

HPSR Software Security Content



2015 Update 1

March 31, 2015

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 2015.1.0), 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 **931** vulnerability categories across **22** programming languages and spans more than **825,000** 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 improvements:

Dangerous File Inclusion

- File inclusion allows an attacker to retrieve sensitive files. Fortify will now protect against this attack regardless whether the file is hosted on the local file system or in a remote location.

Improved signatures

- Various signature improvements in Cross-Site Scripting, SQL Injection, and XML External Entity Injection to lower false positives as well as improve overall accuracy.

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.

Vulnerability support FREAK vulnerability

- The OpenSSL issue described in CVE-2015-0204 allows attackers to trick OpenSSL-based clients into downgrading the cipher to a known-to-be-weak export-class cipher, thus compromising the secrecy and integrity of the secure communication. Users can prevent exploitation of this vulnerability on their server by disabling export-class ciphers in their server configuration. This release includes improvements to the check for detecting weak ciphers in order to enable flagging of export-class ciphers that enable FREAK conditions on the server.

Updated standard policy

- The standard policy guides users in identifying critical weaknesses with a default selection of checks covering numerous web technologies. As technologies enter end of life and fade out of the technical landscape, it is necessary to prune the policy from time to time to remove checks that are no

longer technically necessary. The improved standard policy is tailored to include checks most relevant to security weaknesses in current web environments. This in turn improves overall scan performance and the quality of results without sacrificing accuracy. Our testing has shown performance improvement to be between 3% and 7.5%; however, the actual performance gain metric is largely based on the application and environment variables. The original version of the policy is now available as Standard (Deprecated).

HP WebInspect Agent Technology

Mass Assignment Injection: Insecure Binder Configuration

- A new rule has been added to detect Mass Assignment, also known as over-posting or auto-binding. This refers to a category of vulnerabilities that allow an attacker to abuse framework capabilities by binding request parameters to complex domain objects, enabling them to influence the value of fields of object properties that were not supposed to be exposed for request binding.

Feature Enhancements

Admin Section Must Require Authentication (check ID 4721)

- Administration features within a web application should only be exposed behind some form of authentication. This may include network authentication, application authentication, or a combination of both. This check now improves the ability to detect and analyze different forms of authentication in a more reliable manner, thus reducing false negatives and false positives.

JSON Hijacking (check ID 10733)

- It is possible to override a JavaScript Array constructor to disclose the payload of the array. The regexes used to detect this vulnerability have been optimized in this update to make the check faster and more accurate.

HP Fortify Secure Coding Rulepacks (SCA)

With this release, the HP Fortify Secure Coding Rulepacks detect **669** unique categories of vulnerabilities across **22** programming languages and span over **825,000** individual APIs. In summary, the release includes the following:

Enhanced iOS Coverage

- New support for iOS8 WebKit API¹.

Enhanced Ruby support²

- Enhanced Ruby core and third-party library coverage, along with new support for the following commonly used gems: *Thor*, *pg*, and *sqlite3*³. Updates provide support for an additional **37** vulnerability categories, including a new category for Connection String Parameter Pollution.

Improved Python and Django support

- Improved support for the Python Django⁴ framework, spanning **59** vulnerability categories, including **18** new categories:

¹ Requires HP Fortify SCA 6.30.

² Ruby support requires SCA 6.30. SCA 6.20 technical preview will no longer be supported by this and subsequent rulepacks.

³ The RubyGems *pg* and *SQLite3* require updated stub libraries available from Premium Content (see Premium Content section).

⁴ Django support requires Higher Order Analysis and Type Inference features enabled. Use "--django-template-dirs" to point to Django template directories.

**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

- Cookie Security: CSRF Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set on CSRF Cookie
- Cross-Frame Scripting
- Django Bad Practices: Blacklisted Attributes
- Django Bad Practices: Cookie Stored Sessions
- Django Bad Practices: Overly Broad Host Header Verification
- Django Bad Practices: Pickle Serialized Sessions
- File Disclosure: Django
- HTML5: Misconfigured Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- Insecure Deployment: Non Production Ready
- Insecure Deployment: Predictable Resource Name
- Insecure Transport: HSTS Does Not Include Subdomains
- Insecure Transport: HSTS not Set
- Insecure Transport: Insufficient HSTS Expiration Time
- JavaScript Hijacking: Constructor Poisoning
- Memcached Injection
- Privacy Violation: BREACH

Misuse of Cryptographic APIs

This release includes **27** new vulnerability categories related to the misuse of cryptographic libraries, protocols, and algorithms spanning the following supported languages: ABAP (Secure Store & Forward, pseudo random number, and cryptographic hash APIs⁵), C/C++ (*openssl* and *Microsoft Crypto API*), Java (*security API*), Objective-C (*CommonCrypto*), Python (*hashlib*, *random*, *pycrypto*, *hmac*, and the *Django crypto module*), and Ruby (*openssl*).

Insecure Randomness

- Pseudo-random number generator (PRNG) algorithms depend on random values, provided during initialization, to ensure their security. The following three new categories identify vulnerabilities which lead to situations of insecure randomness due to coding errors.
 - Insecure Randomness: Hardcoded Seed
 - Insecure Randomness: User-Controlled Seed
 - Insecure Randomness: Weak Entropy Source

Key Management

- Mismanagement of how encryption keys are created, used, and stored can lead to sensitive data being compromised. To help identify misuse of APIs related to key management, six new categories have been added.
 - Key Management: Empty HMAC Key
 - Key Management: Empty PBE Password
 - Key Management: Hardcoded HMAC Key
 - Key Management: Hardcoded PBE Password
 - Key Management: Null PBE Password

⁵ Preview Rulepack released with SCA 6.20 is no longer supported. Customers are encouraged to use SCA 6.30 to take full advantage of the new enhancements..

- Key Management: Unencrypted Private Key

Password Management

- The new Password Management: Lack of Key Derivation Function category identifies insecure situations in which a cryptographic hash function has been used by itself to generate a digest for a password being stored.

Weak Cryptographic Hash

- In addition to choosing a secure cryptographic hash, the correct use of the API (e.g. passing sufficient initialization values as parameters and invoking all necessary function calls) is integral to obtaining secure hashes. Ten new categories have been added to support detection of incorrect use of cryptographic hash APIs through poor initialization and invocation.
 - Weak Cryptographic Hash: Empty PBE Salt
 - Weak Cryptographic Hash: Empty Salt
 - Weak Cryptographic Hash: Hardcoded PBE Salt
 - Weak Cryptographic Hash: Insecure PBE Iteration Count
 - Weak Cryptographic Hash: Missing Required Step
 - Weak Cryptographic Hash: Null PBE Salt
 - Weak Cryptographic Hash: Null Salt
 - Weak Cryptographic Hash: Predictable Salt
 - Weak Cryptographic Hash: User-Controlled Algorithm
 - Weak Cryptographic Hash: User-Controlled PBE Salt

Weak Cryptographic Signature

- Strong cryptographic signature algorithms can be rendered less secure when parameters being used to initialize them, or required initialization steps, are not specified correctly. Three new categories identify cases which may lead to weaknesses.
 - Weak Cryptographic Signature: Insufficient Key Size
 - Weak Cryptographic Signature: Missing Required Step
 - Weak Cryptographic Signature: User-Controlled Key Size

Weak Encryption

- Incorrect use of encryption APIs, under specific circumstances, can lead to situations where secured data can be subject to a successful attack. Four new categories detect when specific parameters, specified during encryption algorithm initialization, are considered insecure.
 - Weak Encryption: Insecure Mode of Operation
 - Weak Encryption: Missing Required Step
 - Weak Encryption: Stream Cipher
 - Weak Encryption: User-Controlled Key Size

HP Fortify Runtime Application Protection (RTAP)

HP Fortify Runtime Application Protection provides application vulnerability monitoring and protection, and can operate in conjunction with HP ArcSight Logger/Enterprise Security Manager, in conjunction with HP Fortify Software Security Center, or as a standalone product. New for this release:

**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

Rename Privacy Violation

- To improve clarity and remove confusion, Privacy Violation: Credit Card Number and Privacy Violation: Social Security Number are now merged into Privacy Violation: Internal.

Improved signatures

- Various signature improvements in Cross-Site Scripting, SQL Injection and XML External Entity Injection will lower false positives as well as improve overall accuracy.

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:

Improved Database Trace

- Database trace now includes query time (in milliseconds) and number of records read/affected.

HP Fortify Premium Content

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

Crypto Manifesto

- The updated Crypto Manifesto whitepaper summarizes the HP SSR guidelines for the usage of cryptographic libraries, protocols, and algorithms, reflecting recent advances in the field.

Ruby Stub Libraries

- New stub libraries supporting pg and SQLite3 RubyGems are available to support function resolution of C-extension library APIs used in Ruby projects.

Fortify Annotations for Java

- Support for Fortify Annotations for Java, which provides an alternative to writing rules, has been updated to provide two versions of the annotation library with different retention policies. This enhancement allows users to choose whether or not Fortify Annotations appear only in source code or persist into bytecode.

Learn more at
hp.com/go/hpsr

