Software Security Research Release Announcement

Micro Focus

Fortify Software Security Content

2019 Update 2

June 28, 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 1,005 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 2019.2.0), 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 799 unique categories of vulnerabilities across 25 programming languages and span over one million individual APIs. In summary, this release includes the following:

.NET Updates

Support for API additions introduced in .NET Framework versions 4.7.1 and 4.7.2. Updates include rules support for .NET Standard 2.0 and .NET Core 2.0, which cover the same categories as .NET Framework. Rules for the updated versions of .NET Framework include enhanced support for the following categories:

- Header Manipulation: Cookies
- Insecure SSL: Server Identity Verification Disabled
- Insecure Transport: Weak SSL Protocol
- Weak Cryptographic Hash
- Weak Cryptographic Signature: Insufficient Key Size
- Weak Encryption

Realm Database

Realm Database, an open source lightweight database specifically designed for mobile applications, is now supported for iOS (Swift and Objective-C) as well as Android (Java). Supported categories include the following:

- Access Control: Database
- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key
- Path Manipulation

Additionally, two new categories are supported:

- Insecure Storage: Missing Database Encryption
- NoSQL Injection: Realm

Python urllib3

Python urllib3 library, a commonly used and powerful HTTP client, is now supported. Category coverage includes the following:

- Header Manipulation
- Insecure SSL: Server Identity Verification Disabled
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Server-Side Request Forgery

Java SE 10 and 11 Updates

Coverage for Java SE has been extended to versions 10 and 11, including support for the new HTTP client API.

Cross-Site Scripting: SOP Bypass

Support within JavaScript and TypeScript for the new category "Cross-Site Scripting: SOP Bypass". This new category covers the specific situation where a weakness enables an attacker to bypass the Same-Origin Policy (SOP) to enable a Cross-Site Scripting attack.

PCI SSF 1.0

To support our e-commerce and financial services customers in the area of compliance, this release supports correlation between our Micro Focus Fortify Taxonomy categories and the control objectives specified in the new "Secure Software Requirements and Assessment Procedures", defined in the Payment Card Industry (PCI) Secure Software Standard (SSS) as part of the new Software Security Framework (SSF), version 1.0. The new standard is set to eventually replace the PCI Data Security Standard (DSS) with new Payment Application (PA) DSS submissions ending in mid-2020 and changes under existing PA-DSS expiring in 2022.

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:

Log Forging

Reduction of false positives, across all languages, due to more accurate recognition of APIs that remove new lines to prevent Log Forging and Log Forging (debug) issues.

Unreleased Resource: Database

Within Java, algorithms were not correctly identifying that a ResultSet is automatically closed if the Statement that created it was closed first. Related false positives are now eliminated.

Unsafe JNI and Unsafe JSNI

Customers that upgraded to SCA v19.1.x might have witnessed a surge of new "Unsafe JNI" and "Unsafe JSNI" issues in Java applications. This was due to an improvement in the engine. This meant that a lot of APIs were being flagging that customers have no control over fixing. This has now been rectified so that SCA only flags APIs where the user has control over the source. With this reduction in issues, customers might also notice a reduction in "Access Control: SecurityManager Bypass" issues.

Dynamic Code Evaluation and Other Sinks on Lambdas

In JavaScript applications, confusing results could result where an issue resulted from a lambda call. A common example of this was with setTimeout(). These extraneous issues are now removed, and although there are some cases where these can still occur we are actively working to reduce the frequency. This reduction can only be observed when using SCA v18.20

or later.

Cross-Site Scripting: Content Sniffing support

Previously, SCA reported Cross-Site Scripting issues in situations where the response's content-type prevented a browser from processing the HTML/JS content (e.g. application/json). The reason for this is that users of the web application might be using older browsers that could enable a content-sniffing attack. With this release, we modified these issues to be reported as "Cross-Site Scripting: Content Sniffing". This enables auditors and developers to quickly recognize them and tell them apart from more severe cases of Cross-Site Scripting. Both Spring framework and JAX-RS in the Java Rulepacks support this new category.

Lowering of Fortify Priority Order Based On Taint

Previously, SCA reported a SQL Injection that originated from an HTTP request parameter with the same severity as if it originated from a System Environment variable. We understand that the likelihood of an attacker controlling System variables is very low or at least lower than controlling a request parameter. We were already reducing the Fortify Priority Order value of an issue based on this in certain scenarios, however, as of this release, SCA will more consistently apply the taint origin as a new factor when calculating an issue's Fortify Priority Order value.

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

WebSocket Update[1]

This release includes enhancements to detect information leak and unsafe deserialization (for .NET) vulnerabilities in WebSocket traffic. Specifically, the following categories were enhanced to support WebSocket:

- Dynamic Code Evaluation: Unsafe Deserialization
- Poor Error Handling: Unhandled Exception
- Privacy Violation
- Privacy Violation: Credit Card Number
- Privacy Violation: National ID Disclosure
- Privacy Violation: Social Security Number
- System Information Leak: Internal IP

Secure Response Headers Configuration Update

The server can use a set of HTTP response headers to provide a browser configuration that increases the security of the application. These headers are regarded as an in-depth defense mechanism and when set, they can adequately prevent vulnerabilities.

[1] WebSocket Update requires WebInspect 19.1.0 or later.

This release includes enhanced support for the following headers and relevant categories:

- Cache-Control
  - Cache Management: Insecure Policy
- Content-Security-Policy
  - HTML5: Missing Content Security Policy
  - HTML5: Deprecated Content Security Policy
  - HTML5: Misconfigured Content Security Policy
- X-Content-Type-Options
  - Web Server Misconfiguration: Insecure Content-Type
- X-XSS-Protection
  - HTML5: Cross-Site Scripting Protection

Web Server Misconfiguration: Deprecated SSL/TLS Certificate

All SSL/TLS certificates issued before December 1, 2017 by the Symantec certificate authority (including Symantec-owned brands such as Thawte, VeriSign, Equifax, GeoTrust, and RapidSSL) are distrusted and are no longer accepted by all major browsers, including Chrome, Internet Explorer, Firefox, and Safari. This release includes a check to flag the use of deprecated Symantec certificates.

Insecure Deployment: Unpatched Application

A critical remote code execution vulnerability in the Drupal content management system (CMS) identified by CVE-2019-6340 allows remote attackers to execute arbitrary code on the server. This release includes a check to detect this vulnerability in applications that deploy the Drupal CMS.

Compliance report

PCI SSF 1.0

To support our customers in the area of compliance, this release includes a new compliance template that correlates Micro Focus Fortify Taxonomy to the control objectives specified in the new "Secure Software Requirements and Assessment Procedures", defined in the Payment Card Industry (PCI) Secure Software Standard (SSS) as part of the new Software Security Framework (SSF), version 1.0. The new standard is set to eventually replace the PCI Data Security Standard (DSS) with new Payment Application (PA) DSS submissions ending in mid-2020 and changes under existing PA-DSS expiring in 2022.

Policy Updates

PCI SSF 1.0

A policy customized to include checks relevant to PCI SSF 1.0 has been added to the existing list of supported policies in WebInspect SecureBase.

Miscellaneous Errata

Cache Management: Insecure Policy

Enhancements were made to check ID 11306 to exclude flagging on HTML responses of specific content-types that were most frequently audited as false positive findings upon manual verification.

Expression Language Injection: Spring

The accuracy of vulnerability detection algorithm in SecureBase check ID 11579 was improved.

Micro Focus Fortify Premium Content

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

PCI SSF 1.0

To accompany the new correlations, this release also contains a new report bundle for Fortify SSC with support for PCI SSF 1.0, 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.

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

June 28 2019