Micro Focus

Fortify Software Security Content

2018 Update 4

December 14, 2018

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 992 vulnerability categories across 25 programming languages and spans more than one million 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 2018.4.0), Fortify WebInspect SecureBase (available via SmartUpdate), Fortify Application Defender, and Fortify Premium Content.

Micro Focus Fortify Secure Coding Rulepacks [SCA]

With this release, the Fortify Secure Coding Rulepacks detect 789 unique categories of vulnerabilities across 25 programming languages and span over one million individual APIs. In summary, the release includes the following:

SQLite and iOS improvements

Expanded support for SQLite APIs across Swift, Objective-C, C and C++. Coverage spans 16 existing vulnerability categories, including SQL Injection, Access Control: Database, and issues related to both password and key management. Coding weaknesses related to interaction with any type of database can result in leakage of sensitive information, unintended modification, or even loss of data. As such, there have been additional iOS improvements related to privacy which includes coverage of Privacy Violation: Heap Inspection for Swift.

Akka HTTP

Support for the Scala Akka HTTP modules, which is a Reactive Streams compliant toolkit based upon Akka Streams, that implements a full server- and client-side HTTP stack. Vulnerability category coverage spans 22 existing weakness types.

JAX-RS improvements

Revised support for latest version of JAX-RS and its reference implementation Jersey. In addition to supporting new features added in 2.1, this rulepack also includes support for client side APIs. Affected vulnerability categories include Privacy Violation, Server-Side Request Forgery, and System Information Leak. Additionally, a new weakness category has been added for a specialized subcategory of Cross-Site Scripting which results when responses are sent using XSS-safe content types. In this case, we will report a "Cross-Site Scripting: Content Sniffing" issue since specific browsers may conduct "content sniffing" and execute scripts in the response.

Python six

Support for the "six" Python library. Six is a Python compatibility library that is intended to support codebases that are compatible with both Python 2 and 3 without modification. Vulnerability categories supported include:

- Command Injection
- Dynamic Code Evaluation: Unsafe Pickle Deserialization
- Privacy Violation
- Server-Side Request Forgery
- System Information Leak: External
- Unsafe Reflection

DISA STIG 4.8

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 4.8, has been added.

PCI DSS 3.2.1

In order to support our e-commerce and financial services customers in the area of compliance, this release supports correlation between our Security Fortify Taxonomy categories and the requirements specified in the latest version of the Payment Card Industry Data Security Standard, version 3.2.1.

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

LDAP Injection

LDAP Injection is an attack used to exploit web based applications that construct LDAP statements based upon user input. When an application fails to properly sanitize user input, it is possible to modify LDAP statements through techniques similar to SQL Injection. LDAP injection attacks could result in unauthorized access to sensitive data. This release includes a check to identify LDAP injection vulnerabilities in web applications.

Open Redirect

An Open Redirect vulnerability can enable an attacker to easily exploit user's trust in known sites. According to vendor advisory SA-CORE-2018-006 Drupal 7 and 8 are vulnerable to this weakness.

Drupal Destination Parameter Anonymous Open Redirect

In Drupal 8, inadequate sanitization of the "destination" parameter value can be exploited to trigger an open redirect to a malicious URL that the attacker controls. This release includes a check to detect this vulnerability.

Drupal Path Alias Open Redirect

In Drupal 7, and Drupal 8, a vulnerability in the Path Module allows an attacker to create, edit, and administer path aliases which may trigger an open redirect to a malicious URL that the attacker controls.

Access Control: Authorization Bypass

JSON Web Token (JWT) is a standard for creating a URL-safe means of transferring data between two parties. Information within the token is digitally signed using either the HMAC or the RSA algorithm. However, the standard also allows for the use of "none" as the hash algorithm in the JWT. Servers accepting JWT's encoded with "none" consider all JWT to be valid without performing any verification on the integrity of the data. This can be exploited by malicious users to send arbitrary data to the server. This can result in unauthorized access and compromise of both system and user data. This release includes a check to detect JWT "none" algorithm authorization bypass vulnerability.

Privacy Violation

JSON Web Tokens (JWT) are used to transfer data between two parties. Sensitive data can be exposed to unauthorized users if not adequately encrypted. This release includes updates to existing checks that detect privacy violation related to Credit Card number disclosure, Social Security number disclosure and detecting storage of sensitive information within HTML5 client-side storage.

Dynamic Code Evaluation: Code Injection

Spring Framework by Pivotal has been found to be vulnerable to remote code execution vulnerability as identified by CVE-2018-1270. The vulnerability allows an attacker to send malicious messages to exposed STOMP over WebSocket endpoints that can result in remote code execution. This release contains a check to detect this vulnerability in Spring Framework. The check can be accessed via the WebSocket policy.

WebSocket Discovered

This release includes an informational check to indicate the presence of WebSockets in the scanned application. In addition, the check triggers a reminder for our customers to consider scanning the application with the new WebSocket policy that contains all checks relevant to WebSocket vulnerabilities.

Compliance report

DISA STIG 4.8

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 4.8.

PCI DSS 3.2.1

This release includes support for the latest version of the Payment Card Industry Data Security Standard (DSS) Compliance Template, version 3.2.1.

Policy Updates

DISA STIG 4.8

A policy customized to include checks relevant to DISA STIG 4.8 has been added to the existing list of supported policies in WebInspect SecureBase.

WebSocket

The new WebSocket policy performs a security assessment of the application for WebSocket related vulnerabilities.

Micro Focus Fortify Premium Content

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

DISA STIG 4.8[1]

To accompany the new correlations, this release also contains a new report bundle for Fortify SSC with support for DISA STIG 4.8, which is available for download from the Fortify Customer Support Portal under Premium Content.

PCI DSS 3.2.1[1]

To accompany the new correlations, this release also contains a new report bundle for Fortify SSC with support for PCI DSS 3.2.1, which is available for download from the Fortify Customer Portal under Premium Content.

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, may obtain it from the Micro Focus Fortify Support Portal.

[1] Support for DISA STIG 4.8 and PCI DSS 3.2.1 reports requires Fortify SSC version 18.20 or above.

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 14 2018