Micro Focus

Contenido de seguridad del software Fortify

Actualización 4 de 2020

viernes, 18 de diciembre de 2020

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 1.039 categorías de vulnerabilidad en 27 lenguajes de programación y abarca más de un millón de API distintas.

Más información en: https://software.microfocus.com/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 2020.4.0), 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 817 categorías únicas de vulnerabilidades en 27 lenguajes de programación y abarca más de un millón de API distintas. En resumen, esta versión incluye lo siguiente:

Compatibilidad con Dapper (versión 2.0.78)

Compatibilidad con la herramienta de asignación objeto-relacional (ORM) Dapper. Dapper se usa para asignar el resultado de una consulta nativa a objetos fuertemente tipados en C# mediante la extensión de la interfaz .NET IDdbConnection. Esta nueva compatibilidad trata a Dapper como una fuente de datos controlados por el usuario, así como desencadenador de categorías como las que se enumeran a continuación:

- Access Control: base de datos
- SQL Injection

Actualizaciones de la biblioteca estándar de Kotlin (versión 1.3)

Se ha ampliado la compatibilidad con la biblioteca estándar de Kotlin para que admita los siguientes paquetes:

- kotlin.concurrent
- kotlin.jvm
- kotlin.reflect
- kotlin.system

XML Pull (versión 1)

Compatibilidad para la implementación en Android del paquete XML Pull. XML Pull es una API de streaming sencilla que se utiliza para analizar y serializar archivos XML en la que la aplicación controla el análisis (este puede interrumpirse y reanudarse). Entre las categorías compatibles se incluyen:

- XML Entity Expansion Injection
- XML Injection

AIOPG (versión 1.0.0)[1]

Compatibilidad con la biblioteca aiopg de Python. Aiopg proporciona una forma asíncrona de conectarse a bases de datos PostgreSQL. Entre las categorías compatibles se incluyen:

- Access Control: base de datos
- Password Management
- Password Management: Empty Password
- Password Management: contraseña codificada de forma rígida
- Password Management: Null Password
- Password Management: criptografía débil
- SQL Injection

[1] La detección completa de problemas relacionados con aiopg depende de una futura mejora de SCA asociada a «async with».

Promises de JavaScript

- La compatibilidad de Promises de JavaScript se ha mejorado para los análisis de flujo de datos.

Plantillas de administración de recursos de Azure

Compatibilidad inicial para las plantillas de administración de recursos de Azure (ARM). Las plantillas de ARM se utilizan para implementar infraestructuras como código para soluciones de Azure. Las plantillas de ARM son archivos JSON que usan una sintaxis declarativa para definir y configurar un proyecto de usuario. Entre las categorías compatibles se incluyen:

- Error de configuración de Azure Resource Manager: HTTPS no es necesario
- Error de configuración de Azure Resource Manager: Acceso público permitido

DISA STIG 5.1

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

SP 800-53 Rev. 5 del NIST

Para ofrecer soporte a nuestros clientes federales en lo que respecta al cumplimiento, se agregó una correlación de la taxonomía de Micro Focus Fortify a los controles de seguridad y privacidad de la versión más reciente de la publicación especial (SP) del Instituto Nacional de Estándares y Tecnología (NIST) 800-53 Revision 5. Se admiten 30 controles base, entre los que se incluyen:

- Access Control (AC)
- Auditoría y rendición de cuentas (AU)
- Evaluación, autorización y control (CA)
- Gestión de la configuración (CM)
- Identificación y autenticación (IA)
- Tratamiento y transparencia de datos PII (PT)
- Protección del sistema y las comunicaciones (SC)
- Integridad del sistema y la formación (SI)

Common Weakness Enumeration (CWE™) Top 25 de 2020

La Common Weakness Enumeration (CWE™) Top 25 (enumeración de las 25 principales debilidades comunes) se introdujo en 2019 y remplaza la SANS Top 25. La CWE Top 25 de 2020 se publicó en agosto y se determinó 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 a la CWE Top 25 de 2020.

Otras erratas

En esta versión, seguimos invirtiendo 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:

Desuso para versiones de SCA anteriores a 17.x

Como se anunció en la presentación del lanzamiento de 2020.3, esa fue la última versión de Rulepacks compatible con versiones de SCA anteriores a 17.x. En esta versión, las versiones de SCA anteriores a 17.x no cargarán las últimas instancias de Rulepacks. Los clientes que usen versiones SCA anteriores a 17.x deben usar versiones de Rulepacks anteriores o actualizar la versión de SCA.

En las versiones futuras, admitiremos las últimas cuatro versiones principales de SCA.

Obsolescencia de asignaciones

A lo largo de los años, el Equipo de investigación de seguridad para software continuó creando asignaciones a partir de categorías de Fortify para prácticas recomendadas y estándares externos. Por lo tanto, hoy en día la cantidad de versiones de diferentes estándares que son compatibles ha crecido notablemente, aunque muchas versiones anteriores no se usarán más.

Por ello, hemos marcado estos estándares como "obsoletos":

- Estándar de seguridad de datos para la industria de tarjeta de pago (PCI) 1.1
- Estándar de seguridad de datos para la industria de tarjeta de pago (PCI) 1.2
- Estándar de seguridad de datos para la industria de tarjeta de pago (PCI) 2.0
- Estándar de seguridad de datos para la industria de tarjeta de pago (PCI) 3.0
- Estándar de seguridad de datos para la industria de tarjeta de pago (PCI) 3.1
- Estándar de seguridad de datos para la industria de tarjeta de pago (PCI) 3.2
- Guía de implementación técnica de seguridad (STIG) 4.1
- Guía de implementación técnica de seguridad (STIG) 4.2
- Guía de implementación técnica de seguridad (STIG) 4.3
- Guía de implementación técnica de seguridad (STIG) 4.4
- Guía de implementación técnica de seguridad (STIG) 4.5
- Guía de implementación técnica de seguridad (STIG) 4.6
- Guía de implementación técnica de seguridad (STIG) 4.7

- Guía de implementación técnica de seguridad (STIG) 4.8

Este cambio significa que las aplicaciones SCA de Fortify a partir de la versión 20.2 no mostrarán estas asignaciones anteriores de forma predeterminada.
Si debe comprobar el cumplimiento de estas versiones antiguas, tendrá que modificar las asignaciones para cambiar el atributo *"obsoleto"* a "falso", o bien quitar el atributo directamente.

Mejoras en falsos positivos:
Seguimos escuchando a nuestros clientes y nos esforzamos por mejorar las tasas de falsos positivos. En esta versión, trabajamos en los siguientes aspectos para reducir el número de falsos positivos:

- Se han eliminado los falsos positivos de manipulación de verbos HTTP cuando existe protección en los archivos de configuración
- Se han eliminado los falsos positivos de asignación masiva cuando se utiliza el atributo JSONIGNORE en .NET
- Se han eliminado los falsos positivos de Insecure Storage: HTTP Response Cache Leak cuando los cachés se encuentran deshabilitados de forma explícita en los objetos URLSessionConfiguration
- Se han eliminado los falsos positivos de Privacy Violation de Swift: HTTP GET de URLRequest
- Poor Logging Practice: se ha eliminado el uso de System Output Stream duplicados de Python
- Se han eliminado los problemas de Unreleased Resource cuando se usan variantes adicionales de closeQuietly de Apache Commons

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

Weak Cryptographic Signature: Clave secreta predecible

La integridad de carga de JSON Web Token suele garantizarse mediante el uso de firmas HMAC. Sin embargo, si el algoritmo HMAC utiliza una clave secreta débil, los usuarios malintencionados podrían obtener la clave por fuerza bruta y volver a firmar el JWT con otra carga. Esta versión incluye una comprobación para detectar si una cadena de las claves secretas de uso frecuente se emplea para firmar los tokens JWT.

Password Management: Directiva de contraseñas débil

Resulta esencial disponer de directivas de contraseñas que garanticen la creación de contraseñas seguras por parte de los usuarios para la implementación de sitios web seguros. Las contraseñas deberían validarse a fin de garantizar que no son contraseñas de uso frecuente. Además, una cadena de contraseña debería cumplir las directrices establecidas en el NIST 800-53, el NIST

800118 y el OWASP. Esta versión incluye una nueva comprobación para detectar si la contraseña configurada en la macro de inicio de sesión coincide con una de las contraseñas de uso frecuente. También incluye una actualización de las comprobaciones de la directiva de contraseñas débiles para cumplir con las directrices actualizadas sobre la seguridad de las contraseñas que se establecen en los estándares previamente citados de las directrices NIST y OWASP.

Cache Management: Envenenamiento de la memoria caché web

La caché web almacena una copia de la página cuando el usuario visita una página web por primera vez. La siguiente vez que el usuario visita esa misma página, se le sirve de una copia almacenada en caché. Sin embargo, si esa caché web presenta errores de implementación o diseño, como la aceptación de solicitudes GET con cuerpo de solicitud (p. ej. solicitudes fat GET o entradas no codificadas), puede ser susceptible de un ataque de envenenamiento de la caché web. El envenenamiento de la caché web es una técnica avanzada que los atacantes utilizan para almacenar respuestas maliciosas para solicitudes legítimas de los usuarios. Esta versión incluye comprobaciones que identifican si un sitio web es vulnerable al envenenamiento de la caché web mediante encabezados no codificados y solicitudes fat GET.

Informes de cumplimiento

DISA STIG 5.1

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

SP 800-53 Rev. 5 del NIST

Para proporcionar soporte a nuestros clientes federales en lo que respecta al cumplimiento, esta versión contiene una correlación de las comprobaciones de WebInspect con los controles de la versión más reciente de la publicación especial (SP) del Instituto Nacional de Estándares y Tecnología (NIST) 800-53 Revision 5.

Common Weakness Enumeration (CWE™) Top 25 de 2020

La Common Weakness Enumeration (CWE™) Top 25 (enumeración de las 25 principales debilidades comunes) se introdujo en 2019 y remplaza la SANS Top 25. La CWE Top 25 de 2020 se publicó en agosto y se determinó 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. Esta actualización de Securebase incluye asignaciones para estas categorías de CWE. Se incluyen las verificaciones que realizan asignaciones de manera directa a la categoría identificada en CWE Top 25, o bien a un ID de CWE relacionado con uno de los incluidos en el Top 25 a través de una relación “ChildOf”.

Otras erratas

En esta versión, seguimos invirtiendo 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:

- La verificación HTTP Request Smuggling se ha rediseñado para reducir los falsos positivos, aumentar la eficiencia y mejorar la precisión de sus resultados. La verificación ID 11621 ya no usa un enfoque basado en el tiempo para la verificación de vulnerabilidades.

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 5.1, SP 800-53 Rev. 5 del NIST y CWE Top 25 de 2020

Para acompañar las nuevas correlaciones, esta versión también contiene un nuevo paquete de informes para Fortify Software Security Center compatible con DISA STIG 5.1, la SP 800-53 Rev. 5 del NIST y la CWE Top 25 de 2020, y se puede descargar desde Fortify Customer Support Portal, en la sección Premium Content.

Taxonomía de Micro Focus Fortify: errores en la seguridad del 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

18 de diciembre de 2020