via the Marketplace. The standalone proxy enables Fortify WebInspect Enterprise users to spin up and work with the WebInspect proxy without requiring WebInspect licenses to operate. This is particularly useful for automating workflows via traffic capture.

REST API Updates

The following new endpoints are now available via the WebInspect Enterprise REST API:

Add a Scan Requests endpoint in REST API that adds the following abilities:

- GET Scan Requests (/scanRequests/ or projectVersions/{id:long}/scanRequests") returns a paged list of summaries. Clients can specify page size and start, and also whether to filter completed scans.
- GET Scan Request Details (/scanRequests/{id}/) returns details of a specific scan request. This is the full metadata of the request form.
- GET Scan Request Attachment (/scanRequests/{id}/attachments/{attachmentId}/) downloads the relevant scan attachment if available for the specified scan request.
- PUT Scan Request status update (/scanRequests/{id}/action with specified action as defined in the swagger doc or /scanRequests/ put with serialized ScanRequest object) updates the status if allowed on the specified scan request.

Add a scan export endpoint (/Scans/{id}/export) which exports scan to stream response. Allowed types are FPR, Scan, and XML.