Fortify Software

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.

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.

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 HPE Security Fortify Software 17.20

November 2017

This release of HPE Security Fortify Software includes the following new functions and features.

HPE Security Fortify Software Security Center

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

Setup Wizard

The new setup wizard provides an easy-to-use interface:

- External server configuration tool is no longer necessary
- Configuration is stored outside of the SSC WAR, which eliminates the need to redeploy the SSC WAR file when changes to the configuration are made
- You can now seed the database during setup
- Software Security Center enters maintenance mode during upgrades and notifies team members who access the server that an upgrade is in progress

Export to CSV

Fortify Software Security Center users can export data from the dashboard and audit pages of Software Security Center. From the Issue Stats dashboard page or the audit page, group and filter the data you want to see, and then click **Export** to generate the CSV file. Exported CSV files are available for 30 days unless you change the **Days to preserve** setting (Administration > Configuration > Scheduler).

GitHub Repository

A consolidated GitHub page includes samples that demonstrate the flexibility and power of Fortify Software Security Center's refactored and improved RESTful API.

https://github.com/fortify

Issue Found Date

A new introduced date selection in the **Group by** list lets you see when issues were introduced to an application version.

New Plugin Framework

This release includes a completely rewritten plugin framework. The new framework was designed to support dependency isolation in plugins, enable additional plugin types, and provide greater reliability. This initial release supports two plugin types: data parsers and bug trackers.

Updated Bug Tracker Plugins

The default Fortify bug tracker plugins are part of the Fortify Software Security Center distribution package. To integrate a bug tracking system, navigate to the Administration view in Software Security Center and in the Plugins section, upload the required plugins. You can now manage plugins via the user interface rather than editing the WAR.

HPE Security Fortify Static Code Analyzer

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

.NET Enhancements

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

- .NET Core framework
- MVC framework
- Visual Studio 2017
- .NET 4.7
- C# 7
- VB.NET 15
- MSBuild custom tasks (updated)

PHP Enhancements

Fortify Static Code Analyzer now supports scanning PHP through version 7.1. This release includes support for new classes and interfaces introduced in PHP 7.x.

Scala Language Support

We partnered with Lightbend, the creators of the Scala language, to provide support for Scala 2.11 and 2.12.

Scanning Scala source code requires a Lightbend license.

ECMAScript 2015 Support

JavaScript support has been updated to include ECMAScript 2015 applications. We support popular ECMAScript 2015 constructs such as arrow functions and for of loops.

Swift 3.1 Support

Swift support has been updated to include Swift 3.1 and Xcode 8.3 applications.

Java 9 Support

At the time of development, Java 9 was still in Beta. While we support the language changes in Java 9, we do not currently support multi-release JAR files. Even if your application includes multi-release JAR files, Static Code Analyzer can still scan your applications and find vulnerabilities.

High Performance Parallel Mode Update

High Performance Parallel Mode is on by default. You no longer need to use the –mt parameter on the command line or set any property keys to enable High Performance Parallel Mode. If you had previously included the –mt parameter in your scripts, this parameter will be ignored. You do not need to make any changes to already existing scripts.

HPE Security Fortify Static Code Analyzer Tools

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

Smart View in Audit Workbench

Smart View is a new, graphical view of your security issues. This view presents variable-sized colored blocks that represent the relative number of issues by grouping.

Smart View provides:

- A graphical representation of the number of security issues
- Ability to sort security issues by converged dataflow, source, or sink
- Visual map shows how multiple issues are related from a data flow perspective
- Use Smart View filters to help triage and fix issues

When you click the Smart View button, your security issues are grouped and displayed as a number of blocks. Click a block to display the list of issues in the grouping and then click View Issues to apply the Smart View filter to your issues.

Visual Studio 2017 Support

Using our full-featured Visual Studio package, you can scan, view, and audit issues in the Visual Studio 2017 IDE.

Fortify Remediation Plugin for WebStorm IDE by JetBrains

The Fortify Remediation plugin works with Fortify Software Security Center to allow users to view Fortify Project Results (FPR) and audit those issues inside the WebStorm IDE.

Advanced Scanning in Eclipse IDE

In the Fortify Plugin for Eclipse, you can now use Advanced Analysis to scan non-Java projects (JavaScript, C++, Python, and so on) as well as Java projects. When you scan Java projects, you can now specify a different JDK version, classpath, sourcepath, and other analysis options for each project in a single scan.

HPE Security Fortify WebInspect

The following features have been added to Fortify WebInspect.

Accuracy Improvements to Single Page Application (SPA) Support

SPA support is now more robust; we have improved accuracy by expanding support for W3C tests and additional JS frameworks. This results in greater framework support and increased accuracy when fuzzing XHR traffic. Guidance on scanning SPA is available here: https://www.youtube.com/watch?v=7H07kSE491E.

Incremental Scans via GUI and REST API

Incremental dynamic scanning helps with an optimized quick scan, by using scan data from a previously completed scan. In this release, the ability to integrate with end-user workflows has been enhanced. Incremental dynamic scanning is now easier and more reliable via GUI and REST APIs. For more information on running incremental scans: https://www.youtube.com/watch?v=q9kfGkHTxs0

Site Explorer – Standalone Version

Site Explorer can be used as an interactive tool to help remediate vulnerabilities. Rather than relying on static PDF reports, developers using Site Explorer can drill down to the source of the vulnerability. While Site Explorer is still included as part of the WebInspect package, there’s now a standalone, license-free version. This version can be used by developers and doesn’t require WebInspect installation on the developer’s machine. The standalone version of Site Explorer can be downloaded from the marketplace: https://marketplace.saas.hpe.com/fortify/content/site-explorer-demo

WISwag Tool Improvements -- OData Support

The WISwag tool now uses the OData REST API definition to automate the scanning of APIs. With this update, the WISwag command line tool can parse both Swagger and OData formats, resulting in the ability to automate a larger framework of API definitions.

Autopass Licensing for WebInspect Named-User Licensing Model (Technology Preview)

Autopass licensing for WebInspect-named users allows you to activate your licenses online. This process decreases the manual effort in license acquisition and no longer requires visiting more than one portal to complete the licensing and activation process.

REST API Improvement

The WebInspect REST API introduces the following new endpoints to enable better automation capabilities.

- Use the reports endpoint to generate vulnerability and compliance reports.
- Use the merge endpoint to merge scans.
- Use the securebase endpoint to upload a SecureBase database.

The WebInspect REST API modified the **scans** endpoint to enable better automation capabilities. The scans endpoint includes options for scan reuse and incremental scanning.

HPE Security Fortify WebInspect Enterprise

The following features have been added to Fortify WebInspect Enterprise.

Scan Template Configuration UI

Scan template creation, configuration, and management is now handled through the Guided Scan UI. This unified view brings feature parity across WebInspect and WebInspect Enterprise and is now the default configuration UI.

Critical bug fixes and enhancement

WebInspect Enterprise has the following enhancements:

- Fixed WebInspect Enterprise-Software Security Center scan import times. In some cases, large import scans that took days can now be completed in minutes.
- Fixed scan import visualization failures.

What’s New in HPE Security Fortify Software 17.10

April 2017

This release of HPE Security Fortify Software includes the following new functions and features.

This release of HPE Security Fortify Software includes the following new functions and features.

HPE Security Fortify Software Security Center

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

Cloud Controller as a Service

You can now run the HPE Security Fortify CloudScan controller as a Windows service .

Dynamic Scan Results Highlight Request and Response Associated with Vulnerability

Fortify Software Security Center now highlights the attack payload of the request and response from the web server in HPE Security Fortify WebInspect scan results.

Issue Attachments

Attach image files (in jpg, jpeg, bmp, png, or gif format) to an issue during audits.

Audit Assistant Training

Improvements to user feedback tracking due to enhancements in error handling and notifications.

Viewing Issues Assigned to You

Selectively view issues that are assigned to you. You can now see application versions and the number of issues assigned to you on the Applications view. If no issues are assigned to you, an appropriate message displays.

Setting the Audit Conflict Strategy

If an issue is assessed by two different auditors, then the values assigned to a given custom tag might differ. Previously, if Fortify Software Security Center detected an audit conflict such as this, it ignored all client-side changes and resolved the conflict in favor of the existing Fortify Software Security Center custom tag value. You can now change this strategy so that audit conflicts are resolved in favor of the most recent change.

Setting Content Security Policy for Browser Access to Fortify Software Security Center

Determines the Content Security Policy level (strict CSP, relaxed CSP, or disabled CSP) for browsers that access the Fortify Software Security Center domain.

Scheduled Alerts

In addition to performance indicator, variable, and system event alert types, you can now create scheduled alerts that Fortify Software Security Center sends out for the date, time, and time zone that you specify. Scheduled Alerts have a free-text field that you can use to send a custom message to your team.

HPE Security Fortify Static Code Analyzer

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

Swift Improvements

Fortify Static Code Analyzer now allows you to scan source code written in Swift 2.2 and 3.0.2 with support for the Swift MVC Model Class.

Enhanced .NET Support

- Async/await support
- File extension support for WinMD
- Silverlight app support
- VB.NET 14 support
- C# 6 support

High Performance Parallel Scans

Parallel mode now scales to large hardware, takes advantage of all CPU and memory resources available, and is simple to use.

Apex and Visual Force Support

Scan code created using the Salesforce programming language and user interface framework.

AngularJS Technology Preview

A preview release of SCA support for scanning AngularJS 1.x source code. In the preview release, we support MVC, Partials, and UI Router architectures.

- SCA can find AngularJS specific configuration-related issues
- SCA can find dataflow issues, such as Cross-Site Scripting: DOM, in small AngularJS projects

HPE Security Fortify Static Code Analyzer Tools

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

Kerberos Single Sign On Support

Support for single sign on using the Kerberos network authentication protocol has been added to the HPE Security Fortify Package for Visual Studio, HPE Security Fortify Audit Workbench, and the HPE Security Fortify Plugins for Eclipse (Eclipse Complete Plugin).

x.509 Single Sign On Support

Support for single sign on using x.509 public key encryption has been added to the HPE Security Fortify Package for Visual Studio, HPE Security Fortify Audit Workbench, and the HPE Security Fortify Plugins for Eclipse (Eclipse Complete Plugin).

New Custom Tags

Support for new custom tags was added to the HPE Security Fortify Package for Visual Studio (Remediation Package) to provide greater specificity and flexibility in auditing issues.

- Date
- Decimal
- Text

HPE Security Fortify WebInspect

The following features have been added to Fortify WebInspect.

Single Page Application (SPA) Support Technology Preview

Single page applications can now be crawled and audited directly through Fortify WebInspect by choosing a new scan option within the setup GUI. This functionality was initially only available in the DOM Explorer tool.

Bringing SPA support to Fortify WebInspect allows for automated crawl and discovery of additional SPA resources, which was not possible using the DOM Explorer tool.

Visual Studio Team Services (VSTS) Extension

The WebInspect VSTS task allows you to start a dynamic scan from within VSTS. The dynamic scan task will automatically trigger a scan as part of the build process. The scan settings to be used and the output location for the scan artifact are configurable.

Site Explorer Improvements (Export to CSV)

Site Explorer can now export the results in the Findings tab to a CSV file. The data included in the output are modified according to the filters and visibility settings applied to the Findings tab columns.

WISwag Tool Improvements

- The WISwag tool can now be invoked via the Fortify WebInspect REST API.
- The WISwag tool now adds REST API information to the generated scan settings. This provides rich information about the REST service being scanned which Fortify WebInspect can use to find additional vulnerabilities.
- The JSON Schema parser has been updated to better support references.

REST API Updates

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

- POST /securebase/policy – uploads a policy file and adds it to a local SecureBase
- PUT /wie/scan – uploads a scan to WIE and publishes it to SSC
- PUT /scanner/wiswag –invokes the WISwag tool

The “overrides” parameter in the POST /scanner/scans endpoint now allows specifying thread counts.

Platform Support

Fortify WebInspect 17.10 now supports Windows Server 2016 and SQL Server 2016.

HPE Security Fortify WebInspect Enterprise

The following features have been added to Fortify WebInspect Enterprise.

Full Automation

Fortify WebInspect Enterprise is now fully configurable via CLI scripts and REST APIs, allowing you to integrate Fortify WebInspect into your SDLC process.

With automation, you can:

- Configure a scan
- Onboard a sensor
- Onboard and run a scan

Run Fortify WebInspect Enterprise without HPE Security Fortify Software Security Center

You now have the choice to run Fortify WebInspect Enterprise with or without HPE Security Fortify Software Security Center.

REST API

Swagger support for the REST APIs provides a visual representation of the API and includes detailed schema, parameter, and example code information. The REST API support allows you to more tightly integrate with Fortify products:

- REST API is documented in Swagger definition format
- Enhanced REST API includes new endpoints