# Micro Focus

## Fortify Software Security Content

### 2021 Update 1

### March 26, 2021

**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 1,038 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 2021.1.0), 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 816 unique categories of vulnerabilities across 27 programming languages and span over one million individual APIs. In summary, this release includes the following:

### Micro Focus Visual COBOL support (Version 6)[1]

This release adds support for Micro Focus Visual COBOL version 6. In particular, the release includes support for Micro Focus COBOL Runtime System (RTS) with extended support for the already COBOL supported Path Manipulation category and the following additional categories:

- Command Injection
- Memory Leak
- Memory Leak: Reallocation
- Unreleased Resource
- Unreleased Resource: Synchronization

### Android 11

As part of an ongoing effort to support the latest version of Android (API version 30) the following namespaces are covered:

- android.accounts
- android.app
- android.database
- android.database.sqlite

Users should expect to see better modeling of Android applications that generally improve results, along with additional *SQL Injection* and *Access Control: Database* findings.

### iOS updates

As part of an ongoing effort to improve iOS support, new Swift rules are added for the following classes:

- Foundation.NSCache
- Foundation.URLFileProtection

Users should expect to see improved results related to Data Protection and Privacy Violation, along with general improvements in other weakness types and frameworks (see "Miscellaneous Errata - iOS bug fixes").

### Angular Support updates (Version 11.2.3)

This release brings our Angular support to 11.2.3. In particular, new sources of user-controlled information from the browser were identified, which can lead to many categories triggering where they had not previously.

[1] Requires SCA 21.1 or later.

## Apache Commons updates

Apache Commons provides reusable Java components. In this release, SSR updated support for the following components:

- beanutils (1.9.4)
- collections4 (4.4)
- dbutils (1.7)
- fileupload (1.4)
- lang (3.11)
- math (3.6.1)
- io (2.8.0)
- text (1.9)

These updates improve the modeling of applications using these components, identifies protections against categories such as Log Forging and JSON Injection, as well as identifying new places that the following weakness types may appear:

- Access Control: Database
- Denial of Service
- Insecure Randomness: User-Controlled Seed
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- SQL Injection
- System Information Leak (variants)

## Python (Version 3.9)

Updated support for the latest version of Python, improving modeling of the core language APIs.

## 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:

**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:

- *Code Correctness: Erroneous Class Compare* in Java and Kotlin applications
- *Dynamic Code Evaluation: Code Injection* issues removed in Python 3 scans
- *Key Management* issues have been improved to remove false positives across all languages
- *Cross-Site Scripting: DOM* issues related to jQuery are now correctly categorized as *Cross-Site Scripting: Self* when coming from an input box.
- *Password Management* issues removed in configuration files when matching content that could not be a password
- *Password Management* false positives improvements when matching against localization data.
- *XML External Entity Injections* findings removed on irrelevant functions in Java Spring applications.
- *ASP.NET MVC Bad Practices: Controller Not Restricted to POST* now allows additional verbs as safe (PATCH, DELETE, PUT).

**iOS Bug Fixes:**
Due to improvements to the analysis, rules updates were necessary. This may lead to users seeing improvements in the following weakness types:

- Input Interception: Keyboard Extensions Allowed
- Privacy Violation: HTTP Get
- Privacy Violation: Keyboard Caching
- Privacy Violation: Screen Caching
- Privacy Violation: Shoulder Surfing

Several frameworks have also had minor updates that improve accuracy: Foundation, UIKit, WebKit, HealthKit, WatchKit, MessageUI, CoreLocation, CoreData.

**Removed Categories:**
The following category has been removed in this release to enhance relevance of results:

- Privilege Management: Android Network

## 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

### OGNL Expression Injection: Struts 2

Critical OGNL Expression Language injection vulnerabilities identified by CVE-2019-0231 and CVE-2020-17530 affect Struts versions 2.0 to 2.5.25. Exploitation of these vulnerabilities can lead to arbitrary remote code execution on the server. This release includes a check to detect these vulnerabilities in web applications that use Struts 2.

### WAF Detection[2]

This release includes a check "WAF Detection", which flags informational findings when a Web Application Firewall is detected during a scan. These findings indicate that the scan quality might be compromised because scan requests are blocked before reaching the application.

### Hacker Level Insights[2]

Hacker Level Insights provide developers and security professionals with context relating to the overall security posture of their application. This release includes a check that flags libraries that were detected in the application during the scan. While these findings do not necessarily represent a security vulnerability, it is important to note that attackers commonly perform reconnaissance of these types of targets in an attempt to identify known weaknesses or patterns.

[2] Requires WebInspect 21.1 or later.

## Policy Updates

### NIST SP 800-53 Rev. 5

A policy customized to include checks relevant to NIST SP 800-53 Rev. 5 has been added to the WebInspect SecureBase list of supported policies.

### CWE Top 25 2020

A policy customized to include checks relevant to CWE Top 25 2020 has been added to the WebInspect SecureBase list of supported policies.

### DISA STIG 5.1

A policy customized to include checks relevant to DISA STIG 5.1 has been added to the WebInspect SecureBase list of supported policies.

## 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:

**Web Cache Poisoning**
This release includes an updated check for *Web Cache Poisoning: Unkeyed Headers*. Users can now add custom headers that they suspect are part of the cache-key.

**Unsafe SpringBoot Actuators**
This release includes an updated check for detection of sensitive Spring Boot Actuator available for unprivileged users, which provides more accurate results.

**XSS Improvements**
This release includes improved XSS attack checks for Vue 3 and Angular JS 1.5.9 and above.

# 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, 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



March 26 2021