Micro Focus

Fortify Software Security Content

2020 Update 2

June 26, 2020

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 1,022 vulnerability categories across 27 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 2020.2.0), 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 810 unique categories of vulnerabilities across 27 programming languages and span over one million individual APIs. In summary, this release includes the following:

Kotlin Core Library Support (Version 1.3)[1]

Initial support for Kotlin standard libraries covering the following packages targeting the JVM:

- kotlin
- kotlin.collections
- kotlin.comparisons
- kotlin.io
- kotlin.properties
- kotlin.random
- kotlin.ranges
- kotlin.sequences
- kotlin.streams
- kotlin.text

Limited Java interoperability implies that all categories and libraries supported by Java are all partially supported in Kotlin, as well as the following supported specifically for the Kotlin standard libraries:

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Denial of Service: Regular Expression
- Denial of Service: StringBuilder
- Formula Injection
- Insecure SSL: Overly Broad Certificate Trust
- Log Forging
- Path Manipulation
- Poor Logging Practice: Use of a System Output Stream
- Privacy Violation
- Server-Side Request Forgery
- System Information Leak
- System Information Leak: External
- System Information Leak: Internal
- Trust Boundary Violation
- Unchecked Return Value

[1] Requires SCA 20.1.2 patch release. Using SCA 20.1 will result in multiple errors around rules and specific lambda functions, which do not occur with the patch release.

C# 8 and .NET Core Improvements

Updated support for C# 8 and the .NET Core libraries including versions 2.1, 2.2, 3.0, and 3.1. With this comes full rules support for .NET Standard 2.1 as well as improved dataflow when using C# 8's asynchronous *foreach*, *range*, and *using* operations.

Python Core Library Improvements[2]

Updated support for the Python core libraries including versions 3.7 and 3.8. In addition to previously supported categories, the following new category is now supported:

- Python Bad Practices: Leftover Debug Code

Go Core Library Support Improvements (Version 1.13)

Expanded support for Go core libraries to cover crypto/tls. Go is a statically typed open-source language designed by Google™ which 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. Supported categories include:

- Insecure SSL: Server Identity Verification Disabled
- Path Manipulation
- Privacy Violation
- Server-Side Request Forgery
- Setting Manipulation
- System Information Leak: External

GORM (Version 1.9.12)

Support for GORM library, which is an open source Object Relational Mapping (ORM) project for Golang written by Jinzhu. GORM is a common ORM library that may introduce database related risks to enterprise applications. Supported categories include:

- Access Control: Database
- Connection String Parameter Pollution
- Dynamic Code Evaluation: Code Injection
- Insecure Transport
- Log Forging
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Weak Cryptography
- Privacy Violation
- Setting Manipulation
- SQL Injection
- System Information Leak: Internal
- Weak Cryptographic Hash

OWASP ASVS 4.0

To support our customers looking to frameworks to help run their appsec program, this release supports correlation between our Micro Focus Fortify Taxonomy categories and the requirements in the

[2] Requires SCA 20.2 for improved results when projects include newly introduced syntax such as assignment expressions.

OWASP Application Security Verification Standard, version 4.0. ASVS provides a list of requirements, or tests, which customers can use to assist with their definition, building, testing, and verification of secure applications.

Miscellaneous Errata

In this release, we have continued to invest 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:

Kingdom changes:
In some select places, the kingdom for specific categories was changed for consistency. In older versions of SCA (versions lower than 6.30, meaning any release prior to 2015-04-17), this may cause some issues to be treated as new/removed when merging, instead of staying as "updated". For any version of SCA 6.30 or higher, this issue will not occur.
This can also generally affect filtering, if users are filtering by kingdom. Affected categories include:

- Access Control: ACL Manipulation. Changed from "Input Validation and Representation" to "Security Features"
- Access Control: Authorization Bypass. Changed from "Input Validation and Representation" to "Security Features"
- System Information Leak: Struts 2. Changed from "Input Validation and Representation" to "Encapsulation"

False positive improvements:
We continue to listen to our customers and strive to improve the false positive rates. During this release we have worked on the following in order to reduce the number of false positives:

- Removed a specific JavaScript source rule that was causing false positives across multiple categories.
- Java "Unreleased Resource: Database" rules have been improved to account for connections closing underlying resources as per the JDBC 4.3 specification.
- Removed false positive "Path Manipulation" issues in Java surrounding File.createTempFile().
- Reporting of issues from TypeScript definition files has been disabled.
- Some .NET "Server-Side Request Forgery" false positives have been removed on SendAsync.
- Java "Spring Security Misconfiguration: Incorrect Request Matcher Type" false positives have been reduced.
- Duplicate .NET "Weak Encryption" issues have been removed.
- .NET "ASP.NET Bad Practices: Non-Serializable Object Stored in Session" false positives removed on String types.
- Golang false positives removed that were resulting from unintentional tainting of net.http.Response objects.
- Identified and removed rare "Code Correctness: Class Does Not Implement equals" false positives within Java.
- In JavaScript, many false positive "Key Management" issues have been removed, and further progress will be continued in later releases.

Errors and warnings:

With SCA 19.2, for any supported programming language, rule loading during a scan will result in the following warning being produced in the build and scan logs when combined with the complete set of 2020.2.0 rulepacks:

```
[WARN  20599]
The rule language kotlin has no corresponding mapping in SCA
```

This is a known issue in SCA 19.2 which can be worked around by removing the following Kotlin rulepack file:

<*FORTIFY_DIR*>\Fortify_SCA_and_Apps_19.2.0\Core\config\rules\core_kotlin.bin

Scanning of Kotlin requires SCA 20.1.2.

VulnCat improvements

We have improved the sorting of filter categories as well as filter subcategories so that entries will be displayed in a logical order.

ESAPI validation support

We have listened to our customers, and many feel concerned about SCA rules allowing ESAPI APIs to remove issues as fixed, due to security concerns around the library.
From this release, we have removed validation from the ESAPI libraries, and now dataflow will continue through the encoding functions without preventing dataflow issues from appearing.
Since we know that some customers would like to continue using the ESAPI library, specifically for legacy products, we are making a separate rulepack available to include this validation back again.

If you would like to continue using ESAPI, you can use our ESAPI extension rulepack that can be found on the Support Portal under Premium Content, Fortify Exchange.

Please note, this update also removes all issues flagging as "Obsolete: Deprecated by ESAPI", which can similarly be found using the above mentioned separate rulepack.

Weak Encryption Update

3DES, also known officially as the Triple Data Encryption Algorithm (TDEA), will now be reported under Weak Encryption following recommendations from the National Institute of Standards and Technology (NIST).

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

Web Server Misconfiguration: Information Disclosure

Spring Boot includes a number of additional features also known as actuators that allow administrators to monitor and manage their web applications. This release includes a check to detect sensitive Spring Boot Actuator available for unprivileged users. By using such actuator endpoints an attacker can gather audit, health and metric information, or even perform a Remote Code Execution attack on some configurations.

Cross-Site Scripting: Reflected

ASP.NET API ResolveUrl is used to resolve app-root-relative path at runtime. The API fails to validate relative path that includes cookie less state ID formatted values and enables attacker to conduct a Cross-Site Scripting attack on the application. This release includes a check to detect this vulnerability in .NET applications.

Cookie Security: Missing SameSite Attribute

SameSite attribute on cookies provides a simple mechanism to protect applications against Cross-Site Request Forgery attacks. Recent browser versions may reject cookies that don't set SameSite attribute. This release includes a check to detect set cookie instances that fail to set SameSite attribute.

Cookie Security: Misconfigured Prefix

Cookies with name prefixed with _Host- or_Secure- enforce host level restrictions and that the cookie must only be sent on secure HTTPS connection to protect it against accidental eavesdropping and spoofing. Cookies that don't have adequately set Path, Domain and Secure attribute may be rejected by the browser. A check to detect misconfigured prefixed cookie is included in this release.

Cookie Security: Overly Permissive SameSite Attribute

Strict value for SameSite attribute on cookies enforce browsers to only append that cookie to the requests that resulted because of top level navigation to the domain or when same host is making the request from various HTML tags with link such as iframe, link and form etc. Session IDs should be set with Strict value for SameSite attribute to provide maximum protection to the application against the Cross-Site Request Forgery attacks. This release includes a check to detect instance when the SameSite attribute is not set to Strict for session cookies.

Compliance report

OWASP Application Security Verification Standard (ASVS)

OWASP ASVS provides a methodology for testing web applications for security controls and also provides secure development guidelines. This release contains a correlation of the WebInspect checks to the latest version of the OWASP ASVS 4.0.

Policy Updates

OWASP Application Security Verification Standard (ASVS) Policy

In addition to correlation of WebInspect checks to latest version of OWASP ASVS, this release also includes a policy to identify vulnerabilities that lead to correlated to OWASP ASVS.

Miscellaneous Errata:

In this release, we have continued to invest 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 contents for Often Misused: Weak SSL Certificate now more accurately reflect information about reasons why a certificate is considered as weak. A new check with ID 11635 was added.

Micro Focus Fortify Premium Content

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

OWASP Application Security Verification Standard (ASVS):

The Application Security Verification Standard (ASVS) is a list of application security requirements and tests to perform during a software development lifecycle (SDLC) and configuration to build secure software. We anticipate that this mapping will continue to evolve as we collaborate with industry partners to improve how the mappings are designed. To accompany the new correlations, this release also contains a new report bundle for Fortify SSC with support for OWASP ASVS 4.0, 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, 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

June 26 2020