



Hewlett Packard Enterprise

Software Security Research Release Announcement

HPE Security Fortify Software Security Content

2016 Update 1
March 31, 2016

HPE Security Fortify Software Security Research (SSR) is pleased to announce the immediate availability of updates to HPE Security Application Defender, HPE Security WebInspect SecureBase (available via SmartUpdate), HPE Security Fortify Secure Coding Rulepacks (English language, version 2016.1.0), 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 900 vulnerability categories across 23 programming languages and spans more than 836,000 individual APIs.

Learn more at

hpe.com/software/ssr

HPE Security Application Defender

Managed from the cloud, Application Defender is a software-as-a-service (SaaS) solution that protects production applications against software security vulnerabilities. For this release, the Software Security Research team provides the following feature improvements:

Dynamic Code Evaluation: Unsafe Deserialization

A new non-signature based protection which creates a sandbox Java Security Manager on the fly during deserialization to detect usage of dangerous APIs such as those for making network connection or deleting a file.

Minor enhancements

Improved Header Manipulation now take actions only if the underlying application server is vulnerable, improved XSS signatures and various bug fixes.

HPE SecureBase [WebInspect]

HPE SecureBase combines checks for thousands of vulnerabilities with policies that guide users in identifying critical weaknesses in web and mobile software. In summary, this release includes the following updates available immediately via SmartUpdate:

Vulnerability support

Dynamic Code Evaluation: Unsafe Deserialization

Deserialization vulnerabilities have plagued web applications for a while. However, recent revelations about the commonality and exploitability of this vulnerability have put a renewed attention on detection and remediation of these issues. This release includes an API agnostic check to detect this vulnerability in web applications.

Often Misused: File Upload

Attackers can abuse a file upload functionality to upload dangerous or executable contents to run on the server. This release includes a check to detect if application accepts dangerous scripts or executable contents.

SAP HANA SQL Injection Support¹

WebInspect SQL Injection detection includes the database type and name as evidence of a successful injection in the vulnerability report to aid audit scan results. This release includes support for SQL Injection detection in SAP HANA.

XML Entity Expansion Injection¹

XML entities act as string substitution macros in XML block. An attacker can exhaust the CPU resources on server denying service to other requests by nesting recurrent entity resolutions in a well-defined XML block in user input. This attack is known as XML Entity Expansion or XML Bomb. This release includes a check to detect XML Entity Expansion vulnerability in web applications.

Compliance Report

DISA STIG 3.10

Defense Information Systems Agency has updated guidance on performing security testing of applications. This release includes a new compliance template to classify and report vulnerabilities according to Application Security and Development STIG, version 3.10.

HPE Security Fortify Secure Coding Rulepacks [SCA]

With this release, the Fortify Secure Coding Rulepacks detect 696 unique categories of vulnerabilities across 23 programming languages and span over 836,000 individual APIs. In summary, the release includes the following:

Swift support²

Swift is becoming the defacto language for iOS applications and is extending quickly to other platforms. Initial support for the Swift programming language covers 38 categories spanning Privacy Violation, Key Management, Password Management, Weak Cryptographic Hash, Weak Encryption, Cookie Security, Insecure SSL, Insecure Storage, among others.

SAP Java Web Dynpro

SAP Web Dynpro is increasingly the preferred technology for developing web applications in SAP environments. This rulepack now supports 14 categories in Web Dynpro for Java, including the following:

- Access Control: Database
- Insecure Transport
- Portability Flaw: Native SQL
- Process Control
- Server-Side Request Forgery
- SQL Injection

Dynamic Code Evaluation: JNDI Reference Injection

Attackers able to control the address of any JNDI context lookup may be able to execute arbitrary code remotely. New rulepack adds support for detecting this new type of vulnerability, Dynamic Code Evaluation: JNDI Reference Injection, where user-controlled addresses are used in JNDI context lookup operations.

¹ Requires HPE Security WebInspect 16.10.

² Requires HPE Security Fortify SCA 16.10.

Azure Storage – Node.js

Azure-storage Node.js package provides an elegant way to access and manage Microsoft Azure storage services such as Table & Queue and Blob. In the support of Azure Storage - Node.js package, rule coverage has been expanded to include the following categories:

- Access Control: Azure
- Access Control: Database
- Path Manipulation
- Password Management: Hardcoded Password
- Password Management: Weak Cryptography
- Resource Injection

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

.NET improvements

The "My" feature provides easy and intuitive access to a number of .NET Framework classes, enabling the Visual Basic.Net user to interact with the computer, application, settings and resources. Increased rule coverage for "My" feature includes Microsoft.VisualBasic.MyServices, Microsoft.VisualBasic.Devices & Microsoft.VisualBasic.ApplicationServices namespaces for the following categories:

- Path Manipulation
- Portability Flaw
- Privacy Violation
- Registry Manipulation
- System Information Leak

Java Serialization

Attackers can use classes in your own application codebase to assemble dangerous code chains to be executed during deserialization of any object. This update adds support for finding these classes (gadgets) within scanned code that could be abused by attackers during a Java deserialization attack.

DISA STIG 3.10 Mappings

In order to support our federal customers in the area of compliance, this release contains the mapping of the HPE Security Fortify Taxonomy to the latest version of the Defense Information Systems Agency Application Security and Development STIG, version 3.10.

HPE Security Fortify Premium Content

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

DISA STIG 3.10 Report

To accompany the new mapping, this release also contains a new report bundle with support for DISA STIG 3.10, which is available for download from the Fortify Customer Portal under Premium Content.

© 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.