



Hewlett Packard Enterprise

Software Security Research Release Announcement

HPE Security Fortify Software Security Content

2016 Update 3

September 30, 2016

HPE Security Fortify Software Security Research (SSR) is pleased to announce the immediate availability of updates to HPE Security Fortify Secure Coding Rulepacks (English language, version 2016.3.0), HPE Security Fortify WebInspect SecureBase (available via SmartUpdate), HPE Security Fortify Application Defender, and HPE Security Fortify Premium Content.

About HPE Security SSR

The Software Security Research team translates cutting-edge research into security intelligence that powers the HPE Security products portfolio. Today, HPE Security Fortify Software Security Content supports 907 vulnerability categories across 23 programming languages and spans more than 840,000 individual APIs.

Learn more at

hpe.com/software/ssr

HPE Security Fortify Secure Coding Rulepacks [SCA]

With this release, the Fortify Secure Coding Rulepacks detect 709 unique categories of vulnerabilities across 23 programming languages and span over 840,000 individual APIs. In summary, the release includes the following:

iOS WatchKit¹

New support for *WatchKit*, *WatchConnectivity*, and *ClockKit* frameworks has been added to both Objective-C and Swift rulepacks to enable detection of vulnerabilities spanning from iOS apps to watchOS interfaces via WatchKit extensions. Category coverage for these frameworks includes *Privacy Violation*, *System Information Leak*, and *System Information Leak: External*.

LDAP Entry Poisoning²

Fortify SCA can now find instances of LDAP Entry Poisoning vulnerabilities. This new vulnerability category coverage, which was presented by HPE Security Fortify Software Security Research team at BlackHat USA 2016, allows attackers in control of an LDAP entry to compromise vulnerable applications by performing a search on the entry. This vulnerability is especially pervasive in applications that integrate with LDAP directories for authentication purposes.

Extended support for improperly configured encryption keys

Improper use of cryptographic APIs, related to key management, can reduce the security of applications. Additional rules coverage has been added to ABAP, ActionScript, CFML, JavaScript, SQL, and VB6 to identify the following categories, where appropriate:

- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key

¹ Requires HPE Security Fortify SCA 16.10.

² Blog [post](#) and [whitepaper](#) on LDAP Entry Poisoning are available online.

ASP .NET insecure settings

ASP.NET offers several application level settings to support backward compatibility. Enabling these settings, however, may pose a significant security risk to the application or to the server. Two new sub-categories have been introduced with this release to detect these insecure settings in ASP.NET applications.

- Access Control: Form Authentication Bypass
- ASP.NET Misconfiguration: Missing HMAC Signature

Rule coverage has also been improved to detect insecure settings under several existing categories, including the following: *Denial of Service*, *Dynamic Code Evaluation: Unsafe Deserialization*, and *Open Redirect*.

DISA STIG 4.1

In order to support our federal customers in the area of compliance, this release supports correlation between the HPE Security Fortify Taxonomy categories and the STIG IDs from the latest, and completely revamped, version of the Defense Information Systems Agency Application Security and Development STIG, version 4.1.

HPE Security Fortify SecureBase [WebInspect]

HPE SecureBase combines checks for thousands of vulnerabilities with policies that guide users in following updates available immediately via SmartUpdate:

Vulnerability support

XPath Injection³

Constructing a dynamic XPath query with user input could allow an attacker to modify the statement's meaning. This may allow attackers to gain unauthorized access to sensitive data. This release includes a check to identify XPath injection vulnerabilities in web applications.

Server-Side Template Injection³

Server-Side template provides a way for web page designers to use language expressions in web design in order to render dynamic data generated in models. Expressions can be constructed and evaluated during runtime, thereby, opening web applications to injection attacks. This release includes a check to detect such Server-Side Template Injection attacks. This new check addresses the popular *Django*, *FreeMarker*, *Twig* and *Velocity* templating frameworks with this version.

Weak SSL Protocol: TLS 1.1

NIST publication 800-52 revision 1 recommends all web applications to prefer Transport Layer Security Protocol version 1.2 (TLS 1.2) and mandates government agencies to develop a migration plan for TLS1.2 by January 2015. TLS1.1 is considered weak by crypto experts due to its use of MD5 and SHA1 hash algorithms which are considered weak and now not recommended. This release includes a check to mark TLS1.1 as weak to bring in attention a deadline for migration plan to TLS1.2.

HPE Security Fortify SSR
hpe.com/software/ssr

Contact

Alexander M. Hoole
Manager, Software Security Research
HPE Security Fortify
hoole@hpe.com
+1 (650) 265-5296

³ Requires HPE Security Fortify WebInspect 16.20.

Compliance Report

DISA STIG 4.1 Compliance Template

This release includes a new compliance template to provide support for the latest version of the Defense Information Systems Agency Application Security and Development STIG, version 4.1. The Department of Defense completely revamped the DISA STIG to align with the requirements specified in NIST SP 800-53, marking a significant improvement and difference from the earlier versions.

Improved OWASP 2013 Compliance Template

This release includes improved correlation of checks with OWASP Top 10 2013. The improvements include correlation to many additional checks as well as an alignment to the OWASP Top 10 report generated for HPE Security Fortify SCA scans and HPE Security Fortify Taxonomy categories integrated within HPE Security Fortify Software Security Center (SSC).

HPE Security Fortify Application Defender

HPE Security 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 HPE Security Fortify Software Security Research team provides the following feature improvements:

Context Sensitive Cross-Site Scripting (CsXss) detection

New and powerful CsXss detection further improves our protection for XSS issues. CsXss is a non-signature based detection and it can accurately detect attack vectors that signatures cannot. It can detect Reflected and Persistent XSS issues regardless of where the malicious data is coming from. CsXss currently supports ASP.NET only and will extend to other technology in the near future.

SQL Injection

SQL Injection protection is improved with support for automatic connection cleanup in order to prevent connection leaks in Hibernate, JDO, and JPA.

Improved accuracy

Various enhancements to Cross-Site Scripting and SQL Injection signatures.

HPE Security Fortify Premium Content

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

DISA STIG 4.1 report

To accompany the new mapping, this release contains a new report bundle with support for DISA STIG 4.1, which is available for download from the Fortify Customer Portal under Premium Content.

HPE Security Fortify Taxonomy: Software Security Errors

New DISA STIG 4.1 correlations to the HPE Security Fortify Taxonomy, along with the latest additional weakness categories, are now viewable on the updated Vulncat [website](#).

The legacy HPE Security Fortify Taxonomy site at <https://vulncat.fortify.com> will no longer be available online after Dec 31, 2016. Moving forward please use <https://vulncat.hpefod.com>.

© Copyright 2016 Hewlett Packard Enterprise Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HPE products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.