Micro Focus

Contenido de seguridad del software Fortify

Actualización 4 de 2019

13 de diciembre 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 1.018 categorías de vulnerabilidad en 26 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 (SSR) se complace en anunciar la disponibilidad inmediata de actualizaciones para Fortify Secure Coding Rulepacks (en inglés, versión 2019.4.0), Fortify WebInspect SecureBase (disponible mediante SmartUpdate) y Fortify Premium Content.

Micro Focus Fortify Secure Coding Rulepacks [SCA]

Con esta versión, Fortify Secure Coding Rulepacks detecta 807 categorías únicas de vulnerabilidades en 26 lenguajes de programación y abarca más de un millón de API distintas. En resumen, esta versión incluye lo siguiente:

Compatibilidad inicial con Go[1]

Compatibilidad inicial para Go. Go es un lenguaje de código abierto con un sistema de tipos estático diseñado por Google™ que facilita la compilación de software para que resulte sencillo, confiable y eficiente. En términos de sintaxis, Go es similar a C, pero presenta mecanismos de seguridad de memoria, recopilación de elementos no utilizados y tipado estructural. Esta actualización abarca 10 espacios de nombres básicos de biblioteca estándar para las siguientes 34 categorías:

- Access Control: Database
- Command Injection
- Connection String Parameter Pollution
- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set
- Cookie Security: Overly Broad Domain
- Cookie Security: Overly Broad Path
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- File Permission Manipulation
- Header Manipulation
- Header Manipulation: Cookies
- HTML5: MIME Sniffing
- Insecure Transport
- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key
- Open Redirect
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Path Manipulation
- Path Manipulation: Zip Entry Overwrite
- Privacy Violation
- Server-Side Request Forgery
- Setting Manipulation
- SQL Injection

[1] Requiere SCA v19.2.0 o una versión posterior.

- System Information Leak: External
- System Information Leak: Internal
- Weak Encryption
- Weak Encryption: Insufficient Key Size

Spring Security

Spring Security es un marco de autenticación y control de acceso que también proporciona niveles adicionales de seguridad, tales como los encabezados de seguridad, a fin de aumentar la protección contra ataques del tipo fijación de sesiones, secuestro de clic y falsificaciones de petición de sitios, entre otros. Es el estándar de facto para la protección de aplicaciones basadas en Spring. Esta actualización incluye compatibilidad, hasta la versión 5.2.1, con las siguientes 21 categorías:

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: Overly Broad Domain
- Cross-Site Request Forgery
- Header Manipulation
- HTML5: Cross-Site Scripting Protection
- HTML5: MIME Sniffing
- HTML5: Missing Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- HTML5: Overly Permissive CORS Policy
- HTML5: Overly Permissive Referrer-Policy
- Insecure Transport: HSTS Does Not Include Subdomains
- Insecure Transport: HSTS not Set
- Insecure Transport: Insufficient HSTS Expiration Time
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Privacy Violation
- Session Fixation
- System Information Leak

Asimismo, se presentan los siguientes siete nuevos tipos de debilidad:

- HTML5: protección de marco ausente
- HTML5: política de seguridad de contenido no aplicada
- Configuración incorrecta de Spring Security: permiso predeterminado
- Configuración incorrecta de Spring Security: encabezados de seguridad deshabilitados
- Configuración incorrecta de Spring Security: tipo de emparejador de solicitud incorrecto
- Configuración incorrecta de Spring Security: falta de comprobación de reserva
- Configuración incorrecta de Spring Security: directiva de firewall excesivamente permisiva

Spring Boot

Spring Boot crea aplicaciones de Spring independientes y configura automáticamente bibliotecas de Spring y de terceros siempre que sea posible. También incluye funciones listas para la producción, como métricas, comprobaciones de estado y configuración externalizada. Además de las categorías admitidas previamente, esta actualización incluye compatibilidad, hasta la versión 2.2.1, con las siguientes nueve categorías:

- Cookie Security: HTTPOnly not Set on Session Cookie
- Cookie Security: Overly Broad Session Cookie Domain

- Cookie Security: Overly Broad Session Cookie Path
- Cookie Security: Persistent Session Cookie
- Cookie Security: Session Cookie not Sent Over SSL
- Password Management: Empty Password in Configuration File
- Insecure Transport
- Insecure Transport: Server Identity Verification Disabled
- System Information Leak: External

Asimismo, mientras que Rulepacks anteriormente solo admitía archivos de configuración de propiedades y el sistema de compilación Maven, esta versión también incluye compatibilidad con archivos de configuración YAML y con Gradle.

Java 12[2]

Compatibilidad con nuevas API en Java 12. Estas reglas requieren la versión de SCA 19.1 o posterior cuando se use la nueva sintaxis Java 12 como nueva instrucción Switch.

Biblioteca XML JSTL

La biblioteca de etiquetas estándar (JSTL) JavaServer Pages (JSP) permite manejar y crear documentos XML centrados en JSP. Ahora se ofrece compatibilidad adicional con las siguientes categorías de JSTL v1.1:

- XSLT Injection
- XML External Entity Injection
- Privacy Violation
- System Information Leak: External

Mejoras de OpenXML SDK .NET

La compatibilidad actualizada de OpenXML SDK v2.9.0 incluye tres categorías adicionales:

- Access Control: Database
- Connection String Parameter Pollution
- SQL Injection

Compatibilidad con React-Router

React-Router es una recopilación de componentes de navegación que se integran de forma declarativa en la aplicación. Ya sea que busque incluir URL como marcadores para la aplicación web o una forma de navegación ensamblable en React, React-Router funciona siempre que React esté procesando. Las categorías admitidas para React-Router 5.1.2 son las siguientes:

- Open Redirect
- Privacy Violation
- System Information Leak: External

Top 25 de CWE 2019

La enumeración de debilidades comunes (CWE) de las principales 25 vulnerabilidades básicamente cambió la manera en que se determinan las debilidades, en comparación con la antigua denominación de esta lista, SANS Top 25. Publicadas en septiembre, las principales 25

[2] Requiere SCA v19.2.0 o una versión posterior.

debilidades se determinan mediante una fórmula heurística que normaliza la frecuencia y la gravedad de las vulnerabilidades comunicadas a la base de datos nacional de vulnerabilidades (NVD) en los últimos dos años. Para ofrecer soporte a nuestros clientes que deseen dar prioridad en sus auditorías a las vulnerabilidades críticas más registradas en la NVD, se agregó una correlación de la taxonomía de Micro Focus Fortify con la versión 2019 de las principales 25 debilidades CWE.

DISA STIG 4.10

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 4.10 de la STIG de seguridad y desarrollo de aplicaciones de la Agencia de sistemas de información de defensa (DISA) estadounidense.

Otras erratas

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

- Coherencia de deserialización no segura: anteriormente, algunas reglas solo notificaban si la información provenía de un explorador. Esto se corrigió y ahora notifican en otros posibles escenarios.
- Referencias de descripción verificadas: algunos de los materiales a los que se hace referencia estaban desactualizados o dirigían a vínculos no válidos. Estas instancias se corrigieron y ahora se aplican las referencias correctas.

Micro Focus Fortify SecureBase [Fortify WebInspect]

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

Compatibilidad de vulnerabilidades

SSO Bad Practices: Authentication Token Replay

Los tokens de autenticación intercambiados durante un proceso de inicio único de sesión son susceptibles a los ataques de reproducción y pueden permitir que un atacante se haga pasar por un usuario válido para obtener acceso no autorizado al servicio. Esta versión incluye una comprobación que ejecuta el ataque de reproducción para el marco de identidad de Windows y proveedores de servicios que usan el protocolo SAML.

Cache Management: Headers

El encabezado de respuesta HTTP Vary contiene una lista de encabezados HTTP que se usan a fin de decidir la respuesta correcta almacenada en la memoria caché que se debe emitir a una solicitud entrante. La ausencia de un elemento "Origin" en el encabezado Vary puede dejar la aplicación abierta a ataques de envenenamiento de la memoria caché tanto del lado del cliente como del servidor, sobre todo cuando se realiza una solicitud de origen cruzado. Esta versión incluye una comprobación para detectar cuando falta un encabezado "Origin" en el valor del encabezado Vary.

HTML5: CORS Functionality Abuse

Si se permiten solicitudes CORS con un origen nulo, "Origin: null", se puede comprometer la seguridad del sistema y exponer la aplicación al robo de datos. Esta versión incluye una comprobación para detectar la presencia de valores "null" en el encabezado Access-Control-Allow-Origin de CORS dentro de una respuesta del servidor.

Insecure Deployment: HTTP Request Smuggling[3]

Las vulnerabilidades HTTP Request Smuggling surgen por una discrepancia en el análisis de encabezados HTTP no compatibles por parte de servidores de front-end y back-end. Al proporcionar una solicitud cuya longitud se interpreta de forma diferente por los distintos servidores, un atacante puede contaminar el socket TCP/TLS de back-end y anteponer datos arbitrarios en la siguiente solicitud o traficar solicitudes adicionales en el servidor de back-end sin que el servidor de front-end lo advierta. Esta versión incluye una comprobación que permite detectar esta vulnerabilidad.

Header Manipulation[4]

La comprobación existente de Header Manipulation se mejoró en esta versión y ahora incluye ataques de retorno de carro (CR) y salto de línea (LF), además del ataque CRLF ya conocido.

Informe de cumplimiento

DISA STIG 4.10

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 (4.10) de la STIG para la seguridad y el desarrollo de aplicaciones de la Agencia de sistemas de información de defensa estadounidense.

Actualizaciones de directivas

[3] La comprobación Insecure Deployment: HTTP Request Smuggling requiere WebInspect 19.2.0 o una versión posterior.
[4] La mejora de Header Manipulation requiere WebInspect 19.2.0 o una versión posterior.

DISA STIG 4.10

Se incorporó una directiva personalizada a la lista existente de directivas admitidas en WebInspect SecureBase para incluir las comprobaciones pertinentes a DISA STIG 4.10.

Micro Focus Fortify Premium Content

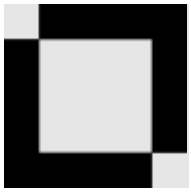
El equipo de investigación crea, amplía y mantiene diversos recursos independientes de nuestros principales productos de inteligencia de seguridad.

DISA STIG 4.10 y Top 25 de CWE 2019

Para acompañar las nuevas correlaciones, esta versión también contiene un nuevo paquete de informes para Fortify Software Security Center compatible con DISA STIG 4.10 y el Top 25 de CWE 2019, que se puede descargar desde Fortify Customer Support 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

13 de diciembre de 2019