# Micro Focus

## Fortify Software Security Content

### 2021 Update 2

### June 25, 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 1,039 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 2021.2.0), 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 817 unique categories of vulnerabilities across 27 programming languages and span over one million individual APIs. In summary, this release includes the following:

### Google Cloud Functions

Google Cloud Functions allow developers to write simple, single-purpose functions to handle events emitted from cloud infrastructure and services. These functions are intended to be executed from within Google Cloud infrastructure so that developers do not need to manage either the server or runtime environment. Rules support for Google Cloud Functions, written in Java, identifies sources of dangerous input originating from web requests and covers existing categories including, but not limited to:

- Cross-Site Scripting
- Cross-Site Scripting: Poor Validation
- Header Manipulation
- System Information leak: External

### Android 11 updates (API Level 30)

Support for the latest version of Android is part of an ongoing effort to expand mobile coverage. For this release, users should expect to see better modeling of Android applications that generally improve results. This release includes the new Android category, *Intent Manipulation: Redirection*. Intent Manipulation: Redirection can enable an attacker to access protected app components or content. Updates have been focused on the following namespaces:

- android.content
- android.location
- android.net
- android.net.http
- android.net.wifi
- android.net.wifi.aware
- android.net.wifi.hotspot2.pps
- android.text
- android.util

This release also includes additional support for the following categories:

- Access Control: Android Provider
- Code Quality: Obsolete
- Denial of Service
- Intent Manipulation
- Path Manipulation
- Privacy Violation
- Privilege Management: Android Location
- Privilege Management: Android Telephony
- Query String Injection: Android Provider
- Resource Injection
- Setting Manipulation
- System Information Leak

- Unreleased Resource: Sockets

## iOS 14 updates

Support for the latest iOS version (iOS 14) for both Foundation and UIKit frameworks is focused on the following Swift and Objective-C APIs:

- app extensions
- data structure - collections
- drag and drop
- file system access
- networking
- pasteboard

Users should expect to see improvements in the *Privacy Violation*, *System Information Leak*, and *Path Manipulation* categories.

## PHP updates (Version 8.0)

Updated support for PHP up to version 8.0. In particular, the release includes support for the following additional categories:

- Access Control: Anonymous LDAP Bind
- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute
- Session Fixation
- XML Entity Expansion Injection
- XML External Entity Injection

## PCI SSF Secure Software Standard 1.1

To support compliance activities of our customers who develop and assess payment software, correlation of the Micro Focus Fortify Taxonomy to PCI Secure Software Standard Version 1.1 of the PCI Software Security Framework 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:

**JavaScript improvements:**
The latest SSR release utilizes improved JavaScript support in SCA 21.1 to reduce the false positives related to the 'Window' and 'Document' interfaces and associated methods as well as JavaScript built-in types.

**False Positive improvements:**
Work has continued on removing false positives in this release. On top of other improvements, customers can expect to see additional removal of false positives in the following areas:

- Missing Check for Null Parameter in Java, and JVM languages.
- SQL Injection in COBOL.
- Cross-Site Scripting in .NET.
- Privacy Violation in Golang involving public keys.

- Command Injection in PHP.
- Path Manipulation duplicates in PHP.
- Mass Assignment: Insecure Binder Configuration in .NET when using Kendo UI.

**PHP Improvements:**
SSR team has improved PHP support to get more accurate default values and type information. Due to these changes, certain issues will be shown as removed and added.

## 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

#### Insecure Deployment: Unpatched Application (CVE-2020–14882)

A critical and easily exploitable remote code execution vulnerability in Oracle WebLogic Server identified by CVE-2020-14882 might allow unauthenticated attackers with network access through HTTP to achieve total compromise and takeover of vulnerable Oracle WebLogic Servers. The vulnerability affects the console component of Oracle WebLogic Server versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, and 14.1.1.0.0. This release includes a check to detect this vulnerability on the server.

#### Insecure Deployment: Unpatched Application (CVE-2021-31166)

A critical HTTP Protocol Stack Unauthenticated Remote Code Execution vulnerability identified by CVE-2021-31166 could be exploited by an attacker by sending a specially crafted packet to a targeted server utilizing the HTTP Protocol Stack (http.sys) to process packets. This stack is used by the Windows built-in Internet Information Services (IIS) server, Windows Remote Management WS-Management (WinRM), and Web Services for Devices (WSD) associated with Network Discovery. It might also be used by any other web servers that require exposure to the internet without using IIS. Therefore, this vulnerability is reachable via any system utilizing http.sys and enables remote code execution (RCE) on the target system. This release includes a check to detect the CVE-2021-31166 vulnerability on target web servers. Due to the nature of this check having the potential to cause a Windows Server to restart, this check is not included in the Standard Policy. Please use either the All Checks policy, customize an existing policy to include the check, or create a custom policy to run this check.

#### Insecure Deployment: Default Configuration

Apache Shiro uses the AES encryption algorithm to encrypt serialized user identity in its "rememberMe" cookie. Prior to version 1.2.5, if user has not defined a custom key, Shiro uses a default key in the AES encryption algorithm. This default configuration, which is identified as CVE-2016-4437, enables unauthorized attackers to easily encrypt untrusted serialized Java objects and decrypt the "rememberMe" cookie. The application is also vulnerable if user uses a "not unique" predefined key like keys from demo application in github. This release includes a check to detect the default key or leaked key of an AES encryption algorithm in the Shiro application.

### Insecure Deployment: Unpatched Application (CVE-2019-12422)

A specific Padding Oracle Attack vulnerability identified by CVE-2019-12422 can be exploited by attackers with a valid "rememberMe" cookie as the prefix. Apache Shiro uses an AES encryption algorithm to encrypt serialized user identity in its "rememberMe" cookie. Prior to version 1.4.2, Shiro uses CBC as default padding mode in the AES encryption algorithm. This release includes a check to detect the CVE-2019-12422 vulnerability on target web servers.

### 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:

**SSL check improvement:**
The SSR team has worked on refining the SSL checks to improve the performance. As a result of these changes, the check became more time efficient.

## Micro Focus Fortify Premium Content

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

### PCI SSF Secure Software Standard 1.1

To accompany the new correlations, this release also contains a new report bundle for Fortify SSC with support for PCI SSF 1.1, 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
Senior Manager, Software Security Research
Micro Focus Fortify
hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
Manager, Software Security Research
Micro Focus Fortify
peter.blay@microfocus.com



June 25 2021