Micro Focus

Fortify Software Security Content

2019 Update 4

December 13, 2019

About Micro Focus Fortify Software Security Research

The Fortify Software Security Research team translates cutting-edge research into security intelligence that powers the Fortify product portfolio – including Fortify Static Code Analyzer (SCA), Fortify WebInspect, and Fortify Application Defender. Today, Micro Focus Fortify Software Security Content supports 1,018 vulnerability categories across 26 programming languages and spans more than one million individual APIs.

Learn more at: https://www.microfocus.com/en-us/solutions/application-security

Fortify Software Security Research (SSR) is pleased to announce the immediate availability of updates to Fortify Secure Coding Rulepacks (English language, version 2019.4.0), Fortify WebInspect SecureBase (available via SmartUpdate), and Fortify Premium Content.

Micro Focus Fortify Secure Coding Rulepacks [SCA]

With this release, the Fortify Secure Coding Rulepacks detect 807 unique categories of vulnerabilities across 26 programming languages and span over one million individual APIs. In summary, this release includes the following:

Go Initial Support[1]

Initial support for Go. Go is a statically typed open-source language designed by Google™ that aims to make it easy to build simple, reliable, and efficient software. Go is syntactically similar to C, but with memory safety mechanisms, garbage collection, and structural typing. This update covers 10 core standard library namespaces and support for the following 34 categories:

- Access Control: Database
- Command Injection
- Connection String Parameter Pollution
- 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: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- File Permission Manipulation
- Header Manipulation
- Header Manipulation: Cookies
- HTML5: MIME Sniffing
- Insecure Transport
- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key
- Open Redirect
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Path Manipulation
- Path Manipulation: Zip Entry Overwrite
- Privacy Violation
- Server-Side Request Forgery
- Setting Manipulation
- SQL Injection
- System Information Leak: External
- System Information Leak: Internal
- Weak Encryption
- Weak Encryption: Insufficient Key Size

[1] Requires SCA v19.2.0 or later.

Spring Security

Spring Security is an authentication and access-control framework that also provides additional layers of security, such as security headers, which offers additional protection against attacks such as session fixation, clickjacking, and cross-site request forgery. It is the de-facto standard for securing Spring-based applications. This update includes support, up to version 5.2.1, for the following 21 categories:

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: Overly Broad Domain
- Cross-Site Request Forgery
- Header Manipulation
- HTML5: Cross-Site Scripting Protection
- HTML5: MIME Sniffing
- HTML5: Missing Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- HTML5: Overly Permissive CORS Policy
- HTML5: Overly Permissive Referrer-Policy
- Insecure Transport: HSTS Does Not Include Subdomains
- Insecure Transport: HSTS not Set
- Insecure Transport: Insufficient HSTS Expiration Time
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Privacy Violation
- Session Fixation
- System Information Leak

Additionally, the following seven new weakness types are introduced:

- HTML5: Missing Framing Protection
- HTML5: Unenforced Content Security Policy
- Spring Security Misconfiguration: Default Permit
- Spring Security Misconfiguration: Disabled Security Headers
- Spring Security Misconfiguration: Incorrect Request Matcher Type
- Spring Security Misconfiguration: Lack of Fallback Check
- Spring Security Misconfiguration: Overly Permissive Firewall Policy

Spring Boot

Spring Boot creates stand-alone Spring applications and automatically configures Spring and third-party libraries whenever possible. It also provides production-ready features such as metrics, health checks, and externalized configuration. In addition to the previously supported categories, this update includes support, up to version 2.2.1, for the following additional nine categories:

- Cookie Security: HTTPOnly not Set on Session Cookie
- Cookie Security: Overly Broad Session Cookie Domain
- Cookie Security: Overly Broad Session Cookie Path
- Cookie Security: Persistent Session Cookie
- Cookie Security: Session Cookie not Sent Over SSL
- Password Management: Empty Password in Configuration File
- Insecure Transport
- Insecure Transport: Server Identity Verification Disabled

- System Information Leak: External

In addition, while previous Rulepacks only supported Properties configuration files and the Maven build system, this release also includes support for YAML configuration files and Gradle.

Java 12[2]

Support for new APIs in Java 12. These rules require SCA version 19.1, or later, when new Java 12 syntax such as the new Switch statement is used.

JSTL XML Library

JavaServer Pages (JSP) Standard Tag Library (JSTL) is a library that provides a JSP-centric way of manipulating and creating XML documents. Support now includes coverage for the following categories for JSTL v1.1:

- XSLT Injection
- XML External Entity Injection
- Privacy Violation
- System Information Leak: External

OpenXML SDK .NET Improvements

Updated support for OpenXML SDK v2.9.0 includes support for three additional categories:

- Access Control: Database
- Connection String Parameter Pollution
- SQL Injection

React-Router Support

React Router is a collection of navigational components that compose declaratively with your application. Whether you want to have bookmarkable URLs for your web application or a composable way to navigate in React, React Router works wherever React is rendering. Categories supported for React-Router 5.1.2 include:

- Open Redirect
- Privacy Violation
- System Information Leak: External

2019 CWE Top 25

The Common Weakness Enumeration (CWE) Top 25 has fundamentally changed how it is determined, compared to the days when it was known as the SANS Top 25. Released in September, the new Top 25 is determined using a heuristic formula that normalizes the frequency and severity of vulnerabilities reported to the National Vulnerability Database (NVD) over the past two years. To support our customers who want to prioritize their auditing around the most commonly reported critical vulnerabilities in the NVD, a correlation of the Micro Focus Fortify Taxonomy to the CWE Top 25, 2019 version has been added.

[2] Requires SCA v19.2.0 or later.

DISA STIG 4.10

To support our federal customers in the area of compliance, correlation of the Micro Focus Fortify Taxonomy to the Defense Information Systems Agency (DISA) Application Security and Development STIG version 4.10 has been added.

Miscellaneous Errata

In this release, we have continued to expend resources to ensure we can reduce the number of false positive issues and improve the ability for customers to audit issues. Customers can also expect to see changes in reported issues related to the following:

- Unsafe deserialization consistency: Previously, some rules would only flag when information came from a browser. This has been remediated to flag in other possible scenarios.
- Description references verified: Some of referenced materials were out of date or pointed to invalid links. These instances have now been fixed and appropriate references are in their place.

Micro Focus 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

SSO Bad Practices: Authentication Token Replay

Authentication tokens exchanged during a single sign-on process are susceptible to replay attack and can enable an attacker to impersonate a valid user to gain unauthorized access to the service. This release includes a check that performs the replay attack for windows identity framework and service providers using the SAML protocol.

Cache Management: Headers

The HTTP Vary response header contains a list of HTTP headers that are used to decide the correct cached response to serve an incoming request. Absence of ‘Origin’ in the Vary header can leave the application open to both client-side and server-side cache poisoning attacks especially when a cross origin request is made. This release includes a check to detect when there is a missing 'Origin' header in the Vary header value.

HTML5: CORS Functionality Abuse

Allowing CORS requests that originate from null origins, 'Origin: null', can compromise system security and leave the application vulnerable to data theft. This release includes a check to detect the presence of 'null' value in the Access-Control-Allow-Origin CORS header within a server response.

Insecure Deployment: HTTP Request Smuggling[3]

HTTP Request Smuggling vulnerabilities arise due to the discrepancy in parsing of non-compliant HTTP headers by front-end and back-end servers. By supplying a request that gets interpreted as being of different lengths by different servers, an attacker can poison the back-end TCP/TLS socket and prepend arbitrary data to the next request or smuggle additional requests to the back-end server without the front-end server being aware of it. This release includes a check to detect this vulnerability.

Header Manipulation[4]

The existing Header Manipulation check has been enhanced in this release to include carriage return ('CR') and line feed ('LF') attacks in addition to the existing CRLF attack.

Compliance report

DISA STIG 4.10

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 4.10.

Policy Updates

DISA STIG 4.10

A policy customized to include checks relevant to DISA STIG 4.10 has been added to the existing list of supported policies in WebInspect SecureBase.

Micro Focus Fortify Premium Content

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

DISA STIG 4.10 and 2019 CWE Top 25

To accompany the new correlations, this release also contains a new report bundle for Fortify Software Security Center with support for both DISA STIG 4.10 and the 2019 CWE Top 25, which is available for download from the Fortify Customer Support Portal under Premium Content.

[3] Insecure Deployment: HTTP Request Smuggling check requires WebInspect v19.2.0 or later.
[4] Header Manipulation enhancement requires WebInspect v19.2.0 or later.

Micro Focus Fortify Taxonomy: Software Security Errors

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

Contact Fortify Technical Support
Micro Focus Fortify
https://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

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

December 13 2019