Micro Focus

Fortify Software Security Content

2018 Update 2

June 29, 2018

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 988 vulnerability categories across 25 programming languages and spans more than 999,000 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 2018.2.0), Fortify WebInspect SecureBase (available via SmartUpdate), Fortify Application Defender, and Fortify Premium Content.

Micro Focus Fortify Secure Coding Rulepacks [SCA]

With this release, the Fortify Secure Coding Rulepacks detect 786 unique categories of vulnerabilities across 25 programming languages and span over 999,000 individual APIs. In summary, the release includes the following:

ASP.NET Core 2.0

Initial support for ASP.NET Core 2.0 covers detection of weaknesses across controllers and models of ASP.NET Core MVC applications. Vulnerability category coverage includes the following:

- ASP.NET Bad Practices: Non-validated Web API Model
- ASP.NET MVC Bad Practices: Controller Action Not restricted to POST
- ASP.NET MVC Bad Practices: Controller Action Without AntiForgery Validation
- ASP.NET MVC Bad Practices: Model With Optional and Required Properties
- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set
- Cookie Security: Overly Broad Domain
- Cookie Security: Overly Broad Path
- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Denial of Service: Regular Expression
- Formula Injection
- Header Manipulation
- Header Manipulation: Cookies
- Mass Assignment: Insecure Binder Configuration
- Mass Assignment: Request Parameters Bound into Persisted Objects
- Open Redirect
- Path Manipulation
- Privacy Violation
- Privacy Violation: Shoulder Surfing
- System Information Leak: External

JavaScript MySQL

Support for MySQL in JavaScript projects includes detection of SQL Injection and Access Control: Database issues.

JavaServer Faces (JSF) improved support

Java security content now supports JSF up to version 2.3 and includes features introduced in 2.1 and 2.2 such as improved CDI alignment and newly introduced JSP tags. As part of the updated support, the following new category has been added:

- Denial of Service

MongoDB

Improved support for Java and .NET client APIs includes better detection for NoSQL Injection, extended DATABASE sources, and new vulnerability categories such as:

- Denial of Service: Regular Expression
- Dynamic Code Evaluation: Code Injection
- Unauthenticated Service: MongoDB

Spring Data

New support for Java Spring Data covers the following modules: Spring Data Commons, Spring Data JPA, Spring Data MongoDB, Spring Data Redis, and Spring Data REST / Spring HATEOAS. Coverage includes Spring Data repositories and dynamic query methods as well as the inclusion of new categories such as:

- Unauthenticated Service: MongoDB
- Unauthenticated Service: Redis
- Dynamic Code Evaluation: Unsafe BeanUtils Deserialization

Spring Webflow

New support for Java Spring Webflow 2.x, and improved support for 1.x, includes the ability to detect the following two new vulnerability categories for Java:

- Mass Assignment: Insecure Binder Configuration
- Missing Form Field Validation

Swift 4[1]

Extended support for detecting weaknesses in iOS apps now includes coverage of new and modified APIs in Swift 4, such as changes to the String and Collection classes, Archival and Serialization, Key-Value Coding, and Generic Subscripts.

Java Path Manipulation: Zip Entry Overwrite improvements

Lately, there have been headlines about the recently detected vulnerabilities of a known weakness type related to the processing of Zip files (Zip Slip). Existing support for detecting Path Manipulation: Zip Entry Overwrite has been revamped for Java to now detect additional weaknesses using dataflow analysis.

DISA STIG 4.6 and DISA CCI correlation

In order 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 4.6, has been added. Furthermore, in order to more easily report and align reported vulnerability issues with NIST SP 800-53 Controls Fortify results now provide correlation to the DISA Control Correlation Identifiers (CCI).

[1] Translation and scanning of Swift 4 projects require Fortify SCA version 18.11 or above.

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

Cross-Site Scripting

Edge side includes (ESI) is a markup language used in various HTTP devices, such as reverse proxies and load balancers, that are positioned between client and server. An attacker can inject ESI markup to perform critical attacks such as cross-site scripting and HTTPOnly cookie protection bypass. This release includes an enhancement to cross-site scripting check to evaluate applications for ESI injection in addition to existing cross-site scripting attack combinations.

Directory Traversal

Spring Framework by Pivotal has been found to be vulnerable to Directory Traversal attack identified by CVE 2018-1271. The vulnerability allows an attacker to manipulate URLs that serve static resources from the file system and can lead to a directory traversal attack. This release contains a check to detect the presence of non-validated user input sent to URLs that may result in this vulnerability.

Insecure Deployment: Unpatched Application

A critical remote code execution vulnerability in Drupal content management system (CMS) identified by CVE-2018-7600 allows remote attackers to execute arbitrary code on server. This release includes a check to detect this vulnerability in applications deploying Drupal CMS.

Object Injection

Deserializing user provided, or untrusted data, can cause the system to load and create an object of an arbitrary attacker-specified type, potentially leading to dynamic code execution during the deserialization process. This release includes a check to detect this vulnerability in PHP scripts on web server.

Expression Language Injection: Spring

A critical Spring Expression Language injection vulnerability identified by CVE-2018-1273 affects Spring Data Commons, versions prior to 1.13.10, 2.0 to 2.0.5. A remote attacker can supply specially crafted request parameters against Spring Data REST backed HTTP resources or using Spring Data's projection-based request payload binding that can lead to a remote code execution attack. This release includes a check to detect this vulnerability in Spring Data applications.

Insecure Transport: TLS_RSA

Return Of Bleichenbacher's Oracle Threat (ROBOT) is a vulnerability in the implementation of the RSA PKCS#1v1.5 algorithm that allows an attacker to decrypt and encrypt arbitrary cipher text without access to the server's private key. This release includes a check to detect this vulnerability on the server. The check performs various combinations of attack methods detailed in ROBOT attack research paper[2].

Privacy Violation: National ID Disclosure

This check detects the presence of National IDs in HTTP traffic that compromises an individual's privacy and is in violation of the GDPR regulation that went into effect on May 25, 2018. This check is available to our customers as part of the GDPR policy. The 10 EU countries currently supported by this check include:

- Belgium
- Denmark
- Finland
- France
- Germany
- Netherlands
- Poland
- Spain
- Sweden
- United Kingdom

Compliance report

DISA STIG 4.6 and DISA CCI correlation

In order 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 4.6, has been added. Furthermore, in order to more easily report and align reported vulnerability issues with NIST SP 800-53 Controls, this release contains a new compliance template that maps WebInspect checks to the DISA Control Correlation Identifiers (CCI).

Policy Updates

A policy customized to include checks relevant to DISA STIG 4.6 has been added to the existing list of supported policies in WebInspect SecureBase.

[2] Return Of Bleichenbacher's Oracle Threat

Micro Focus Fortify Application Defender

Fortify Application Defender is a runtime application self-protection (RASP) solution that helps organizations manage and mitigate risk from homegrown or third-party applications. It provides centralized visibility into application use and abuse while protecting from software vulnerability exploits and other violations in real time. For this release, the Micro Focus Fortify Software Security Research team provides the following feature improvements:

NoSQL Injection: MongoDB

A new rule has been added to extend existing coverage to detect the NoSQL Injection: MongoDB on the .NET platform. The new rule covers NoSQL Injections in applications with MongoDB C#/.NET Driver version 1.x and 2.x.

Micro Focus Fortify Premium Content

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

DISA STIG 4.6 and DISA CCI reports

To accompany the new correlations, this release also contains a new report bundle with support for DISA STIG 4.6 and DISA CCI, 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, containing descriptions for newly added category support, is available at https://vulncat.fortify.com. Customers looking for the legacy site, with the last supported update, may 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 29 2018