



# Hewlett Packard Enterprise

---

Software Security Research Release Announcement

## HPE Security Fortify Software Security Content

2015 Update 4

December 18, 2015

---

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 2015.4.0), 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 895 vulnerability categories across 22 programming languages and spans more than 835,000 individual APIs.

### **Learn more at**

[\*\*hpe.com/software/ssr\*\*](http://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:

#### **XPath Injection for Java and .NET platforms**

XPath Injection allows an attacker to alter the query structure and therefore allows him to access XML data he normally cannot. The attack is protected by Application Defender on the following supported libraries: Apache Xerces, JDOM, .NET System.XML.

#### **Dynamic Code Evaluation: Unsafe Deserialization**

Deserializing objects from untrusted data stream can lead to remote code execution. A "Deserialization Firewall" is now implemented in Application Defender to detect if the application is deserializing any forbidden data classes.

#### **.NET 4.5 granular request validation**

Improved .NET 4.5 granular request validation support.

### **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.

### **Vulnerability support**

#### **HTTP Verb Tampering**

Web applications that use verb-based authentication and access control are susceptible to HTTP Verb tampering attacks that bypass access control systems. A new check has been added to detect if the system's authentication and access control measures can be bypassed to access restricted system resources.

### **Overly verbose error during login**

Inconsistent error messages, detailing specifics of the failed control during a login failure, may allow an attacker to enumerate and identify application users. A new check has been added to detect the presence of such inconsistent feedback during a failed login sequence.

### **Weak Password Policy**

The security and reliability of a password-based authentication system depends on the strength of the password. Password policies that ensure users create strong passwords are therefore crucial to deploying secure websites. A new check flags applications that do not enforce the minimum set of requirements for a strong password.

### **Archived directories**

Enhancements to WebInspect now provides the capability to detect various archived directories that are deployed along with the application. Several checks have been added to detect such directories that are specific to the application being tested.

## **SecureBase enhancements**

### **Password disclosure detection**

Updates have been made to existing checks to more accurately detect the presence of login credentials in sessions, cookies and HTTP queries, thus improving the confidence of the reported vulnerabilities.

### **Open Redirect improvements**

Changes to the detection of the open redirect vulnerability now allows for the detection of script-based redirects in applications that use JavaScript to initiate a redirection, by using WebInspect's advanced script engine.

## **HPE Security Fortify Secure Coding Rulepacks [SCA]**

With this release, the Fortify Secure Coding Rulepacks detect 691 unique categories of vulnerabilities across 22 programming languages and span over 835,000 individual APIs. In summary, the release includes the following:

### **Enhanced core JavaScript support<sup>1</sup>**

Improvements to core JavaScript support include handling of anonymous functions, callbacks, as well as function and variable aliasing. Additionally, the coverage of standard APIs has been expanded to indexed collections and structured data, including JSON.

### **Node.js support<sup>2</sup>**

Support for core Node.js modules including handling callbacks and events via EventEmitter APIs. This is the first support for server-side JavaScript and included in the support for 18 categories are several primarily server related categories, previously not supported for client-side JavaScript, such as:

- Command Injection
- JSON injection
- XML injection
- Persistent and Reflected Cross-Site Scripting
- Log Forging

---

<sup>1</sup> Requires HPE Security Fortify SCA version 4.40 or higher. In addition, enhanced JavaScript support requires JavaScript to be enabled as a language using higher order analysis.

<sup>2</sup> Requires HPE Security Fortify SCA version 4.42 or higher. In addition, Node.js support requires JavaScript to be enabled as a language using higher order analysis.

### **jQuery support<sup>3</sup>**

Support for jQuery core APIs, including understanding of the DOM model for jQuery selectors, jqXHR objects, along with handling of callbacks and event handling. Enhancements span 11 categories and also include limited support for deprecated event binding APIs in order to follow dataflow correctly.

### **Android improvements<sup>3</sup>**

Improvements to Android support include the ability to track data flow through callbacks.

### **Expression language resolution support<sup>3</sup>**

Support for Spring EL and Struts 2 OGNL resolution, effectively connecting views and controllers/actions for improved vulnerability inspection and complete dataflow analysis.

### **Java8 lambda support<sup>4</sup>**

Support for Java APIs taking lambdas as parameters. New support models lambda execution derived from these APIs.

### **Java Unsafe Deserialization**

A new category has been added to the Java rulepack: Dynamic Code Injection: Unsafe Deserialization. This category reports unsafe deserialization of untrusted data within application, library, or framework code that can allow attackers to compromise the application.

### **JMX support**

Added support for Java Management Extension (JMX) entrypoints and sinks within Spring and J2EE frameworks.

### **Spring JMS support**

Support for Spring JMS and new Spring Messaging module (that contains some JMS wrappers) now tracks untrusted input from network sources and reports categories such as Resource Injection and System Information Leak.

### **.NET improvements and database provider specific ADO.Net support**

Improved coverage for vendor specific ADO.Net libraries, spanning 14 categories, for major databases such as MySQL, Sybase ASE, Oracle, IBM DB2, Informix, nPGSql, and Sqlite. Support for two additional categories are also provided for core .NET: Code Correctness: Readonly Collection Reference, and Uninitialized Variable.

### **HPE Security Fortify SSR**

[hpe.com/software/ssr](http://hpe.com/software/ssr)

### **Contact**

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

---

<sup>3</sup>Requires HPE Security Fortify SCA version 4.40 or higher. In addition jQuery support requires JavaScript to be enabled as a language using higher order analysis during the scan phase, and DOM modeling to be enabled during the translation phase.

<sup>4</sup> Requires HPE Security Fortify SCA version 4.42 or higher.

© Copyright 2015 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.