

What's New in HP Fortify Software Security Center 4.30 and HP WebInspect 10.40 Products

April 2015

This release of HP Fortify Software Security Center includes the 10.40 release of WebInspect and WebInspect Enterprise. The WebInspect products were developed in conjunction with the 4.30 components and are an integral part of the HP Fortify Software Security Center 4.30 release.

HP Fortify Static Code Analyzer

- Core Ruby 1.9 is now fully supported. (It is no longer a technology preview.)
- Java Bytecode is now supported. Enable it using the following properties:
 - `com.fortify.sca.fileextensions.class=BYTECODE`
 - `com.fortify.sca.fileextensions.jar=ARCHIVE`

During the translation phase, specify the jar files and any source files you want to scan.

- Django 1.7 is now supported. Enable it using the following properties:
 - `-Dcom.fortify.sca.limiters.MaxPassthroughChainDepth=8`
 - `-Dcom.fortify.sca.limiters.MaxChainDepth=8`

Note: Do not change the value of these properties. Other values are not currently supported. Do not set these values when scanning non-Django projects as they could negatively impact performance.

During the translation phase, set the switch:

```
-django-template-dirs path/to/template/dirs
```

- The ABAP Parser now supports all ABAP constructs.
- Higher Order Analyzer is provided as a technology preview. For languages other than Java, it enables SCA to perform analysis on higher order functions such as lambdas.

To enable languages for higher order analysis, add a comma-delimited list of languages to the `fortify-sca.properties` file. For example:

```
com.fortify.sca.Phase0HigherOrder.Languages=javascript,ruby,python
```

To enable type inference for languages that are enabled for higher order analysis, add a comma-delimited list of languages to the `fortify-sca.properties` file. For example:

```
com.fortify.sca.TypeInferenceLanguages=javascript,ruby,python
```

- Xcode 6.0, 6.1, and 6.2 are now supported.
 - Xcode 5.0, 5.1, 6.0, 6.1, and 6.2 on Mac OS X 10.9 and 10.10 are supported.
 - Projects targeting any processor architecture, not only i386, are supported.
 - SCA no longer requires that `xcodebuild` command lines include “`-sdk iphonesimulator`”.
 - Build integration with the `llvm-gcc` compiler has been removed; SCA no longer recognizes `llvm-gcc` as the name of a compiler.
 - Build integration with Xcode 4.5 and 4.6 has been removed.

HP Fortify Software Security Center

- Using the new Administration section of the user interface (UI), you can now:
 - Specify many of the settings that were previously in the configuration tool.
 - Use a wizard to create new applications and versions.
 - Generate reports.
 - Create and manage alerts.
 - Filter, group, and aggregate Bar charts, Trend charts, and Table charts by custom attributes.
- Data purging performance has been greatly improved.
- FPR processing performance has been greatly improved.

HP Fortify Runtime Products: Runtime Application Logging, Runtime Application Protection, and WebInspect Agent

The installation of Runtime agents for the following products has been greatly simplified:

- Runtime Application Protection (RTAP)
- WebInspect Agent
- HP ArcSight Application View

HP Fortify GUI Tools

- Bug tracking support has been added for Application Lifecycle Manager 12 and Jira 6. GUI Tool properties are described in the *HP Fortify Static Code Analyzer Tools Properties Reference Guide*.
- There is a new scanning plugin for IntelliJ 13 and Android Studio.
- Microsoft has deprecated command-line support for Visual Studio 2015. Microsoft will need to reestablish command-line support before HP can address this.

WebInspect Version 10.40

- WebInspect Software Development Kit (SDK)

After the successful release of the WebInspect API a year ago, customers asked for deeper integration with WebInspect to get the most out of the product. The WebInspect team has developed a full SDK so that customers can write their own vulnerability checks, called custom agents, for direct consumption by the WebInspect engines. The SDK is distributed as a Visual Studio starter kit and includes documentation, code samples, and templates to assist users in writing their custom agents. Once created, custom agents can be published to WebInspect or WebInspect Enterprise to be used in scans. For more information, see the “About the WebInspect SDK” topic in the WebInspect help.

- Merge Scan Files

An option has been added to the WebInspect command line utility that allows customers to merge the results of multiple scans into a single scan. Users can now split large websites into smaller scans and merge the results back together. For more information, see the “Command Line Execution” topic in the WebInspect help.

- Vulnerability Rollup

Application developers reuse code to the extent that sometimes every page in an application uses the same code. If a reused piece of code, such as a search bar, has a vulnerability, then WebInspect may report that vulnerability dozens or even hundreds of times. Users can now roll up all of these vulnerabilities into a single parent vulnerability for easier reporting to management and development. For more information, see the “About Vulnerability Rollup” topic in the WebInspect help.

- SmartUpdate – **Checks** and **Policies** Tabs

Users can now easily identify which policies will be affected by an addition or change in a vulnerability check when they run HP SmartUpdate. Two new tabs on the SmartUpdate window, **Checks** and **Policies**, allow users to see which policies are affected by a specific check or which checks are affected in a given policy. This information helps users understand whether the differences between scans are due to a change in WebInspect or a change in the application being scanned. For more information, see the “SmartUpdate” topic in the WebInspect help.

- WebInspect Feedback Program

The WebInspect team has built a telemetry server and added telemetry functionality to WebInspect, which allows customers to choose to send important **generic** information about how the application is performing. This information will help the engineering and research teams more quickly identify ways to improve the product for higher quality results.

- Additional Supported Systems

WebInspect now supports Windows Server 2012 R2, SQL Server 2012 SP2, and ALM 12 as well as Internet Explorer 11 and Firefox 33.

- Performance

The WebInspect team has been focusing on performance improvements over the last few releases. Customers may again notice a decrease in scan times as further updates and fine tuning have resulted in additional performance gains with WebInspect 10.40.

WebInspect Enterprise Version 10.40

- WebInspect Enterprise Search

WebInspect Enterprise is designed for companies to run and store dynamic scans on all of their applications, no matter how many that may be. However, the security professionals running the scans may not be familiar with every project and may not have re-scanned a particular URL for a year or more. WebInspect Enterprise now gives users a way to search for information such as application names, version names, and URLs. Now, even with 1000 applications stored in their WebInspect Enterprise server, users can find exactly what they are looking for quickly and easily. For more information, see the WebInspect Enterprise Web Console help.

- Scan Template Change Inheritance

Any changes made to scan templates can now be propagated out to currently scheduled scans that use the template being updated. Customers can now change the settings of large numbers of scheduled scans without needing to modify each schedule individually. For more information, see the “Scan Template - Scan: General” topic in the WebInspect Enterprise Web Console help.

- SSC Scan Request Data Harvesting

Now, when a user creates a scan from an SSC scan request, the URL will be copied over for them automatically. WebInspect Enterprise determines the start URL from the data in the Scan Request that was sent from SSC. The Scan Wizard opens and the Start URL field is auto-filled with the URL from the scan request. The URL, Username, and Password fields are also right-clickable to allow users to copy the data to the clipboard. For more information, see the “Using Scan Requests from SSC” topic in the WebInspect Enterprise Web Console help.

- Server Setup Verification Checks

As a part of the WebInspect Enterprise installation, checks will now be run to validate that the server has been set up correctly and that users have the correct permissions. This will help customers avoid needless support calls or odd behavior of their installation. For more information, see the *WebInspect Enterprise Installation Guide*.

What Was New in 4.21

SSC Software Version 4.21

WebInspect Products Software Version 10.30

October 2014

This release of HP Fortify Software Security Center includes the 10.30 release of WebInspect and WebInspect Enterprise. The WebInspect products were developed in conjunction with the 4.21 components and are an integral part of the HP Fortify Software Security Center 4.21 release.

HP Fortify Static Code Analyzer

Enhanced Python 2.7.x Support—The Python analyzer adds support for 25 new rules categories, 60 built-in categories, and 60 additional built-in modules. In addition, the Python analyzer includes the following enhancements:

Import Processing

- Import processing now correctly handles different forms of import statements
- Improved resolution of nested modules
- Ability to import a class that has the same name as the module in which it was defined

File Set Processing

- Parses only used modules; no longer includes all modules in the `-python-path` regardless of whether or not they are used
- Removed requirement to add the analyzed project root directory to the `-python-path` parameter to resolve the project's modules
- Improved support of symbolic links used as values with the `-python-path` parameter
- Fixed the bug that prevented use of absolute path in the `-python-path` parameter on MS Windows systems

Diagnostics Improvements

Removed the double printing of warnings about unresolved imports to the log file and corrected the source location information.

Corrections and Enhancements made to Language Constructs

- Exception handling blocks (`try/except/finally`)
- Named function arguments
- Slices and array subscriptions
- `Break`, `continue` statements
- `Exec` statement

Quick Scan—Quick Scans provide a starting point for your investigation. Use a Quick Scan to quickly scan your code. Quick Scans provide a subset of the findings of a full scan. Quick Scans are not a replacement for a full scan, but rather a means of generating preliminary information that your team can immediately begin to address. A Quick Scan can be launched from an SCA command line or through the Advanced Scan in *HP Fortify Audit Workbench*.

Technical Previews

Technology Preview features are currently unsupported, may not be functionally complete, and are not suitable for deployment in production. However, these features are provided to the customer as a courtesy and the primary objective is for the feature to gain wider exposure with the goal of full support in the future.

Ruby Technical Preview—An advance look at scanning code created using core Ruby version 1.9. This preview supports standard libraries, rack, MySQL, MySQL 2, Thor, thin, lambdas, and gem translation.

ABAP Parser Technical Preview—An advance look at a more robust ABAP parser. This technology preview provides better findings in most cases.

Buffer Analyzer Technical Preview—An advance look at a new and improved solver, CVC4. It provides improved precision in handling nested loops and incorporates a number of bug fixes.

HP Fortify Software Security Center

SSC Performance Improvements—Significant reduction in the time it takes to simultaneously process multiple FPRs.

Faster Report Generation and One-Click Mapping—Five report types (CWE/SANS Top 23, DISA STIG, FISMA, OWASP Top 10, and PCI) have been migrated to a new format that is much faster to generate and provides one-click access to mapping options.

Quick View—A filter designed to surface the most important issues, based on SSC Priority Order impact and likelihood metrics. When selected, the Quick View filter hides all medium- and low-priority findings that have a lower impact on source code security. It also hides findings that have a high potential impact but are least likely to be exploited.

HP Fortify Runtime Products: Runtime Application Logging, Runtime Application Protection, and WebInspect Agent

Java 7 and Java 8 Support—HP Fortify Runtime products now support Java 7 and Java 8 runtime environments.

HP Fortify Audit Workbench and GUI Tools

Jenkins Plugin—The HP Fortify Jenkins Plugin (Jenkins plugin) is used in conjunction with HP Fortify Software Security Center (SSC). If you scan your source code after each build, the Jenkins plugin automatically uploads the Fortify project results (in an FPR file) to an SSC server and enables you to view the details within Jenkins. It also provides metrics for each build and an overview of the results.

Enhanced Visual Studio 2013 Support—Added support for AND/OR syntax and compatibility with collaborative bugtrackers to the HP Fortify Visual Studio packages.

Maven 3.x Support—Added support for Maven version 3.x.

IntelliJ 13 Support—Added support for IntelliJ version 13 to the HP Fortify Remediation Plugin for JetBrains IntelliJ IDEA package.

WebInspect Version 10.30

64-bit and 32-bit Installation packages—WebInspect is now available in both 32- and 64-bit installations. The 64-bit architecture allows WebInspect to take better advantage of additional system memory and enables it to crawl and audit sites with larger memory footprints and provide a higher degree of parallel processing, resulting in a net performance improvement. This improvement should be seen in both standalone WebInspect and WebInspect Enterprise sensors.

Japanese language version—HP Fortify WebInspect 10.30 is available with either an English or Japanese interface.

.Net 4.5.1—WebInspect's core scan engine now uses the .NET 4.5.1 common language runtime (CLR) and takes advantage of a special feature called Large Object Heap Compaction. This compacting process prevents heap fragmentation which has previously contributed to out of memory errors. This API combined

with the additional memory overhead afforded by 64-bit processes will allow scans to take full advantage of the resources available.

Performance Improvements—The WebInspect 10.30 release includes several behind the scenes enhancements and optimizations that improve the performance of WebInspect. These enhancements and optimizations, in combination with the architecture changes, should yield a noticeable improvement in scan performance.

Expansion of the WebInspect API—The WebInspect API has been expanded to allow manual vulnerabilities to be added to a scan remotely. As an example of this and our other API functionality, we have built and published a plugin for the BURP suite. Customers familiar with the BURP suite can retrieve the plugin jar file installed with WebInspect or download the plugin from the BApp store and install the plugin to combine any work done in BURP with the enterprise-level reporting and scanning capabilities of WebInspect and the rest of the Fortify software security suite.

Scan Comparison View—The upgraded scan comparison view now allows customers to compare the vulnerabilities and site structure (trees) between two scans. By showing the union and distinctions between the two scans, both WebInspect and WebInspect Enterprise customers will be able to pinpoint changes made to an application.

Dashboard Enhancements—In an effort to reduce customer confusion around scan activity and completeness, the scan dashboard has been modified to split the audit progress bar into four separate progress bars, each representing a specific part in the scan cycle. Each bar also states the number of sessions in its queue and how many of them have been processed. Network and computational activity graphs have also been added to the dashboard to better inform users how much activity the scan is performing.

Additional Supported Systems—WebInspect adds support for Windows 8, Windows Server 2012, SQL Server 2012, ALM 11.5, and ALM 11.52.

Support for Windows Devices Added to Mobile Testing UI—Windows Phone and Windows RT have been added to the User Agents list for mobile Web site scans. This means that WebInspect can now impersonate either of these platforms to render and test a mobile Web site.

Support for the Windows Phone platform has also been added to the native mobile Web service scan. Traffic from a physical Windows Phone device or an emulator can be captured by the proxy and used to identify vulnerabilities in the backend servers.

WebInspect Enterprise Version 10.30

64-bit WebInspect Enterprise Sensors—The WebInspect scan sensors are now available in both 32- and 64-bit installations. The 64-bit architecture allows

WebInspect to take better advantage of additional system memory and enables WebInspect to crawl and audit sites with larger memory footprints and provides a higher degree of parallel processing, resulting in a net performance improvement.

64-bit WIE admin console—The WebInspect Enterprise Admin Console will now be released in 64 and 32 bit versions. The upgrade to 64 bit will allow the console to take advantage of additional system memory for smoother performance.

Scan Comparison—The upgraded scan comparison view now allows customers to compare the vulnerabilities and site structure (trees) between two scans. By showing the union and distinctions between the two scans, both WebInspect and WebInspect Enterprise customers will be able to pinpoint and track changes made to an application.

Dashboard Enhancements—In conjunction with the dashboard updates of WebInspect, the scan visualization dashboard in WebInspect Enterprise has been updated to provide additional insight into scan activity and progress. Activity meters have been added to show network and computational activity. The progress bars now show all sessions in the queue and the audit progress bar has been split into four separate progress bars, each showing a different part of the audit process.

What Was New in 4.10

April 2014

HP Fortify Static Code Analyzer

Python 2.7.x—HP Fortify SCA now supports Python version 2.7.x. There were also improvements made to the parsing engine including the processing of import statements to resolve modules.

Support for XCode 5—XCode 5 support was added.

C++ Improvements—Translation quality has been significantly increased. The control-flow and dataflow analyzers have been improved. A new CPFE has been enabled by default; the previous version of the CPFE is still available and can be invoked with the `-use-cpfe441` command-line option.

Microsoft Visual Studio 2013 and .NET 4.5.1—Support for the latest version of Microsoft Visual Studio and the .NET framework have been added.

HP Fortify Software Security Center

Reporting and Grouping—The Vulnerability Report is now available in SSC. You can generate a report based on WebInspect Enterprise dynamic testing results.

The DISA STIG 3.5 report (that is, the Defense Information Systems Agency, Security Technical Implementation Guide report, version 3.5) and grouping are now available.

The OWASP 2013 report (that is, the Open Web Application Security Project Top 10 report, 2013 version) and grouping are now available.

HP Fortify Runtime Products: Runtime Application Logging, Runtime Application Protection, and WebInspect Agent

Performance Improvement in WebInspect Agent — We improved the attack surface filtering for WebInspect Agent to increase WebInspect's overall performance and better focus its attacks.

Improved Application View Functionality and Visibility in HP ArcSight ESM

Performance Improvement in HP ArcSight ESM — Event generation and processing are now faster in Application View.

Platform Support — All Runtime products now support additional platforms. Please refer to the *HP Fortify Software Security Center System Requirements* document for details.

Setup Wizard Improvements — Improved setup wizard now supports more platforms.

The Size of the Installed Runtime Products has Been Reduced

Improved Compatibility with Syslog Servers

HP Fortify Audit Workbench and GUI Tools

Additional Platform and OS Support—GUI Tools now support Visual Studio 2013, Mac OSX 10.8, and Eclipse 4.3 (Kepler). For a complete list of platform and OS support, see the *HP Fortify Software Security Center System Requirements* document.

WebInspect Version 10.20

Native Mobile Scanning—Manually crawl a native mobile application and capture the Web traffic as a workflow macro. Once captured, the HTTP traffic from the Android or iOS app directed to the backend service can be replayed and security tested using WebInspect’s standard set of manipulation, fuzzing and injection attacks. There is a new policy specifically added to bundle mobile checks.

WebInspect Agent Improvements—The WebInspect Agent (formerly SecurityScope) is now available with WebInspect at no additional cost and has deeper integration with the UI and the scan engine. Agent compatibility is now detected by the pre-scan profiler and installation links are presented in the UI when compatibility exists. The agent also operates in a new active mode that can suggest attack strategies to WebInspect to improve accuracy and performance.

Seven Pernicious Kingdoms Taxonomy—Seven Pernicious Kingdoms is a taxonomy of software security errors developed by the Fortify Software Security Research Group together with Dr. Gary McGraw. This taxonomy is designed to help developers and security practitioners understand common types of coding errors that lead to vulnerabilities. By organizing these errors into a simple taxonomy, developers can easily recognize categories of problems that lead to vulnerabilities and identify existing errors as they build and test software.

FIPS Compatibility—WebInspect can now run in Windows environments configured for compliance with the Federal Information Processing Standards (FIPS).

Mobile Site Scanning via Browser Impersonation—Mobile sites can be scanned with custom user agents or popular mobile platform user agents like Safari or Chrome for Android. In this mode, WebInspect scans the site content as it would be rendered to a mobile browser.

WebInspect API—In addition to the command line tool, WebInspect now exposes a REST service endpoint to allow remote clients to configure, control, and retrieve data from scans.

Significant Improvements to the JavaScript Engine—Improved support for HTML5 and modern Web standards by upgrading to the latest Gecko engine. Performance improved by intelligently eliminating redundant script execution.

Updated Web Macro Recorder

- Native HTML5 recording support
- Improved accuracy
- Upgraded to the latest Gecko engine

Improved HTML5 Support—DOM manipulation using HTML5 features for client side auditing.

Updated Platform Support

- Windows 8
- Windows Server 2012
- IE 10

License and Infrastructure Manager (LIM) Now Delivered via WebInspect Install—The LIM is no longer a separate purchase. LIM 3.0 is a simple Windows installer file that resides on the file system after WebInspect is installed.

Auto-Detect CSRF Tokens and Reconfigure Scan Settings

Burp Imports—WebInspect can open Burp files in the Web Proxy tool and can import Burp Traffic as Workflow Macros.

Added Support for GWT Scanning

WebInspect Enterprise Version 10.20

AMP Migration—During WebInspect Enterprise 10.20 installation, you can migrate an AMP version 9.20 database, which is automatically converted to the WebInspect Enterprise database schema, and you can optionally migrate the AMP 9.20 user accounts to SSC user accounts. During and/or any time after the installation, you can migrate the AMP sites you select to SSC project versions.

Reporting—WebInspect Enterprise allows you to create the following scan-level reports: Alert View, Attack Status, Compliance, Crawled URLs, Duplicates, Executive Summary, False Positive, QA Summary, Scan Log, Vulnerability, and Vulnerability (Legacy).

Auto-Publish to SSC—New scans whose associated project versions are Finished are automatically published to SSC.

Added Support for:

- Windows 8 for the Administrative Console
- Windows 8, Windows Server 2008 SP2, and Windows Server 2012 for the WebInspect Enterprise sensor
- Internet Explorer 10 and Firefox 26 for the WebInspect Enterprise sensor

Native Mobile Scanning—You can manually crawl a native mobile application and capture the Web traffic as a workflow macro. Once captured, the HTTP traffic from the Android or iOS app directed to the backend service can be replayed and security tested using WebInspect Enterprise’s standard set of manipulation, fuzzing and injection attacks. There is a new policy specifically added to bundle mobile checks.

WebInspect Agent Improvements—The WebInspect Agent (formerly SecurityScope) is now available with WebInspect Enterprise at no additional cost and has deeper integration with the UI and the scan engine. Agent compatibility is now detected by the pre-scan profiler and installation links are presented in the UI when compatibility exists. The agent also operates in a new active mode that can suggest attack strategies to WebInspect Enterprise to improve accuracy and performance.

Seven Pernicious Kingdoms Taxonomy—Seven Pernicious Kingdoms is a taxonomy of software security errors developed by the Fortify Software Security Research Group together with Dr. Gary McGraw. This taxonomy is designed to help developers and security practitioners understand common types of coding errors that lead to vulnerabilities. By organizing these errors into a simple taxonomy, developers can easily recognize categories of problems that lead to vulnerabilities and identify existing errors as they build and test software.

FIPS Compatibility—WebInspect Enterprise can now run in Windows environments configured for compliance with the Federal Information Processing Standards (FIPS).

Mobile Site Scanning via Browser Impersonation—Mobile sites can be scanned with custom user agents or popular mobile platform user agents like Safari or Chrome for Android. In this mode, WebInspect Enterprise scans the site content as it would be rendered to a mobile browser.

Updated Web Macro Recorder

- Native HTML5 recording support
- Improved accuracy

- Upgraded to the latest Gecko engine

Burp Imports—WebInspect Enterprise can open Burp files in the Web Proxy tool and can import Burp Traffic as Workflow Macros.

Other Improvements Based on Updates to the WebInspect Sensor (see the *WebInspect Version 10.20* section above):

- Significant Improvements to the JavaScript Engine
- Improved HTML5 Support
- Auto-Detect CSRF Tokens and Reconfigure Scan Settings
- Added Support for GWT Scanning

What Was New in 4.00

September 2013

HP Fortify Static Code Analyzer

Speed Increases through Parallelization—HP Fortify SCA is now up to ten times faster because we take advantage of multiple CPUs and cores within a single machine.

Improved Quality of Results—Updates to global class modeling and improvements in limiters have led to a significant reduction in false positives without increasing false negatives.

Client Upgrade Detection—Audit Workbench and IDE plug-ins can be configured to check Software Security Center for updates, making it easier to deploy clients across an organization.

Default C/C++ Translator Upgrade—We have improved the C/C++ Translator. It could previously be invoked with the `-use-new-cpfe` option, but it is now enabled by default. This upgrade fixes a variety of bugs in C/C++ analysis and enables limited support of C++11 features (such as lambda expressions, rvalue references and variadic templates). The former default C/C++ translator is disabled but can be invoked if needed by specifying the `-use-cpfe39` option on the `sourceanalyzer` command line during the translation phase.

HP Fortify Software Security Center

Performance Improvements—We have improved background job processing so that multiple FPR uploads can be processed at one time without affecting the web interface. We have also made several general performance and scalability improvements to Software Security Center.

Support for Multiple LDAP Servers—You can now configure Software Security Center to interoperate with multiple LDAP servers for user authentication. As with earlier releases, you configure the first LDAP server using the Software Security Center Configuration Tool. You must configure additional LDAP servers manually. For configuration instructions, see the *HP Fortify Software Security Center Installation and Configuration Guide*.

Client Upgrades—Software Security Center can host multi-platform client installers for the Static Code Analyzer applications. This lets you make easier upgrades across your organization by upgrading Software Security Center first.

HP Fortify Runtime Products: Runtime Application Logging, Runtime Application Protection, and SecurityScope

New HP ArcSight Application View—Fortify released a new solution based on Fortify Runtime that provides application layer security logging and visibility to HP ArcSight ESM customers.

Improved Performance Tuning— To support Application View, we have implemented improved tuning and new rules configuration settings for Application Logging.

Installer Improvements—We made a maintenance update to improve installation times and reduce the steps required to install Runtime.

HP Fortify Audit Workbench

Upgrading the HP Fortify Static Code Analyzer Suite from Audit Workbench—You can now check on the availability of new Static Code Analyzer suite versions from the Audit Workbench user interface. If a version newer than the one you have installed is available, you can download it and upgrade your instance. For details, see the *HP Fortify Audit Workbench User Guide*. You can also configure Audit Workbench to check for, download, and install new versions automatically at startup.

What Was New in 3.90

July 2013

HP Fortify Software Security Center

Results Processing—We have improved the way we process results in order to provide better information for your team. Now, new scan results are merged more quickly with past results so you can track the progress of a particular application over time with efficiency.

Improved Performance for Simultaneous Users—Response times are faster now for multiple users working to triage security issues through both the web interface and IDE remediation plug-ins.

HP Fortify Static Code Analyzer

Xcode 4.6—We added support for Xcode 4.6 and iOS 6.1.

Eclipse 4.2—We added support for Eclipse 3.8 (Indigo) and 4.2 (Juno) for both auditing and scanning, and also as a remediation plug-in.

Support Diagnostic Tool—We added a new support diagnostic tool to Audit Workbench to provide platform and log information on support tickets. This tool is available at `Help->Contact Support`.

HP Fortify Runtime Products: Runtime Application Logging, Runtime Application Protection, and SecurityScope

Setup Wizard—The installers for the Java versions of runtime products now include a Setup Wizard which automatically configures the web application server (Tomcat, JBoss, WebLogic, and WebSphere) to invoke the runtime.

Unified Logging—HP Fortify Runtime Application Logging now supports unified logging. If an application is using one of the following frameworks: Log4j, java.util.logging, Apache Common Logging, Slf4j, Log4Net, NLog, or Microsoft Enterprise Logging Library, logs can automatically be redirected from within the application through the syslog connector to ArcSight ESM. This avoids the creation of custom connectors and custom parsers to get information from the log files into ArcSight ESM. With this release, Runtime Application Logging can also record all queries that an application executes against the database.

Improved Integration with WebInspect—The HP Fortify SecurityScope component of WebInspect Real-Time was improved and it now supports five additional categories of vulnerabilities: Leftover Debug Code, Value Shadowing, Open Redirect, Insecure Randomness, and Validation Traces.

Minor Improvements

Software Security Center

- Integration improvements when deploying Software Security Center on WebSphere 8, WebLogic, and DB2.

Static Code Analyzer

- It is easier now to navigate through your scan results within Visual Studio.
- Audited issues in Audit Workbench and the IDE plug-ins load faster in 3.90.
- We have updated ASP.NET's ASPX compiler integration for .NET 4.5 projects.
- SCA 3.90 has an updated COBOL language translator.
- During the translation phase, SCA now provides updated PHP parsing and file resolution via `include()` and `require()`, whose relative paths may be provided by `-php-source-root <path>`.

What Was New in 3.80

February 2013

HP Fortify Software Security Center

Batch Bug Management—Development teams can group security issues together and track them within the Software Security Center bug-tracking system. Software Security Center uses selection criteria to specify which issues to include (for example, those that have been manually audited and deemed “exploitable”); then it applies a grouping strategy to combine multiple issues into specific bugs (for example, “by category, then file”). The program then uses subsequent SCA and WebInspect scans to perform state management of the bug, to determine whether the security issue remains or has been properly remediated.

Manual WebInspect Results Import—When your development or security team imports WebInspect’s dynamic analysis results, the Audit Issues interface will differentiate between issues found by WebInspect’s automated analysis and issues that were manually identified by a dynamic tester.

HP Fortify Static Code Analyzer

Visual Studio 2012 Support—HP Fortify SCA adds scanning abilities for software compiled against .NET 4.5 and Visual Studio 2012, and enables you to audit inside Visual Studio 2012.

Eclipse Remediation Plug-in—HP Fortify added a lightweight plug-in for Eclipse that helps developers and security leads triage security issues from Software Security Center. (This is in addition to the existing Auditing and Scanning plug-in.) The Eclipse remediation plug-in can be served from Software Security Center’s Eclipse update site, and any changes you make in this plug-in happen directly in Software Security Center.

Improved Syntax for Searching or Prioritizing Issues in Project Templates—Audit Workbench and Software Security Center feature a new search syntax that enables you to use both “AND” and “OR” operators to group the conditions in your search string.

Minor Improvements

Software Security Center

- Administrators can update rules directly from HP Fortify, or they can do a manual upload of Rulepacks either individually or as a zip file.
- Disk space utilization is improved for those who open collaborative audits on WebSphere.
- The ability to group issues by extensible metadata is improved. (This affects PCI-DSS, STIG, and other compliance mappings.)
- We have added support for the C89 compiler.

Static Code Analyzer

- The ability to group issues by extensible metadata is improved. (This affects PCI-DSS, STIG, and other compliance mappings.)
- Scan time has been improved.
- We upgraded the versions of LLVM and Clang used in our systems, to provide better support for customers using iOS6 SDK and to improve Objective C scanning.
- Audit Workbench now offers a quick audit option. (See HP Fortify Audit Workbench User Guide for more information.)
- Font sizes in Audit Workbench and other GUI tools now change automatically when you change the size in your system.

What Was New in 3.70

November 2012

HP Fortify Software Security Center 3.70 (Software Security Center) was a minor release focused on stability and performance, rather than new features.

HP Fortify Software Security Center

Combined Reports for Static (HP Fortify Static Code Analyzer, or SCA) and Dynamic (WebInspect) Issues—Updated reports provide a more comprehensive mapping of dynamic results into the Seven Pernicious Kingdoms report. This helps showcase results of static and dynamic application assessments in the same security tracking system, following the vulnerability taxonomy available at <http://www.hpenterprisesecurity.com/vulncat/>

Updated STIG Reporting—Improved reports provide more information about project attributes, and also leverage extensible metadata.

eLearning Integration—A direct link between Software Security Center and the HP Fortify eLearning portal provides developers and security leads with easy access to computer-based training.

HP Fortify Static Code Analyzer

Improved PHP Parsing—Improved translation and parsing for PHP 5.3 now includes PHP namespaces, anonymous functions, and other language features.

Updated Xcode Compatibility—SCA now supports more recent versions of Xcode and provides smoother compiler integration.

Improved C/C++ Translation—We upgraded the C/C++ translator to improve the parsing capabilities of C++ 11, Unicode compatibility, and various Visual Studio solution files. The updated translator is disabled by default for compatibility. (To use the new translator, specify `-use-new-cpfe` during the `sourceanalyzer` translation phase.)

Search Auto-complete in Audit Workbench—This feature assists users in locating particular security issues within Audit Workbench. You can search within a particular folder, or across all folders within a project template.

Updated Installation Process—We now have installers on all platforms; not just Windows. And our new, smaller installation package makes it possible to perform automated (silent) installations of SCA and Apps.

HP Fortify SecurityScope

Enhanced Vulnerability Detection—This includes unused parameters, user authentication, and Java 7 I/O.

Improved .NET Application Analysis—Our security analysis of .NET applications that use RESTful services is now deeper and more thorough.

GUI-based Runtime Configuration Editor—This makes it easier for users to customize their analysis configurations.

New Runtime Diagnostic Tool—This analyzes your system for issues that could impact SecurityScope installation or operation.

Sleeker, Quicker Installer—The new installer works for all platforms, including Linux. There is now a single install image for each supported platform which contains all of the Runtime features in a single package.

Bugs Eliminated—Issues related to duplicate XSS findings, SQL Injection detection, and SSN detection have been resolved.

HP Fortify Runtime Application Protection (formerly HP Fortify Real-Time Analyzer)

New and Enhanced Vulnerability Detection—Improvements have been made in hidden field manipulation, leftover debug code, and Java 7 I/O.

ArcSight ESM SIEM Logging—Runtime can now log application events and security vulnerabilities to ArcSight ESM SIEM.

GUI-based Runtime Configuration Editor—This makes it easier for users to customize their analysis configurations.

New Runtime Diagnostic Tool—This analyzes your system for issues that could impact Runtime Application Protection installation or operation.

Sleeker, Quicker Installer—The new installer works for all platforms, including Linux. There is now a single install image for each supported platform which contains all of the Runtime features in a single package.

Bugs Eliminated—Issues related to duplicate XSS findings, SQL Injection detection, and SSN detection have been resolved.

Minor Improvements

Software Security Center

- Ability to import rules as zip files, rather than as individual xml or bin files.
- Updated AD/LDAP configuration and look-ups
- Improved processing of extensible metadata compliance mapping rules
- Ability to clean old events from HP Fortify Runtime Application Protection

Static Code Analyzer

- Updated underlying Eclipse version to take advantage of the latest Eclipse features and provide an improved user experience

What Was New in 3.60

September 2012

HP Fortify Software Security Center

WebInspect Enterprise Integration—HP Fortify has added support for WebInspect Enterprise, a system to centralize and scale the production of dynamic scans. Developers can use Software Security Center to request a dynamic scan and then view the unified static and dynamic results from Software Security Center.

Extensible Metadata—You can now map scan results to external lists. This separates mappings from scan rules, making it easier to correlate results with compliance mappings such as custom internal application security standards.

Folder Tracking—This new feature enables central security teams to track variables and performance indicators within a specific folder more easily. Sample data includes key performance indicators such as “Number of Exploitable issues inside the Critical folder” and “Percentage of issues in the Critical folder audited as ‘Not an Issue.’”

Collaborative Audit Bug-Tracking Workflow—Developers can now more easily submit individual security vulnerabilities into bug-tracking. Thick client applications will use the bug-tracker configuration from Software Security Center when opening a collaborative audit from Audit Workbench or an IDE plug-in.

Improved Search Capabilities—You can now search for users based on their roles within Software Security Center.

Purging—It is now possible to purge data by using web services or through the command line, regardless of the purge date. Note: If the specified purge date is more recent than any of the existing scans, the most recent scans of each engine type are left untouched, and all other scans in the project version are purged.

Analysis Result Processing Rule—HP Fortify now provides a rule for automatically verifying the certification of the FPR.

HP Fortify Static Code Analyzer

Java 7 Support—HP Fortify now provides support for scanning source code written against the Java 7 platform. (HP Fortify still supports Java 1.4, 5, and 6.)

Extensible Metadata—You can now map scan results to external lists (such as OWASP 2010, PCI 1.2, and CWE) after your scans are complete. This separates mappings from scan rules, making it easier to correlate results with compliance mappings such as industry-specific requirements or custom internal application security standards. Mappings can now be updated quarterly, along with Rulepacks, which means that new standards (such as OWASP 2013) can be added in advance of the next product release.

ABAP Enhancements and BSP Support—HP Fortify now supports coverage of ABAP BSPs. HP Fortify Static Code Analyzer (SCA) includes a new extractor to assist with retrieving ABAP code from SAP NetWeaver so that it can be scanned by SCA or HP Fortify CloudScan.

Xcode 4.3 Support—HP Fortify now supports Xcode 4.3 for Objective-C.

Collaborative Audit Bug-Tracking Workflow—Developers can now more easily submit individual security vulnerabilities into bug-tracking. Thick client applications leverage the bug-tracker configuration from Software Security Center when opening a collaborative audit from Audit Workbench or an IDE plug-in.

WebInspect Attachment Visualizations—In Audit Workbench and the Eclipse plug-in, screenshots and attachments retrieved by WebInspect’s dynamic assessments are now displayed to help developers better understand dynamic scan results.

HP Fortify WebInspect Real-Time

CAPTCHA Support—HP Fortify has added support for major CAPTCHA frameworks so that WebInspect accurately submits CAPTCHA answers.

Minor Improvements

Software Security Center

- Improved performance through issue caching
- Upgraded, more responsive, interface to Flex 4/Adobe Flash player 10
- Improved ability to create custom reports against results from Fortify Real-Time Analyzer (RTA)

Static Code Analyzer

- Extracted custom rules editor to an individual process
- Additional options available within Scan Wizard

What Was New in 3.50

May 2012

HP Fortify Software Security Center

Change Project Template—Security teams may re-prioritize issues for a particular project version by changing the associated project template. Issues and folders can be re-ranked based on current threats and compliance obligations.

Copy Project Versions—It is now simple to copy project attributes, access provisioning, and initial scan data from one project version to seed the next.

HP Fortify Static Code Analyzer

Objective-C Support—Objective-C Support enables scanning of applications and frameworks written in Objective-C. Scanning can be done through the newly added integration with the Xcodebuild command-line interface. New Rulepacks will soon be available to provide insight into Objective-C vulnerabilities with an emphasis on iOS applications.

IntelliJ Remediation Plug-in—Collaborative auditing of Software Security Center results is now possible, by way of a lightweight plug-in for IntelliJ. This guides development teams to scan periodically in the build environment, publish results into HP Fortify Software Security Center, and then triage and remediate issues from IntelliJ. (Note that this plug-in does not provide scan capabilities.)

508-Compliant Interface—Compatibility has been improved between screen-reading applications such as JAWS from Freedom Scientific and the HP Fortify interfaces (Software Security Center, Audit Workbench, the HP Fortify plug-in for Eclipse, and the HP Fortify Package for Microsoft Visual Studio).

Minor Improvements

Software Security Center

- New scan-processing rule to validate that your SCA and Software Security Center versions are compatible
- The ability to specifically download a backward-compatible FPR for viewing in an older version of Audit Workbench
- Improved archive capacity for RTA events
- Improved PCI DSS 2.0 compatibility and reports

Static Code Analyzer

- Improved extraction and translation of SAP ABAP code

- Ability to scan partial classes of .NET applications across multiple files
- Improved PCI DSS 2.0 compatibility and reports

What Was New in 3.40

February 2012

HP Fortify Software Security Center

Configurable Bug Tracking—Development teams can now publish static, dynamic, or manual security results in their own bug-tracking systems. Immediate support is available for HP ALM/QC 11, JIRA 4, and Bugzilla 3. Sample code is provided for those needing support for additional bug-tracking systems or requiring customization to supported plug-ins.

CloudScan Admin Console—Using the console, developers can submit CloudScan jobs directly to Software Security Center, meaning that they need awareness of only one system, which both generates and presents security results. CloudScan also features an optional “lockdown mode,” which requires that all CloudScan jobs be authenticated and tracked by Software Security Center.

Dynamic Visualizations—Visual representations of issues are generated by HP WebInspect’s dynamic analysis, highlighting attack payloads. Screenshots are available during triage of select HP WebInspect issues.

HP Fortify Static Code Analyzer

PCI-DSS 2.0 Support—SCA now maps issues to the PCI-DSS 2.0 compliance standard for reporting inside Software Security Center and Audit Workbench.

MSBuild Support—This is additional support for analyzing .NET and C/C++ solutions compiled through MSBuild, using touchless integration or custom tasks.

Scan Wizard—The Wizard simplifies the production of repeatable scans that help track issues over time via Software Security Center. It also provides build integration support for Ant, Devenv, Make, and MSBuild.

Visual Studio Remediation Plug-in—SCA now supports collaborative auditing of Software Security Center results, by way of a lightweight plug-in for Visual Studio 2010. The plug-in guides development teams to scan periodically in the build environment, publish results into HP Fortify Software Security Center, and then triage and remediate issues from Visual Studio. (Note that this plugin does not provide scan capabilities.)

HP Fortify SecurityScope

Java RESTful Service Support—Future versions of HP WebInspect can now understand and optimize assessment of Java applications using JAX-RS RESTful services. We now provide support for each service and its associated parameters.

HP WebInspect .NET Support—This new support provides internal application knowledge of .NET applications to HP WebInspect, making security analysis more thorough, more accurate, and faster. This informs developers with line-of-code level detail for dynamic results.

What Was New in 3.30

December 2011

HP Fortify Software Security Center

Instant-On Assessment—This feature helps facilitate communication between the Software Security Center administrator and development teams and helps new users gain access to the system by submitting requests for new projects and new access. We have also added an instructional process guide.

Custom Roles—In addition to the predefined roles you receive with Software Security Center, you can now define custom roles and assign them certain permissions. Software Security Center users with the appropriate permissions can view, create, edit, and delete custom roles.

ALM integration—Software Security Center provides integration with HP Application Lifecycle Management or HP Quality Center defect-tracking software. Once you have performed the integration steps, you may file defects through the Software Security Center Collaboration Module. The integration also enables Software Security Center to identify which changesets might have led to a particular issue found by SCA. This change set information is then included in the defect report.

HP Fortify Static Code Analyzer

Ant Tasks—SCA can now create an Ant task to upload an FPR file.

HP Fortify SecurityScope

HP Fortify SecurityScope implementation for .NET feature parity with Java—Communication between HP Fortify SecurityScope and HP WebInspect Real-Time for .NET was added, to achieve feature parity with Java communication.

What Was New in 3.20

September 2011

HP Fortify Audit Workbench and GUI Tools

Audit Workbench enables both standalone analysis and auditing of projects in conjunction with Software Security Center (known at the time as 360 Server).

HP Fortify SCA Scan Wizard

Leveraging the lessons learned from analyzing thousands of applications, SCA Scan Wizard provides an intelligent interface for integrating with build processes. This allows new users to easily integrate SCA with their build process in a way that generates repeatable analysis results.

HP Fortify Analyzers

HP Fortify Static Code Analyzer (SCA) provides root-cause identification of vulnerabilities in source code, while SecurityScope provides real-time monitoring of attacks and root-cause identification of vulnerabilities while an application is undergoing a penetration test.

HP Fortify Static Code Analyzer

Support for Adobe Flex—Extending the set of supported languages, SCA now provides full analysis support for Adobe Flex. Adobe Flex is a popular framework used to create rich user interfaces for web applications. SCA supports the analysis of Adobe Flex MXML files and also of the embedded ActionScript. This is the twentieth language supported by SCA.

HP Fortify CloudScan—Adapting technology from HP Fortify on Demand, SCA now provides a managed, centralized service that orchestrates the execution of SCA scans. HP Fortify CloudScan enables security teams to perform SCA scans for large sets of users without putting any additional requirements on distributed development teams.

What Was New in 3.10

June 2011

Major enhancements include breakthrough integration between HP Fortify SecurityScope and HP WebInspect. SecurityScope, an analysis engine embedded in a running application, now communicates directly with WebInspect, a traditional web-application penetration testing engine, during the analysis of an application. This communication allows for improved accuracy, confirmation of vulnerabilities, and more actionable detail in the vulnerability reports found in the WebInspect interface. This integration takes the “black” out of “black-box testing.”

HP Fortify Software Security Center (formerly Fortify 360 Server)

Improved Documentation of Extensibility API—The v3.1 release of 360 Server provides reference implementations for all extensibility APIs provided by the server. This includes samples integrating with Version Control Systems, Defect Tracking Systems, and example utilities leveraging the Web-Service API (for automated project creation and user assignment to issues).

HP Fortify Source Code Analyzer (SCA)

Improved JSP Analysis—It is now easier to configure SCA to analyze JSP while at the same time seeing significant improvements in the reporting of issues and accuracy of results.

HP Fortify SecurityScope

Confirmed Vulnerabilities—By confirming the presence of defects at the API level, SecurityScope enhances the accuracy of the issues reported by WebInspect.

Attack Surface Identification—Analyzing the running application enables SecurityScope to identify additional URLs and parameters to be attacked by WebInspect.

Issue Collapsing—Providing root cause information enables WebInspect to reduce duplicate issues into single report.

What Was New in 3.00

February 2011

Major enhancements include Real-Time Hybrid Analysis and SCA support for SAP's ABAP language. Real-Time Hybrid Analysis technology correlates dynamic test results with static test results. Correlating results from these different analysis engines provides a more comprehensive view of the root-cause issues in the source code.

HP Fortify Software Security Center (formerly Fortify 360 Server)

Real-Time Hybrid Analysis—Users can correlate SCA, WebInspect, and Security Scope results files for a deeper understanding of potential security vulnerabilities in their applications.

Due Date in Governance—The Governance module now allows users to specify due dates in a process template. In addition, a user can set an alert when a process template activity isn't completed by the due date.

Alerts for System Events—You can now set alerts to notify a user when specific system events occur, such as:

- A result file is processed
- An error occurred while processing a results file
- A results file requires approval for processing
- A report is generated
- A user is granted access to a project

Enhancements to Custom Tags—Each user can now create and manage custom tags separately from project templates. Also, custom tags can now be restricted so that only privileged users can set their value; and custom tags can be defined so that end users can dynamically add new values while auditing.

Paginated Dashboard—You can now organize your dashboard into pages.

HP Fortify Audit Workbench and Process Designer

Support for WebInspect—Audit results now appear in WebInspect.

Integration with HP Quality Center 9.2—Legacy support has been enhanced to include HP Quality Center 9.2 in addition to HP Quality Center 10.

Custom Tag Support—AWB supports the new custom tag features in 360 Server.

HP Fortify Source Code Analyzer

ABAP Support—SAP's ABAP programming language is now the nineteenth language supported by SCA.

HP Fortify Real-Time Analyzer

.NET 4.0 Support—RTA now offers expanded support for the 4.0 .NET runtime environment.

WebSphere 6.0—It also supports the WebSphere 6.0 application server.

HP Fortify SecurityScope

No-touch Deployment—Using the same interface made available to debuggers and profilers, SecurityScope deploys without modifying any part of the runtime environment or application.

Source Code Insight—This feature provides full runtime context for attacks performed on a running application. Developers benefit from security results that come complete with line-of-code information, stack traces, HTTP request and response details, and data the application was handling during an attack.

Intelligent Correlation—Sitting between the code and the attacker, SecurityScope provides the critical data that enables accurate correlation between SCA and WebInspect results.

Data Analysis—SecurityScope's position inside an application enables it to analyze not only the code but also the data in the application. This provides accurate detection of privacy violations related to Social Security numbers and credit cards— categories of issues previously unreported by WebInspect.

Minor Improvements

Software Security Center

- Improved metric reporting on “Time to Fix”
- Enhanced defect-tracking integration
- Enhanced user selection when using LDAP
- Enhanced LDAP integration
- Enhanced purging to reduce the database footprint.
- Distribution of a default project template with Rulepack updates, enabling organizations to define the default view of issues when users scan code that is not associated with a project in 360 Server

Audit Workbench

- Improved performance during the saving of incremental changes
- Enhanced Visual Studio support for manually created issues
- Now available as a 32-bit or 64-bit process
- Improved flexibility in working with source code
- Import of third-party penetration test results
- Enhanced user interface
- Expanded defect-tracking integration API

- Improved defect-tracking integration with HP Quality Center
- Enhanced presentation of runtime issues

Real-Time Analyzer

- Enhanced support for OSGI

Static Code Analyzer

- Enhanced X-Tier support for TSQL
- Enhanced Classic ASP, VBScript, and JavaScript support
- Enhanced web application dataflow analysis