Software Security Research Release Announcement

Micro Focus

Fortify Software Security Content

2019 Update 3

September 27, 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 1,009 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 2019.3.0), 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 800 unique categories of vulnerabilities across 25 programming languages and span over one million individual APIs. In summary, this release includes the following:

React version 16.5[1]

New support for the JavaScript library React has been added to increase coverage of user interfaces. This includes support for all regular HTML-based weakness categories through JSX (templating framework with the full power of JavaScript), as well as those relevant to React-specific APIs. Support also includes DOM attributes that are different between JSX and standard HTML.

Categories for React-specific APIs and DOM attributes include:

- Cross-Site Scripting: DOM
- Cross-Site Scripting: Poor Validation
- Privacy Violation
- System Information Leak: External

Scala 2.13

Updated support for Scala 2.13 includes refactored Scala Collection packages. No new categories are added, however, new rules enable dataflow analysis through 2.13 applications.

Open XML SDK v2.9.0

Support for Open XML SDK, which provides tools for working with Microsoft Office Word, Excel, and PowerPoint documents, along with any other Open XML files. Categories supported include:

- Privacy Violation
- System Information Leak
- Path Manipulation

Along with a newly-introduced category:

- XML Injection: Open XML

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:

- Improvements to the security content which backs the Fortify Java Annotation library now more accurately reflect Fortify Priority Order. Furthermore, the @FortifyDangerous can now take Fortify Priority Order values critical, high, medium and low (String parameter is no longer case-sensitive).

[1] Requires SCA v19.2.0 or above.

- Fortify Priority Order values have been changed in dozens of rules for consistency. As a result, a small subset of issues may change their priority values.
- Reduced false positives for C++ Memory Leak rules to account for smart pointers.
- Reduced false positives for Java and .NET JSON Injection rules.
- Reduced false positives for Log Forging issues found in JavaScript/TypeScript projects when logging to a non-persistent console.
- Reduced false positives in .NET with the removal of general passthroughs.

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

SAML Dupekey Injection (CVE-2019-1006)

Earlier this quarter, SAML Dupekey Injection vulnerability was disclosed publicly at Blackhat 2019. The vulnerability targets a critical authorization bypass weakness in Microsoft WCF, WIF 3.5 and later within the .NET Framework, WIF 1.0 component in Windows, the WIF Nuget package, and the WIF implementation in Microsoft SharePoint. An update for Securebase was made available impromptu to release a check for detection of this vulnerability. The check is identified by ID 11612. Further enhancements have been made to the check since the mid-quarter release. This release contains the enhancement to support compressed values, expand attack surface by adding a new payload with a symmetric key, and inclusion of the check in the standard policy. You can find additional details about the vulnerability in the whitepaper released by Micro Focus Software Security Research at Black Hat USA 2019.

Access Control: Authorization Bypass[2]

XML parsing and canonicalization issues can leave SAML message validation vulnerable to the authorization bypass vulnerability enabling an attacker to impersonate a different user. Examples of this vulnerability include CVE-2017-11427, CVE-2017-11428, CVE-2017-11429, CVE-2018-0489, and CVE-2018-7340. This release includes a check to detect this vulnerability. This might require auditors to update the default scan setting that excludes audit of logout URLs.

SAML Message Replay Vulnerabilities[3]

SAML Bad Practices: Missing Assertion Signature

SAML messages are cryptographically signed to guarantee validity and integrity of the assertion. Man-in-the-middle attackers can tamper with the SAML response message without signatures. The attacker can modify the permissions and impersonate a user at

[2] SAML Authorization Bypass requires WebInspect 19.2.0 or above.

[3] SAML Message Replay Vulnerabilities require WebInspect 19.2.0 or above.

the service provider. This release includes a check that passively inspects SAML response messages and reports if any message includes an assertion without signature.

SAML Bad Practices: Insecure Message ID Implementation

To prevent replay attacks SAML request and SAML response messages are related with a unique ID. Additionally, assertions in SAML responses includes a unique ID. Failure to include these unique IDs leaves SAML implementations susceptible to impersonation and authentication bypass attacks. This release includes a check that passively inspects SAML response messages and reports if the messages fail to include a unique ID in SAML request, SAML response, and Assertion.

SAML Bad Practices: Insufficient Session Expiration

The SAML response message can contain a timestamp to indicate when the SAML response message was issued and for how long it is valid. These values are communicated in the IssueInstant, NotOnOrAfter, and NotBefore attributes. Ideally, the value for these attributes should set a message to be valid for one to five minutes. This release includes a check that reports if the message is set to be valid for more than five minutes. This default period can be set to a custom value by setting associated check input in policy manager or scan settings.

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:

LDAP Injection

LDAP Injection is an attack that exploits web-based applications that construct LDAP statements based on user input. This release includes an updated check with modification to the logic on how the check is flagged to provide more accurate results.

Insecure Transport: Weak Cipher Suites

MD5 is known to be weak and collision attacks on SHA-1 have now shown to be practical. This release includes an enhancement to the Insufficient Transport Layer Protection - Weak Cipher check to flag all ciphersuites that use either MD5 or SHA-1 as cryptographic hash functions, as weak.

Flash Misconfiguration: Vulnerable Flash Engine

Flash has had innumerable vulnerabilities associated with it since its inception, including various remote code execution and cross-site scripting vulnerabilities that can compromise user systems and data. Adobe has announced that they will discontinue support for Flash with end-of-life at the end of December 2020. WebInspect check - Vulnerable Flash Engine, is now updated to flag the use of Flash in the target application.

Micro Focus Fortify Premium Content

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

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

September 27 2019