

HPSR Software Security Content



2014 Update 4

December 19, 2014

HP Software Security Research is pleased to announce the immediate availability of updates to HP Application Defender, HP WebInspect SecureBase (available via SmartUpdate), the HP Fortify Secure Coding Rulepacks (English language, version 2014.4.0), and HP Fortify Premium Content.

About SSR

The Software Security Research team translates cutting-edge research into security intelligence that powers the HP Enterprise Security Products portfolio. Today, HPSR Software Security Content supports over **890** vulnerability categories across **22** programming languages and spans more than **815,000** individual APIs.

HP Application Defender

Managed from the cloud, HP 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 highlights:

ClassLoader Manipulation: Apache Struts

- Remote code execution likely tops the list of issues you'd rather not expose to the world via the Internet. This featured security content item protects your applications against the recent Apache Struts remote code execution advisory as described in [CVE-2014-0112](#) and [CVE-2014-0114](#).

Support for the Google Web Toolkit (GWT) x-gwt-rpc protocol

- Supporting GWT enables HP Application Defender to securely inspect parameters sent from client browsers to GWT RPC objects hosted on the server side; further extending the reach of real-time application protection.

Improved protection for file upload features

- Much as "there's more than one way to do it" with Perl, there's more than one way to exploit cross-site scripting (XSS). HP Application Defender now protects against files uploaded in HTTP multipart data that may also be used as a vehicle to execute XSS attacks.

Protection from the latest XML attacks

- Weaknesses in XML parsing logic can lead to vulnerabilities categorized as XML entity expansion and XML external entity injection. Protect your production applications today from resource exhaustion, remote file inclusion attacks, and more with this rulepack.

HP SecureBase (WebInspect)

HP SecureBase combines checks for thousands of vulnerabilities with policies that guide users in identifying critical weaknesses in web and mobile software.

POODLE attack detection

Shortly after its initial disclosure, HPSR's Software Security Research team released immediate support for a critical Transport Layer Security issue identified by [CVE-2014-3566](#) - dubbed POODLE, or Padding Oracle on Downgraded Legacy Encryption.

Enriched Transport Layer Security support

- **SSL certificates signed using the MD5 hash**

The MD5 hash is susceptible to collision attacks and is deemed insecure for protecting the confidentiality of sensitive data in transit. HP WebInspect now ensures that certificates are signed using strong hashing algorithms.

- **Detecting unknown Certificate Authorities**

Ensure SSL implementations preserve the critically important concept of non-repudiation and uncover the unsafe practice of using self-signed certificates.

- **Weak SSL protocol – SSLv3**

SSL 3.0 is no longer considered a secure protocol, namely due to the absence of strong cipher support and the emergence of attacks such as POODLE.

Application configuration support

- **Insufficient Session Expiration**

Valid but inactive sessions increase the probability of success for session hijacking threats by allowing attackers to reuse or brute-force session identifiers stolen over time. This release includes a runtime agent to detect inadequate session expiration limits.

- **Misconfigured Application Cache Manifest**

Offline caching brings improved performance and usability to web applications. However, a misconfigured offline cache manifest can prevent timely updates of offline content, resulting in stale functionality that may have unintended consequences.

Privacy violations

- **Mobile MAC address disclosure**

Unauthorized access to Media Access Control (MAC) addresses can pose privacy concerns for the user of the device. This content update includes the ability to identify mobile applications that use and send MAC identifiers in web requests.

Compliance templates

DISA STIG 3.9

- Support for the latest version of the Defense Information Systems Agency Application Security and Development STIG, version 3.9.

HP Fortify Secure Coding Rulepacks (SCA)

With this release, the HP Fortify Secure Coding Rulepacks detect **624** unique categories of vulnerabilities across **22** programming languages and span over **815,000** individual APIs. In summary, the release includes the following:

Mass assignment

- Mass assignment, also known as over-posting or auto-binding, refers to a category of vulnerabilities that allow an attacker to abuse framework capabilities to bind requests to complex domain objects, enabling them to influence the value of object properties that were not supposed to be exposed for request binding. New supported categories include: Mass Assignment: Insecure Binder Configuration and Mass Assignment: Sensitive Field Exposure.
- The following frameworks are supported:
 - *Java*: Spring MVC, Struts 1, Struts 2, Restlet, JAX-RS, Spring REST
 - *Microsoft .NET*: ASP.NET MVC, ASP.NET WebForms, ASP.NET WebAPI

MyBatis 3 support

- Support for MyBatis 3 for Java, to improve upon existing iBatis 1.2, including support for testing SQL Injection within both configuration files and annotations.
- Detection of mapper files for data going into, and coming out of, the database is provided by a new category SQL Injection: MyBatis Mapper.
- Updates include coverage for 16 categories, including SQL Injection, Privacy Violation, System Information Leak, and XPath Injection.

HP Software Security Research

hp.com/go/ssr

Contact

Joe Sechman
Director, Software Security Research
HP Security Research
sechman@hp.com
+1 (770) 343 - 7052

JSON libraries

- Support for JSON libraries is crucial to enable SCA to follow dataflows through JSON serialization/deserialization operations. This is especially relevant for mobile applications and REST services that heavily use JSON to exchange data. New rulepacks add support for JSON libraries for multiple languages:
 - *Java*: Jackson, Gson, org.json, javax.json
 - *Microsoft .NET*: JSON.NET, NativeDataContractJsonSerializer class, FastJSON
 - *PHP*: Native JSON methods
 - *Python*: Json module
 - *Objective-C*: Native NSJSONSerialization class

OWASP Java HTML sanitizer

- Support for detecting potential XSS vulnerabilities under the category Insecure Sanitizer Policy in Java projects using OWASP HTML Sanitizer.

Enhanced SAP ABAP support¹

- Support for methods of GUI Frontend Services Utility and related APIs in the preview ABAP rulepack to be used with the new SCA ABAP translator². Categories covered are Access Control: Database, Command Injection, Obsolete, Path Manipulation, and Resource Injection.

DISA STIG 3.9

- Support for the latest version of the Defense Information Systems Agency (DISA) Application Security and Development STIG, version 3.9.

HP ArcSight Application View

HP ArcSight Application View automatically monitors applications to provide unparalleled insight into application behavior, enabling comprehensive visibility into threats that would otherwise go unnoticed. This release contains the following new features and enhancements:

Deeper insight into database activity

- Dashboard views now display multi-layer visibility for your database activities, providing a clearer, more accurate picture of the behavior of your applications. These new dashboards include visibility for overall database health, suspicious activity, and more.

HP Fortify Premium Content

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

DISA STIG 3.9 report²

- A new report bundle with support for DISA STIG 3.9 is available for download from the Fortify Customer Portal under Premium Content.

¹ Requires HP Fortify SCA 6.20 for Technology Preview functionality or later SCA versions.

² Requires HP Fortify SSC 4.20

Learn more at

hp.com/go/hpsr

