Micro Focus

Contenido de seguridad del software Fortify

Actualización 2 de 2019

28 de junio de 2019

Acerca del Equipo de investigación de seguridad para software Micro Focus Fortify

El Equipo de investigación de seguridad para software Fortify transforma la investigación más avanzada en inteligencia de seguridad que impulsa la cartera de productos de Fortify, incluidos Fortify Static Code Analyzer (SCA), Fortify WebInspect y Fortify Application Defender. Actualmente, el contenido de seguridad del software Micro Focus Fortify admite 1.005 categorías de vulnerabilidad en 25 lenguajes de programación y abarca más de un millón de API distintas.

Puede obtener más información en:

https://software.microfocus.com/en-us/software/security-research

El Equipo de investigación de seguridad para software Fortify (SSR) se complace en anunciar la disponibilidad inmediata de actualizaciones para Fortify Secure Coding Rulepacks (en inglés, versión 2019.2.0), Fortify WebInspect SecureBase (disponible mediante SmartUpdate), Fortify Application Defender y Fortify Premium Content.

Micro Focus Fortify Secure Coding Rulepacks [SCA]

Con esta versión, Fortify Secure Coding Rulepacks detecta 799 categorías únicas de vulnerabilidades en 25 lenguajes de programación y abarca más de un millón de API distintas. En resumen, esta versión incluye lo siguiente:

Actualizaciones de .NET

La compatibilidad con las adiciones de API introducida en las actualizaciones para las versiones 4.7.1 y 4.7.2. de .NET Framework incluye compatibilidad con reglas para .NET Standard 2.0 y .NET Core 2.0, que cubren las mismas categorías que .NET Framework. Las reglas para las versiones actualizadas de .NET Framework incluyen compatibilidad mejorada para la siguientes categorías:

- Header Manipulation: Cookies
- Insecure SSL: Server Identity Verification Disabled
- Insecure Transport: Weak SSL Protocol
- Weak Cryptographic Hash
- Weak Cryptographic Signature: Insufficient Key Size
- Weak Encryption

Realm Database

Realm Database, una base de datos ligera de código abierto diseñada específicamente para las aplicaciones móviles, ahora es compatible con iOS (Swift y Objective-C) y Android (Java). Entre las categorías admitidas se incluyen las siguientes:

- Access Control: Database
- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key
- Path Manipulation

Además, se admiten dos nuevas categorías:

- Insecure Storage: Missing Database Encryption
- NoSQL Injection: Realm

urllib3 para Python

Se incluye compatibilidad con la biblioteca urllib3 para Python, un cliente HTTP de gran capacidad y uso frecuente. Se cubren las siguientes categorías:

- Header Manipulation
- Insecure SSL: Server Identity Verification Disabled
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Server-Side Request Forgery

Actualizaciones para Java SE 10 y 11

Se ha aumentado la cobertura para Java SE a las versiones 10 y 11, con compatibilidad para la nueva API de cliente HTTP.

Cross-Site Scripting: SOP Bypass

Compatibilidad en JavaScript y TypeScript para la nueva categoría "Cross-Site Scripting: SOP Bypass". Esta nueva categoría cubre la situación específica en la cual una debilidad permite que un usuario malintencionado omita la directiva del mismo origen (SOP) para habilitar un ataque de scripts de sitios.

PCI SSF 1.0

Para ofrecer soporte en materia de cumplimiento a nuestros clientes de servicios financieros y de comercio electrónico, esta versión admite la correlación entre nuestras categorías de taxonomía de Micro Focus Fortify y los objetivos de control especificados en los nuevos requisitos y procedimientos de evaluación de seguridad de software, definidos en el estándar de software seguro (SSS) para la industria de tarjetas de pago (PCI) como parte del nuevo marco de seguridad de software SSF versión 1.0. Con el nuevo estándar se pretende reemplazar en última instancia el estándar de seguridad de datos (DSS) para PCI y completar la implementación de los nuevos métodos de DSS para aplicaciones de pago (PA) para mediados de 2020 y fijar la caducidad de los cambios vigentes con el estándar PA-DSS en 2022.

Otras erratas

En esta versión, hemos seguido ampliando recursos para garantizar la reducción del número de problemas de falsos positivos y mejorar la capacidad de auditoría de problemas por parte de los clientes. Los clientes también verán cambios en los problemas comunicados en relación con lo siguiente:

Log Forging

Reducción de los falsos positivos, en todos los lenguajes, gracias a un reconocimiento más preciso de las API que eliminan nuevas líneas para evitar los problemas de falsificación de registros Log Forging y Log Forging (debug).

Unreleased Resource: Database

En Java, los algoritmos no identificaban correctamente el cierre automático de un ResultSet si se cerraba primero la declaración que lo creó. Ahora se han eliminado los falsos positivos relacionados.

Unsafe JNI y Unsafe JSNI

Los clientes que actualizaron a SCA v19.1.x pueden haber observado el aumento de nuevos problemas "Unsafe JNI" y "Unsafe JSNI" en las aplicaciones de Java. Esto se debía a una mejora aplicada al motor, cuya consecuencia fue la identificación de muchas API sobre las cuales los clientes no tenían control de corrección. Este problema se ha solucionado de manera que SCA solo identifica las API cuando el usuario tiene control sobre el origen. Al reducirse estos problemas, los clientes también pueden observar una disminución de los problemas de

tipo "Access Control: SecurityManager Bypass".

Dynamic Code Evaluation and Other Sinks on Lambdas

En aplicaciones de JavaScript, se podían obtener resultados confusos al producirse un problema con una llamada lambda. Un ejemplo común es el de setTimeout(). Ahora se han eliminado estos problemas externos y, aunque se pueden seguir produciendo en algunos casos, trabajamos de forma activa para reducir su frecuencia. Esta reducción solo se puede observar al utilizar SCA 18.20 o una versión posterior.

Cross-Site Scripting: Content Sniffing

Anteriormente, SCA informaba sobre los problemas de Cross-Site Scripting en situaciones en las que el Content-Type de la respuesta impedía que un explorador procesara el contenido HTML/JS (por ejemplo, aplicación/json). Esto se podía producir cuando los usuarios de la aplicación web usaban exploradores anteriores donde se podía habilitar un ataque de rastreo de contenido. Con las modificaciones de esta versión, este tipo de problemas se identifican como “Cross-Site Scripting: Content Sniffing”. De este modo, los auditores y los desarrolladores pueden reconocerlos rápidamente y diferenciarlos de casos más graves de Cross-Site Scripting. Tanto el marco Spring como JAX-RS en los Rulepacks de Java admiten esta nueva categoría.

Reducción del orden de prioridad de Fortify según la corrupción

Anteriormente, SCA asignaba la misma gravedad a los problemas SQL Injection originados en un parámetro de solicitud HTTP que a los originados en una variable de entorno de sistema. Somos conscientes de que la probabilidad de que un usuario malintencionado controle las variables de sistema es muy baja o, al menos, más baja que la de controlar un parámetro de solicitud. Aunque ya habíamos reducido el valor de orden de prioridad de Fortify para los problemas de este tipo en determinadas situaciones, a partir de esta versión, SCA aplicará de manera más coherente el origen de corrupción como un nuevo factor a la hora de calcular el valor de orden de prioridad de Fortify de los problemas.

Micro Focus Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase combina las comprobaciones de miles de vulnerabilidades con las directivas que guían a los usuarios en las siguientes actualizaciones disponibles inmediatamente mediante SmartUpdate:

Compatibilidad de vulnerabilidades

Actualización de WebSocket[1]

Esta versión incluye mejoras para detectar vulnerabilidades de fugas de información y deserialización no segura (para .NET) en el tráfico de WebSocket. Concretamente, se han mejorado las siguientes categorías para admitir WebSocket:

- Dynamic Code Evaluation: Unsafe Deserialization
- Poor Error Handling: Unhandled Exception
- Privacy Violation
- Privacy Violation: Credit Card Number
- Privacy Violation: National ID Disclosure
- Privacy Violation: Social Security Number
- System Information Leak: Internal IP

Actualización de la configuración de encabezados de respuesta seguros

El servidor puede utilizar un conjunto de encabezados de respuesta HTTP para ofrecer una configuración de explorador que aumente la seguridad de la aplicación. Estos encabezados se consideran un mecanismo de defensa en profundidad que, al configurarse, puede evitar las vulnerabilidades según corresponda. Esta versión incluye compatibilidad mejorada con los siguientes encabezados y las categorías pertinentes:

- Cache-Control
  - Cache Management: Insecure Policy
- Content-Security-Policy
  - HTML5: Missing Content Security Policy
  - HTML5: Deprecated Content Security Policy
  - HTML5: Misconfigured Content Security Policy
- X-Content-Type-Options
  - Web Server Misconfiguration: Insecure Content-Type
- X-XSS-Protection
  - HTML5: Cross-Site Scripting Protection

Web Server Misconfiguration: Deprecated SSL/TLS Certificate

Todos los certificados SSL/TLS emitidos antes del 1 de diciembre de 2017 por la entidad certificadora Symantec (incluidas las marcas propiedad de Symantec, como Thawte, VeriSign, Equifax, GeoTrust y RapidSSL) dejan de ser de confianza y ya no se aceptan en los exploradores más importantes, como Chrome, Internet Explorer, Firefox y Safari. Esta versión incluye una comprobación para identificar el uso de certificados obsoletos de Symantec.

Insecure Deployment: Unpatched Application

Una vulnerabilidad crítica de ejecución de código de control remoto en el sistema de gestión de contenido (CMS) Drupal identificada en CVE-2019-6340 permite a los atacantes remotos ejecutar código arbitrario en el servidor. Esta versión incluye una comprobación que detecta esta vulnerabilidad en aplicaciones que implementan el CMS Drupal.

Informe de cumplimiento

[1] La actualización de WebSocket requiere WebInspect 19.1.0 o una versión posterior.

PCI SSF 1.0

Para ofrecer soporte en materia de cumplimiento a nuestros clientes, esta versión incluye una nueva plantilla de cumplimiento que establece una correlación entre la taxonomía de Micro Focus Fortify y los objetivos de control especificados en los nuevos requisitos y procedimientos de evaluación de seguridad de software, definidos en el estándar de software seguro (SSS) para la industria de tarjetas de pago (PCI) como parte del nuevo marco de seguridad de software SSF versión 1.0. Con el nuevo estándar se pretende reemplazar en última instancia el estándar de seguridad de datos (DSS) para PCI y completar la implementación de los nuevos métodos de DSS para aplicaciones de pago (PA) para mediados de 2020 y fijar la caducidad de los cambios vigentes con el estándar PA-DSS en 2022.

Actualizaciones de directivas

PCI SSF 1.0

Se ha incorporado una directiva personalizada a la lista existente de directivas admitidas en WebInspect SecureBase para incluir las comprobaciones pertinentes a PCI SSF 1.0.

Otras erratas

Cache Management: Insecure Policy

Se han introducido mejoras en la comprobación ID 11306 para excluir la identificación de respuestas HTML de content-types específicos que se solían auditar frecuentemente como resultados de falsos positivos en la verificación manual.

Expression Language Injection: Spring

Se ha mejorado la precisión del algoritmo de detección de vulnerabilidades en la comprobación ID 11579 de SecureBase.

Micro Focus Fortify Premium Content

El equipo de investigación crea, amplía y mantiene diversos recursos independientes de nuestros principales productos de inteligencia de seguridad.

PCI SSF 1.0

Para acompañar las nuevas correlaciones, esta versión también contiene un nuevo paquete de informes para Fortify SSC compatible con PCI SSF 1.0 que se puede descargar de Fortify Customer Portal, en la sección Premium Content.

Taxonomía de Micro Focus Fortify: errores de seguridad de software

El sitio Taxonomía de Fortify, que contiene descripciones de la compatibilidad con las nuevas categorías añadidas, está disponible en https://vulncat.fortify.com. Los clientes que busquen el sitio antiguo con la última actualización compatible, pueden encontrarlo en Micro Focus Fortify Support Portal.

Comuníquese con el soporte técnico de Fortify
Micro Focus Fortify
https://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

Comuníquese con SSR
Alexander M. Hoole
Director del Equipo de investigación de seguridad para software
Micro Focus Fortify
hoole@microfocus.com
+1 (650) 258-5916

28 de junio de 2019