Micro Focus

Contenido de seguridad del software Fortify

Actualización 4 de 2018

14 de diciembre de 2018

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 992 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/es-es/software/security-research

El Equipo de investigación de seguridad para software (SSR) de Fortify tiene el placer de anunciar que ya están disponibles las actualizaciones de Fortify Secure Coding Rulepacks (en inglés, versión 2018.4.0), 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 789 categorías únicas de vulnerabilidades en 25 lenguajes de programación y abarca más de un millón de API distintas. En resumen, la versión incluye lo siguiente:

Mejoras para iOS y SQLite

Mayor compatibilidad para las API de SQLite en Swift, Objective-C, C y C++. Abarca 16 categorías de vulnerabilidad existentes, como SQL Injection, Access Control: Database, y problemas relacionados con la administración de contraseñas y claves. Los puntos débiles en la codificación correspondientes a la interacción con cualquier tipo de base de datos pueden provocar fugas de información confidencial, modificaciones no autorizadas o incluso pérdidas de datos. Por tanto, se han realizado mejoras adicionales para iOS relacionadas con la privacidad que cubren, entre otras categorías, Privacy Violation: Heap Inspection para Swift.

Akka HTTP

Compatibilidad con los módulos de Akka HTTP para Scala, un kit de herramientas compatible con Reactive Streams basado en Akka Streams que implementa una pila HTTP completa tanto del lado servidor como del lado cliente. La cobertura de categorías de vulnerabilidad abarca 22 tipos de debilidades existentes.

Mejoras para JAX-RS

Compatibilidad revisada para la versión más reciente de JAX-RS y su implementación de referencia, Jersey. Además de la compatibilidad con nuevas funciones añadidas a la versión 2.1, este rulepack también incluye compatibilidad para API del lado cliente. Algunas de las categorías de vulnerabilidad afectadas son Privacy Violation, Server-Side Request Forgery y System Information Leak. Además, se ha añadido una nueva categoría de debilidad para una subcategoría especializada de Cross-Site Scripting, que se produce cuando se envían respuestas usando tipos de contenido seguro contra XSS. En este caso, registraremos un problema "Cross-Site Scripting: Content Sniffing", dado que determinados exploradores pueden realizar "rastreo de contenido" y ejecutar scripts en la respuesta.

Python six

Compatibilidad con la biblioteca "Six" de Python. Six es una biblioteca de compatibilidad de Python destinada a admitir códigos base compatibles con Python 2 y 3 sin modificación. Entre las categorías de vulnerabilidades compatibles se incluyen:

- Command Injection
- Dynamic Code Evaluation: Unsafe Pickle Deserialization
- Privacy Violation
- Server-Side Request Forgery
- System Information Leak: External
- Unsafe Reflection

DISA STIG 4.8

Para ofrecer soporte a nuestros clientes federales en lo que respecta al cumplimiento, se agregó una correlación de la taxonomía de Micro Focus Fortify con la versión 4.8 de la STIG de seguridad y desarrollo de aplicaciones de la Agencia de sistemas de información de defensa (DISA) estadounidense.

PCI DSS 3.2.1

Para ofrecer asistencia a nuestros clientes de servicios financieros y de comercio electrónico en lo que respecta al cumplimiento, esta versión admite la correlación entre nuestras categorías de taxonomía de Security Fortify y los requisitos especificados en la versión más reciente del estándar de seguridad de datos para la industria de tarjeta de pago (versión 3.2.1).

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

LDAP Injection

LDAP Injection es un ataque que se utiliza para aprovechar las aplicaciones web que crean instrucciones LDAP basadas en entradas de usuario. Si una aplicación no logra corregir correctamente la entrada del usuario, es posible modificar las instrucciones LDAP mediante técnicas similares a las utilizadas en SQL Injection. Los ataques de LDAP Injection podrían provocar el acceso no autorizado a datos confidenciales. Esta versión incluye una comprobación para identificar vulnerabilidades de LDAP Injection en aplicaciones web.

Open Redirect

Una vulnerabilidad de Open Redirect puede permitir que un usuario malintencionado aproveche fácilmente la confianza del usuario en sitios conocidos. Según información del proveedor, SA-CORE-2018-006 Drupal 7 y 8 son vulnerables a esta debilidad.

Drupal Destination Parameter Anonymous Open Redirect

En Drupal 8, la corrección inadecuada del valor del parámetro "destination" se puede utilizar para desencadenar un redireccionamiento abierto a una URL malintencionada controlada por el responsable del ataque. Esta versión incluye una comprobación que permite detectar esta vulnerabilidad.

Drupal Path Alias Open Redirect

En Drupal 7 y Drupal 8, una vulnerabilidad en el módulo de ruta permite que un atacante cree, edite y administre alias de ruta que pueden desencadenar un redireccionamiento abierto a una URL malintencionada que él controle.

Access Control: Authorization Bypass

JSON Web Token (JWT) es un estándar para la creación de URL seguras para la transferencia de datos entre dos partes. La información del token se firma digitalmente

usando algoritmos HMAC o RSA. Sin embargo, el estándar también permite el uso del valor "none" como algoritmo de hash en JWT. Los servidores que acepten JWT codificado con "none" consideran que todo JWT es válido sin realizar ninguna comprobación de la integridad de los datos. Los usuarios malintencionados pueden usar este comportamiento para enviar datos arbitrarios al servidor. Esto puede derivar en un acceso no autorizado y comprometer tanto los datos del sistema como los del usuario. Esta versión incluye una comprobación que permite detectar la vulnerabilidad por omisión de la autorización mediante el algoritmo "none" en JWT.

Privacy Violation

JSON Web Tokens (JWT) se utilizan para transferir datos entre dos partes. Si el cifrado no es adecuado, los datos confidenciales podrían quedar expuestos a usuarios no autorizados. Esta versión incluye actualizaciones de las comprobaciones existentes que detectan infracciones de la privacidad relacionadas con la revelación de números de tarjetas de crédito y de la seguridad social, y detectan almacenamiento de información confidencial en el almacenamiento HTML5 del lado cliente.

Dynamic Code Evaluation: Code Injection

Se ha detectado que Spring Framework de Pivotal es vulnerable a la ejecución remota de código, tal y como se señala en CVE-2018-1270. La vulnerabilidad permite que un atacante envíe mensajes malintencionados a STOMP expuesto mediante extremos de WebSocket que pueden provocar la ejecución remota de código. Esta versión incluye una comprobación que permite detectar esta vulnerabilidad en Spring Framework. Es posible acceder a esta comprobación mediante la directiva de WebSocket.

WebSocket Discovered

Esta versión incluye una comprobación informativa para indicar la presencia de WebSockets en la aplicación explorada. Adicionalmente, la comprobación desencadena un recordatorio para que nuestros clientes valoren la posibilidad de explorar la aplicación con la nueva directiva de WebSocket que contiene todas las comprobaciones relevantes con respecto a las vulnerabilidades de WebSocket.

Informe de cumplimiento

DISA STIG 4.8

Para proporcionar soporte a nuestros clientes federales en lo que respecta al cumplimiento, esta versión contiene una correlación de las comprobaciones de WebInspect con la versión más reciente (4.8) de la STIG para la seguridad y el desarrollo de aplicaciones de la Agencia de sistemas de información de defensa estadounidense.

PCI DSS 3.2.1

Esta versión incluye compatibilidad con la versión más reciente de la plantilla de cumplimiento del estándar de seguridad de datos (DSS) para la industria de tarjeta de pago (versión 3.2.1).

Actualizaciones de directivas

DISA STIG 4.8

Se ha incorporado una directiva personalizada a la lista existente de directivas admitidas en WebInspect SecureBase para incluir las comprobaciones pertinentes a DISA STIG 4.8.

WebSocket

La nueva directiva de WebSocket realiza una evaluación de la seguridad de la aplicación para detectar vulnerabilidades relacionadas con WebSocket.

Micro Focus Fortify Premium Content

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

DISA STIG 4.8[1]

Para acompañar las nuevas correlaciones, esta versión también contiene un nuevo paquete de informes para Fortify SSC compatible con DISA STIG 4.8 que se puede descargar de Fortify Customer Portal, en la sección Premium Content.

PCI DSS 3.2.1[1]

Para acompañar las nuevas correlaciones, esta versión también contiene un nuevo paquete de informes para Fortify SSC compatible con PCI DSS 3.2.1 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.

[1] La compatibilidad con informes DISA STIG 4.8 y PCI DSS 3.2.1 requiere la versión 18.20 o superior de Fortify SSC.

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

14 de diciembre de 2018