Micro Focus

Fortify Software Security Content

2020 Update 4

December 18, 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 1,039 vulnerability categories across 27 programming languages and spans more than one million individual APIs.

Learn more at: https://software.microfocus.com/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 2020.4.0), 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 817 unique categories of vulnerabilities across 27 programming languages and span over one million individual APIs. In summary, this release includes the following:

Dapper Support (Version 2.0.78)

Support for Dapper object-relational mapping (ORM). Dapper is used to map native query output to strongly typed C# objects by extending the .NET IDdbConnection interface. New support treats Dapper as a source of user-controlled data and also as a trigger for categories such the following:

- Access Control: Database
- SQL Injection

Kotlin Standard Library Updates (Version 1.3)

Extended support for the Kotlin Standard Library to include coverage of the following packages:

- kotlin.concurrent
- kotlin.jvm
- kotlin.reflect
- kotlin.system

XML Pull (Version 1)

Support for Android's implementation of the XML Pull package. XML Pull is a simple streaming API used to parse and serialize XML files where the application controls the parsing (it can be interrupted and resumed). Categories supported include:

- XML Entity Expansion Injection
- XML Injection

AIOPG (Version 1.0.0)[1]

Support for the Python aiopg library. Aiopg provides an asynchronous way to connect to PostgreSQL databases. Categories supported include:

- Access Control: Database
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- SQL Injection

[1] Full detection of issues related to aiopg depends on a future improvement to SCA related to 'async with'.

JavaScript Promises

- Support for JavaScript Promises is improved for dataflow analysis.

Azure Resource Management Templates

Initial support for Azure Resource Management (ARM) templates. ARM templates are used to implement infrastructure as code for Azure solutions. ARM templates are JSON files that utilize a declarative syntax to define and configure a user's project. Categories supported include:

- Azure Resource Manager Misconfiguration: HTTPS Not Required
- Azure Resource Manager Misconfiguration: Public Access Allowed

DISA STIG 5.1

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 5.1 has been added.

NIST SP 800-53 Rev. 5

To support our federal customers in the area of compliance, correlation of the Micro Focus Fortify Taxonomy to the security and privacy controls in the latest version of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 has been added. Thirty base controls are covered, spanning the following control families:

- Access Control (AC)
- Audit and Accountability (AU)
- Assessment, Authorization, and Monitoring (CA)
- Configuration Management (CM)
- Identification and Authentication (IA)
- PII Processing and Transparency (PT)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

2020 Common Weakness Enumeration (CWE™) Top 25

The Common Weakness Enumeration (CWE™) Top 25 was introduced in 2019 and replaces SANS Top 25. Released in August, the 2020 CWE 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 2020 CWE Top 25 has been added.

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:

Deprecation of SCA versions prior to 17.x

As mentioned in our 2020.3 release announcement, that was the last release of the Rulepacks that support SCA versions prior to 17.x. For this release, SCA versions prior to 17.x will not load the latest Rulepacks. Customers using SCA versions prior to 17.x must either downgrade the Rulepacks or upgrade the SCA version.

In future releases, we will support the last four major releases of SCA.

Obsoletion of mappings
The Software Security Research team has continued to create mappings from Fortify categories to external standards and best practices over the years. As such, we are now at the point that the versions of different supported standards has grown very large, even though many old versions will no longer be used.

As such, we have now marked the following standards as "obsolete":
- Payment Card Industry Data Security Standard (PCI) 1.1
- Payment Card Industry Data Security Standard (PCI) 1.2
- Payment Card Industry Data Security Standard (PCI) 2.0
- Payment Card Industry Data Security Standard (PCI) 3.0
- Payment Card Industry Data Security Standard (PCI) 3.1
- Payment Card Industry Data Security Standard (PCI) 3.2
- Security Technical Implementation Guide (STIG) 4.1
- Security Technical Implementation Guide (STIG) 4.2
- Security Technical Implementation Guide (STIG) 4.3
- Security Technical Implementation Guide (STIG) 4.4
- Security Technical Implementation Guide (STIG) 4.5
- Security Technical Implementation Guide (STIG) 4.6
- Security Technical Implementation Guide (STIG) 4.7
- Security Technical Implementation Guide (STIG) 4.8

This change means that Fortify SCA Applications version 20.2 and later, will not show these old mappings by default.
If you are required to check compliance with these old versions, then you must change the mappings to set the *obsolete* attribute to "false", or remove the attribute entirely.

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 HTTP Verb Tampering false positives when protection is present in configuration files
- Removed Mass Assignment false positives when using the JSONIGNORE Attribute in .NET
- Removed Insecure Storage: HTTP Response Cache Leak false positives when caches are explicitly disabled in the URLSessionConfiguration objects
- Removed Swift Privacy Violation: Http Get false positives from URLRequest
- Poor Logging Practice: Use of a System Output Stream duplicates removed in Python
- Unreleased Resource issues removed when using additional Apache Commons closeQuietly variants

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

Weak Cryptographic Signature: Predictable Secret Key

JSON Web Token payload integrity is often ensured using HMAC signatures. However, if the HMAC algorithm uses a weak secret, a malicious user could obtain the secret key by brute force and re-sign the JWT with any payloads. This release includes a check to identify if a string from commonly used secrets is used to sign the JWT token.

Password Management: Weak Password Policy

Password policies that ensure users create strong passwords are crucial to deploy secure websites. Passwords should be validated to ensure they are not one of the commonly used passwords and a password string should meet the guidelines set per NIST 800-53, NIST 800-118, and OWASP. This release includes a new check to detect if the password configured in the login macro matches one of the commonly used passwords. The release also includes an update to weak password policy checks to meet revised guidelines on password strength as set in the above mentioned NIST standards and OWASP guidelines.

Cache Management: Web Cache Poisoning

Web caches store a copy of the page when the user first visits a website. The next time the user visits the same page, a cached copy is served to them. However, if these web caches have implementation or design flaws, such as accepting GET requests with request body (e.g. fat GET requests or unkeyed inputs), they are susceptible to web cache poisoning. Web cache poisoning is an advanced technique used by attackers to cache malicious responses for legitimate user requests. This release includes checks to identify if a website is vulnerable to web cache poisoning via unkeyed headers and fat GET requests.

Compliance Reports

DISA STIG 5.1

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 5.1.

NIST SP 800-53 Rev. 5

To support our federal customers in the area of compliance, this release contains a correlation of the WebInspect checks to the controls in the latest version of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5.

2020 Common Weakness Enumeration (CWE™) Top 25

The Common Weakness Enumeration (CWE™) Top 25 was introduced in 2019 and replaces SANS Top 25. Released in August, the 2020 CWE 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. This Securebase update includes mappings to these CWE categories. We include checks that map either directly to the category identified by the CWE Top 25, or a CWE-ID related to a CWE-ID in the Top 25 via “ChildOf” relationship.

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:

- The HTTP Request Smuggling check is redesigned to reduce false positives, increase efficiency, and improve the accuracy of its results. The check ID 11621 no longer uses a time-based approach for vulnerability verification.

Micro Focus Fortify Premium Content

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

DISA STIG 5.1, NIST SP 800-53 Rev. 5, and 2020 CWE Top 25

To accompany the new correlations, this release also contains a new report bundle for Fortify Software Security Center with support for DISA STIG 5.1, NIST SP 800-53 Rev. 5, and 2020 CWE Top 25, which is available for download from the Fortify Customer Support 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

December 18 2020