Micro Focus Security

Fortify Software Security Content

2017 Update 4

December 15, 2017

About Micro Focus Security Fortify SSR

The Software Security Research team translates cutting-edge research into security intelligence that powers the Micro Focus Security Fortify product portfolio – including SCA, WebInspect, & AppDefender. Today, Micro Focus Security Fortify Software Security Content supports 968 vulnerability categories across 25 programming languages and spans more than 970,000 individual APIs.

Learn more at

https://software.microfocus.com/en-us/software/security-research

Fortify Software Security Research (SSR) is pleased to announce the immediate availability of updates to Fortify Secure Coding Rulepacks (English language, version 2017.4.0), Fortify WebInspect SecureBase (available via SmartUpdate), Fortify Application Defender, and Fortify Premium Content.

Micro Focus Security Fortify Secure Coding Rulepacks [SCA]

With this release, the Fortify Secure Coding Rulepacks detect 770 unique categories of vulnerabilities across 25 programming languages and span over 970,000 individual APIs. In summary, the release includes the following:

Scala Play framework[1]

Initial support has been added for the Scala Play framework in security content. Play is a web framework developed by Lightbend for building web applications in Scala. Four new vulnerability categories can now be detected in applications using Scala Play:

- JSON Path Manipulation
- Missing Form Field Constraints
- Missing Form Field Validation
- Same-Origin Method Execution

Additionally, many categories already supported in Scala are extended to cover Play APIs, including the following:

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: HttpOnly not Set
- Cookie Security: Overly Broad Domain
- Cookie Security: Overly Broad Path
- Cross Site Scripting: Reflected
- Cross Site Scripting: Persistent
- Cross Site Scripting: Poor Validation
- Header Manipulation
- Open Redirect
- Privacy Violation
- Server-Side Request Forgery
- System Information Leak

Scala Slick library[1]

Slick is a Functional Relational Model library developed by Lightbend to ease the access to databases. While numerous categories are now supported, in relation to Slick, the two principally supported vulnerability categories of interest are *SQL Injection* and *Access Control: Database*.

Same-Origin Method Execution

Coverage for a new vulnerability category, *Same-Origin Method Execution* (SOME), has been added for Scala Play and Java Spring frameworks. SOME is a web application attack which abuses callback endpoints by forcing a victim into executing arbitrary scripting methods of any page on the endpoint's domain.

[1] Translation of Scala using Fortify SCA requires a Lightbend subscription and requires SCA version 17.20

Support for Oracle JDBC

Java rulepacks now contain extended JDBC support for the Oracle JDBC Java API. Vulnerability category coverage includes the following:

- Access Control: Database
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- SQL Injection

NoSQL Injection: MongoDB

A new category, *NoSQL Injection: MongoDB*, has been added to detect insecure MongoDB queries. This vulnerability category may allow attackers to change the query structure, bypass query conditions, or cause the application to throw unexpected exceptions. This release supports both the Java and .NET MongoDB client SDKs.

OWASP Java Encoder project

Java rulepacks also contain added support for the OWASP Java Encoder project used in Java applications as well as with JSP tags. The OWASP Java Encoder project is maintained by OWASP and created to help Java developers defend against Cross-Site Scripting vulnerabilities through contextual output encoding.

ASP.NET improvements

Improvements have been made to existing vulnerability category support for ASP.NET. Support has been added for new attributes and APIs available for use for model and request validation under multiple namespaces including the following:

- System.Web.Mvc
- System.Web.Mvc.Ajax
- System.Web.Mvc.Html
- System.Web.WebPages

Objective-C AFNetworking library

Coverage for the most popular Objective-C HTTP client library, AFNetworking, has been introduced in this release. Amongst others, detection of the following vulnerability categories is now possible in applications using AFNetworking:

- Header Manipulation
- Insecure SSL: Overly Broad Certificate Trust
- Insecure SSL: Server Identity Verification Disabled
- Insecure Storage: HTTP Response Cache Leak
- Insecure Transport
- Insecure Transport: Weak SSL Transport
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Path Manipulation
- Privacy Violation
- Privacy Violation: Health Information
- Privacy Violation: HTTP GET
- Resource Injection
- System Information Leak: External

OWASP Top 10 2017

In order to support customers wanting to mitigate Web Application risk, correlation of the Micro Focus Fortify Taxonomy to the newly released OWASP Top 10 2017 has been added.

DISA STIG 4.4

In order to support our federal customers in the area of compliance, correlation of the Micro Focus Fortify Taxonomy to the Defense Information Systems Agency Application Security and Development STIG, version 4.4 has been added.

Micro Focus Security Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase combines checks for thousands of vulnerabilities with policies that guide users in the following updates available immediately via SmartUpdate:

Vulnerability support

Cross Site Scripting Enhancements

Dangling tag injection can be used to bypass Content-Security-Policy protections, execute malicious script and exfiltrate sensitive information (e.g. CSRF tokens from HTTP response). This release includes enhancements for the Cross-Site Scripting check to detect dangling tag injection vulnerabilities in web applications. Further payloads to detect DOM-based XSS have been enhanced to detect additional instances where the payload is reflected in script block.

Performance improvements

Optimizations to WebInspect checks to reduce the amount of WebInspect traffic generated during a scan are also included. Depending on the nature of the application being scanned, these updates will reduce the duration of scan times.

Compliance report

OWASP Top 10 2017 compliance template

This release includes a new compliance report template that provides correlation between OWASP Top 10 2017 categories and WebInspect checks.

DISA STIG 4.4

In order to support our federal customers in the area of compliance, this release contains a correlation of the WebInspect checks to the latest version of the Defense Information Systems Agency Application Security and Development STIG, version 4.4.

SANS Top 25 2011 compliance template

This release also includes a new compliance report template correlating WebInspect checks to the 2011 CWE/SANS TOP 25 Most Dangerous Software Errors list.

Policy Updates

In order to support customers in the area of compliance, this release includes the following new Policies:

- OWASP Top 10 2017
- DISA STIG V4R4
- SANS Top 25 2011

These policies contain a subset of the available WebInspect checks that allow customers to run compliance specific WebInspect scans. In our constant effort to improve performance and relevancy of results from WebInspect scans, we have also improved the existing OWASP 2013 policy and compliance to exclude checks that are considered legacy and deprecated. Applications can be evaluated against these excluded checks by running “deprecated checks” policy.

Micro Focus Security Fortify Application Defender

Fortify Application Defender is a runtime application self-protection (RASP) solution that helps organizations manage and mitigate risk from homegrown or third-party applications. It provides centralized visibility into application use and abuse while protecting from software vulnerability exploits and other violations in real time. For this release, the Micro Focus Security Fortify Software Security Research team provides the following feature improvements:

Improved Runtime Taint rulepack for IAST

Performance optimization when repeatedly reading the same database column across multiple rows. This release has also improved support on Microsoft WebApi which maps more .NET Attributes as Taint sources.

Micro Focus Security Fortify Premium Content

The research team builds, extends, and maintains a variety of resources outside our core security intelligence products.

Insider Threat Rulepacks

The Fortify Insider Threat rulepacks were designed for security experts who want help finding malicious code in software. The rulepacks previously identified 22 categories of potentially malicious code, including Time Bombs, Custom Authentication, and Password Bypass. With this update, the Insider Threat Rulepacks now supports a new category, *Insider Threat: Static SQLite Query*, and expands coverage of *Insider Threat: Runtime Compilation* to the following four Java libraries:

- ObjectWeb ASM
- Apache BECL
- Javassist
- CGLib

Insider Threat rulepacks are available for both Java and .NET on the Fortify Customer Support Portal under Premium Content.

OWASP Top 10 2017 and DISA STIG 4.4 reports

To accompany the new correlations, this release also contains a new report bundle with support for OWASP Top 10 2017 and DISA STIG 4.4, which is available for download from the Fortify Customer Support Portal under Premium Content.

Micro Focus Security Fortify Taxonomy: Software Security Errors

The Fortify Taxonomy site, containing descriptions for newly added category support, is available at https://vulncat.fortify.com and https://vulncat.hpefod.com Customers looking for the legacy site, with the last supported update, may obtain it from the Micro Focus Security Fortify Support Portal.

Contact Fortify Technical Support
Micro Focus Security Fortify
fortifytechsupport@hpe.com
+1 (844) 260-7219

Contact SSR
Alexander M. Hoole
Manager, Software Security Research
Micro Focus Security Fortify
hoole@microfocus.com
+1 (650) 258-5916

December 15 2017