Micro Focus

Contenido de seguridad del software Fortify

Actualización 1 de 2019

29 de marzo 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 999 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 2019.1.0), 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 796 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:

Angular 7[1]

La compatibilidad con Angular (todas las versiones hasta la 7.0.0, incluida) identifica los orígenes de las entradas desde un explorador y modela la validación de seguridad que realiza Angular de forma predeterminada. Las plantillas de Angular se modelan de forma que se admitan todos los receptores regulares de JavaScript para proyectos de Angular, incluida la capacidad de buscar categorías como Cross-Site Scripting: DOM, Privacy Violation y Dynamic Code Evaluation, entre muchas otras.

Compatibilidad con funciones de AWS Lambda

Nueva compatibilidad con las funciones de Amazon Web Services (AWS) Lambda para los lenguajes Java y Python. La funcionalidad permite que el flujo de datos desde Lambda desencade eventos en la lógica de la función Lambda, dando cobertura a los posibles problemas de XSS cuando Lambda se conecta a una puerta de enlace de API.

AWS Java SDK v2

Nueva compatibilidad con el AWS SDK para Java v2 para los servicios S3 y DynamoDB. Se incluyen nuevas categorías, como las siguientes:

- Access Control: ACL Manipulation
- Insecure Storage: S3 Full Anonymous Access
- Insecure Storage: S3 Read ACP Anonymous Access
- Insecure Storage: S3 Read Anonymous Access
- Insecure Storage: S3 Write Anonymous Access
- Insecure Storage: S3 Write ACP Anonymous Access
- NoSQL Injection: DynamoDB

Python Django[1]

Compatibilidad actualizada con el marco web de Python Django (todas las versiones hasta la 2.1.7, incluida). Entre los cambios, se incluye una compatibilidad mejorada con las vistas basadas en clases y los flujos de trabajo asociados, así como compatibilidad con las funciones y los métodos de Django introducidos a partir de Django 1.8.

[1] La compatibilidad con Angular 7, Django y Wicket requiere la versión 19.1.0 o posterior de Fortify SCA para un rendimiento óptimo.

Apache Wicket[1]

Compatibilidad mejorada con el marco web de Apache Wicket (incluidas las versiones 6, 7 y 8 del marco).

DISA STIG 4.9

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

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

Often Misused: File Upload

Se ha detectado una vulnerabilidad del widget jQuery File Upload de Blueimp ante la ejecución de código remoto, según se ha identificado en CVE-2018-9206. La vulnerabilidad permite que un usuario malintencionado cargue y ejecute archivos PHP arbitrarios. Esta versión incluye una comprobación para detectar esta vulnerabilidad.

SQL Injection

Esta versión ofrece mejoras en la comprobación de SQL Injection para incluir compatibilidad con aplicaciones que utilizan Microsoft Azure SQL Database.

Sensitive Information Leak: External

Esta versión incluye una comprobación para detectar si Magento CMS se ejecuta en modo de desarrollador. Este modo está pensado para usarse en un entorno de pruebas o de desarrollo. Si se habilita en un entorno de producción, puede desvelar datos importantes sobre el sistema y la aplicación a posibles usuarios malintencionados y crear un riesgo para la seguridad.

Cross-Frame Scripting

El encabezado de directiva *frame-ancestors* de la política de seguridad de contenidos ofrece protecciones de política frente a las vulnerabilidades Cross-Frame Scripting. Define como obsoleto el encabezado HTTP X-Frame-Options que se utiliza actualmente. Esta versión incluye mejoras en la comprobación de Cross-Frame Scripting para

garantizar la compatibilidad con el encabezado de directiva frame-ancestors de la política de seguridad de contenidos.

Content Management System (CMS) Fingerprinting

Esta versión incluye mejoras para detectar la presencia de uno de los siguientes sistemas CMS en el servidor de destino durante un análisis de WebInspect: WordPress, Drupal, Django, Joomla, Liferay, Magento, Sitecore, Sitefinity[2] y Umbraco. Se desencadena una comprobación de información para documentar el hallazgo.

Informe de cumplimiento

DISA STIG 4.9

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

Actualizaciones de directivas

DISA STIG 4.9

Se ha incorporado una directiva personalizada a la lista existente de directivas admitidas en WebInspect SecureBase para incluir las comprobaciones pertinentes a DISA STIG 4.9.

Micro Focus Fortify Application Defender

Fortify Application Defender es una solución de autoprotección de aplicaciones en tiempo de ejecución (RASP) que ayuda a las organizaciones a administrar y mitigar los riesgos de aplicaciones propias o de terceros. Proporciona una vista centralizada del uso y el abuso de aplicaciones, y protege contra la explotación de vulnerabilidades de software y otras infracciones en tiempo real. En esta versión, el Equipo de investigación de seguridad para software Micro Focus Fortify proporciona las siguientes mejoras de características:

OGNL Expression Injection: Struts 2

Compatibilidad ampliada para la detección de OGNL Expression Injection en Apache Struts2, a fin de cubrir la vulnerabilidad crítica de Struts identificada en CVE-2018-11776. Las aplicaciones que utilizan Apache Struts2 desde la versión 2.3.x hasta 2.3.34, o desde la versión 2.5.x hasta 2.5.16, permiten que los usuarios malintencionados ejecuten expresiones OGNL arbitrarias si estas contienen resultados de acciones que están configuradas sin ningún espacio de nombres o con un espacio de nombres de comodín y también tienen configurada la

[2] La detección de Sitefinity requiere WebInspect 19.1.0 o una versión posterior.

propiedad struts.mapper.alwaysSelectFullNamespace en verdadero en la configuración de Struts.

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 4.9[3]

Para acompañar las nuevas correlaciones, esta versión también contiene un nuevo paquete de informes para Fortify SSC compatible con DISA STIG 4.9 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.

[3] La compatibilidad con el informe DISA STIG 4.9 requiere Fortify SSC 18.20 o una versión posterior.

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

29 de marzo de 2019