Fortify Software Security Content

2021 Update 3

September 24, 2021

About CyberRes 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, CyberRes Fortify Software Security Content supports 1,051 vulnerability categories across 27 programming languages and spans more than one million individual APIs.

CyberRes
A Micro Focus Line of Business

Fortify Software Security Research (SSR) is pleased to announce the immediate availability of updates to Fortify Secure Coding Rulepacks (English language, version 2021.3.0), Fortify WebInspect SecureBase (available via SmartUpdate), and Fortify Premium Content.

CyberRes Fortify Secure Coding Rulepacks [SCA]

With this release, the Fortify Secure Coding Rulepacks detect 831 unique categories of vulnerabilities across 27 programming languages and span over one million individual APIs. In summary, this release includes the following:

Golang Standard Library updates (Version: 1.16)

Expanded support for Go standard library. 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. This update covers standard library namespaces, adding support for the following new categories:

- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute
- Go Bad Practices: Leftover Debug Code
- Insecure Randomness: Hardcoded Seed
- Insecure Randomness: User-Controlled Seed
- Insecure Transport: Cipher Suite Downgrade
- Insecure Transport: Weak SSL Protocol
- Often Misused: Privilege Management
- Weak Cryptographic Signature

Android 11 updates (API Level: 30)

Android platform is an open-source software stack designed for mobile devices. A primary component of Android is the Java API Framework, which exposes Android features to application developers. This release expands vulnerability detection in native Android applications written in Java or Kotlin that leverage Android's Java API Framework. Users should expect improved results from updates to Android application modeling and API coverage. This release also includes the following new privilege management weakness categories which provide guidance for dangerous Android permissions:

- Privilege Management: Android Activity Recognition
- Privilege Management: Android Calendar
- Privilege Management: Android Call Log
- Privilege Management: Android Camera
- Privilege Management: Android Contacts
- Privilege Management: Android Microphone
- Privilege Management: Android Sensors

iOS Standard Library updates (Version: iOS 14)

This release updates our support for the iOS 14 library APIs for both Swift and Objective-C. Updates are focused on the following frameworks:

- UIKit
- UserNotification
- SwiftUI
- MessageUI

Users should expect to see improvements in the Insecure IPC, Link Injection, Path Manipulation, Privacy Violation, Shoulder Surfing, and System Information Leak categories.

Micro Focus Visual COBOL updates (Version: 7.0)

Extended support for Micro Focus Visual COBOL version 7 to add support for the following two weakness categories:

- Integer Overflow
- Race Condition: File System Access

SAPUI5/OpenUI5 support[1] (Version: 1.93)

SAPUI5 is a client-side JavaScript framework, created by SAP, which shares a set of core control libraries with the open-sourced OpenUI5. This release provides initial support of identifying vulnerabilities for the following categories:

- Cross-Site Scripting: DOM
- Cross-Site Scripting: SAPUI5 Control
- Cross-Site Scripting: Self
- Privacy Violation
- SAPUI5 Misconfiguration: Unsanitized Editor
- System Information Leak: External

JSON support[2]

JavaScript Object Notation (JSON) is a lightweight data-interchange format. This release provides improved support to identifying vulnerabilities in JSON for the following categories:

- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Password in Comment[3]

[1] Improved results to be expected when using SCA v21.2.0 or above.
[2] Requires SCA v21.1.0 and the flag: '-Dcom.fortify.sca.use.json-analyzer=true'.
[3] Requires SCA v21.2.0 or above. No flag is required from SCA v21.2.0 onwards.

Kotlin Standard Library updates (Version: 1.4.30)

Kotlin is a general-purpose, statically-typed language featuring Java interoperability. This release includes updated support for new standard library APIs introduced in Kotlin 1.4 targeting the Java Virtual Machine (JVM).

ECMAScript 2021 (Version: ECMA-262)

Support for new APIs introduced in ECMAScript 2021. ECMAScript is a general-purpose programming language, as defined by the ECMAScript language specification, best known for being integrated into all modern web browsers. However, it is increasingly common to be used in order to build web servers, mobile applications, and other types of traditional applications. Customers should expect improved dataflow when scanning applications that targeting the latest ECMAScript standard.

2021 Common Weakness Enumeration (CWE™) Top 25

The Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) was introduced in 2019 and replaces SANS Top 25. Released in July, the 2021 CWE Top 25 was 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 CyberRes Fortify Taxonomy to the 2021 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 18.x:

As observed with the 2020.4 release, we are continuing to support the last four major releases of SCA. Therefore, this will be the last release of the Rulepacks that support SCA versions prior to 18.x. For the next release, SCA versions prior to 18.x will not load the most recent Rulepacks. This will require either downgrading the Rulepacks or upgrading the version of SCA.
For future releases, we will continue to support the last four major releases of SCA.

Java J2EE improvements:

Improved support for javax.servlet APIs in the *Privacy Violation* and *System Information Leak* categories.

Android Bound Services:

With our continued Android support, this release includes coverage for Android Bound Services. Customers can expect new dataflow issues originating from the Android Bound Service method parameters. This potentially can introduce duplicate dataflow sub-traces when methods are called within the bound service.

Weak Cryptographic Hash in Node.js:

Identify uses of weak cryptographic hashes in Node.js applications.

OWASP ASVS 4.0 mapping now contains support for levels

In support of customers who desire the ability to query reported issues that violate specific OWASP Application Security Verification Standard (ASVS) Application Security Verification Levels (L1, L2, and L3), the latest security content has added these levels to the mapping names. Customers are able to now search within the *OWASP ASVS 4.0* grouping for the related *L1*, *L2*, and *L3* keywords as well as design related filtersets and filtertemplates for use in AuditWorkbench and Software Security Center (SSC).

False Positive improvements:

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

- *Cross-Site Scripting* false positives in jQuery code
- *Privacy Violation: Shoulder Surfing* in .NET applications using JsonIgnore attribute
- More consistency in lowering Fortify Priority Order on *Path Manipulation* issues where only a number can be controlled
- We no longer identify passwords in Swift when they are part of an enumeration
- *Missing XML Validation* issues in .NET
- *Missing Check against Null* in Java projects

CyberRes 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: HTTP Request Smuggling

HTTP2 over clear text smuggling, or h2c smuggling, is an alternative to traditional HTTP request smuggling that abuses h2c-unaware frontends, such as proxy servers, to create a tunnel to backend systems. An attacker can use this tunnel to smuggle additional requests to the back-end server without detection by the front-end server. This can give attackers the ability to bypass authorization controls on frontends and access restricted resources on backend systems. This release includes a check to detect configurations that can be used for h2c smuggling attacks.

Access Control: Missing Authorization Check

GraphQL Introspection enables the querying of the server to obtain information about an underlying schema. Introspection gives details about elements such as queries, types, and fields. GraphQL Introspection is generally enabled by default. An attacker without proper authorization can misuse this information for attacks such as SQL Injection and batching attacks. This release includes a check to detect GraphQL endpoints that have introspection enabled.

NoSQL Injection: MongoDB

NoSQL script injection vulnerabilities allow attackers to inject malicious queries in the database. MongoDB is one of the NoSQL databases and its documentation states that it allows applications to run JavaScript operations. NoSQL Injection is very dangerous because an unauthenticated attacker can extract data or execute JavaScript code. This can lead to remote code execution, compromise of confidentiality, integrity of application data, and Denial of Service (DoS) attacks. This release includes a check to detect NoSQL script injection in MongoDB.

Dynamic Code Evaluation: Unsafe Deserialization

A pre-authorization insecure Java deserialization vulnerability in ForgeRock AM server before 7.0, and OpenAM server before 14.6.4, has been identified by CVE-2021-35464. This vulnerability allows attackers to craft a malicious serialized object in the jato.pageSession parameter and send it to the endpoint "/ccversion/Version" by a single request. The vulnerability exists due to the usage of an insecure third-party Java library in the application. This issue normally allows attackers to execute arbitrary code on the server, abuse application logic, or Denial of Service (DoS) attacks. This release includes a check to detect this vulnerability on target web servers.

Cross-Site Scripting: DOM[4]

Cross-Site Scripting occurs when dynamically generated web pages display user input, such as login information, that is not properly validated, allowing an attacker to embed malicious scripts into the generated page and then execute the script on the machine of any user that views the site. In case of Document Object Model (DOM)-based XSS, malicious content is executed as part of DOM manipulation. If successful, DOM Cross-Site Scripting vulnerabilities can be exploited to manipulate or steal cookies, create requests that can be mistaken for those of a valid user, compromise confidential information, or execute malicious code on end user systems. This release contains a new check to detect DOM XSS on client-side URI fragments.

Web Server Misconfiguration: Insecure Mapping Directives

Configuring Nginx to execute PHP on the web server sometimes advocates passing every URI ending in .php to the backend PHP interpreter (such as FastCGI). Nginx with this unsafe PHP configuration will consider the folders in the URL path as the target file to execute if the requested full path does not lead to an actual existing file. This misconfiguration allows attacker to execute arbitrary PHP code in any type of file, such as an image file, if it can be uploaded to the web server and be accessed. This release includes a check to detect this vulnerability on target web servers.

[4] Requires WI v21.2.0 or above.

Integer Overflow

Nginx versions since 0.5.6, up to and including 1.13.2, are vulnerable to an integer overflow vulnerability identified by CVE-2017-7529. This issue exists in the Nginx range filter module and allows an attacker to acquire potentially sensitive information by sending specially crafted request. This release includes a check to detect the CVE-2017-7529 vulnerability on target web servers.

Compliance Reports

2021 Common Weakness Enumeration (CWE™) Top 25

The Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) was introduced in 2019 and replaces SANS Top 25. Released in July, the 2021 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. This SecureBase update includes 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.

Policy Updates

CWE Top 25 2021

A policy customized to include checks relevant to CWE Top 25 2021 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:

LDAP Injection

This release includes improvements for the LDAP Injection check to reduce false positives and improve the accuracy of its results.

CyberRes Fortify Premium Content

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

2021 CWE Top 25

To accompany the new correlations, this release also contains a new report bundle for Fortify Software Security Center with support for the 2021 CWE Top 25, which is available for download from the Fortify Customer Support Portal under Premium Content.

CyberRes 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 CyberRes Fortify Support Portal.

Contact Fortify Technical Support

CyberRes Fortify
http://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

Contact SSR

Alexander M. Hoole
Senior Manager, Software Security Research
CyberRes Fortify
hoole@microfocus.com
+1 (650) 258-5916

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

September 24, 2021

CyberRes
A Micro Focus Line of Business