Micro Focus

Contenido de seguridad del software Fortify

Actualización 1 de 2021

viernes, 26 de marzo de 2021

Acerca de Software Security Research Micro Focus Fortify

Software Security Research 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 1.038 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

Software Security Research (SSR) se complace en anunciar la disponibilidad inmediata de actualizaciones para Fortify Secure Coding Rulepacks (en inglés, versión 2021.1.0), 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 816 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 Micro Focus Visual COBOL (Versión 6)[1]

Esta versión añade compatibilidad con la versión 6 de Micro Focus Visual COBOL. En concreto, la versión incluye compatibilidad con Micro Focus COBOL Runtime System (RTS) con la compatibilidad ampliada para la categoría Path Manipulation, ya compatible con COBOL, y las siguientes categorías adicionales:

- Command Injection
- Memory Leak
- Memory Leak: Reallocation
- Unreleased Resource
- Unreleased Resource: Synchronization

Android 11

Como parte de nuestro constante esfuerzo por ofrecer compatibilidad con la última versión de Android (nivel de API 30), se abarcan los siguientes espacios de nombres:

- android.accounts
- android.app
- android.database
- android.database.sqlite

Los usuarios deberían poder ver un mejor modelado de las aplicaciones de Android que, por lo general, da lugar a mejores resultados, así como resultados de *SQL Injection* y *Access Control: Database* adicionales.

Actualizaciones de iOS

Como parte de nuestro constante esfuerzo por mejorar la compatibilidad con iOS, se añaden nuevas reglas Swift a las siguientes clases:

- Foundation.NSCache
- Foundation.URLFileProtection

Los usuarios deberían poder ver mejores resultados en relación con Data Protection y Privacy Violation, así como mejoras generales en otros tipos de debilidades y marcos (consulte "Otras erratas: corrección de errores en iOS").

Actualizaciones de la compatibilidad con Angular (versión 11.2.3)

Esta versión aumenta nuestra compatibilidad con Angular hasta la versión 11.2.3. En concreto, se identificaron nuevas fuentes de información controlada por el usuario desde el navegador, lo que puede hacer que muchas categorías se desencadenen donde antes no lo hacían.

Actualizaciones de Apache Commons

Apache Commons ofrece componentes Java reutilizables. En esta versión, SSR actualizó la compatibilidad con los siguientes componentes:

- beanutils (1.9.4)

[1] Se requiere SCA 21.1 o una versión posterior.

- collections4 (4.4)
- dbutils (1.7)
- fileupload (1.4)
- lang (3.11)
- math (3.6.1)
- io (2.8.0)
- text (1.9)

Estas actualizaciones mejoran el modelado de las aplicaciones usando estos componentes, e identifican las protecciones frente a categorías como Log Forging y JSON Injection, así como nuevos lugares donde pueden aparecer los siguientes tipos de debilidades:

- Access Control: base de datos
- Denial of Service
- Aleatoriedad insegura: Propagación controlada por el usuario
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- SQL Injection
- System Information Leak (variantes)

Python (Versión 3.9)

Se ha actualizado la compatibilidad con la última versión de Python, que mejora el modelado de las API de lenguaje básicas.

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:

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:

- *Corrección de código: Comparación incorrecta de clases* en aplicaciones de Java y Kotlin
- *Dynamic Code Evaluation:* Problemas de *Code Injection* resueltos en los escáneres de Python 3
- Se han mejorado los problemas de *Key Management* para eliminar falsos positivos en todos los lenguajes
- *Cross-Site Scripting:* Los problemas de *DOM* relacionados con jQuery ya se han categorizado correctamente como *Cross-Site Scripting: Self* cuando provienen de un cuadro de entrada.
- Se han resuelto los problemas de *Password Management* en los archivos de configuración cuando se coteja contenido que no podría ser una contraseña.
- Mejoras en los falsos positivos de *Password Management* al cotejar con datos de localización.
- Se han eliminado resultados de *XML External Entity Injections* sobre funciones irrelevantes en aplicaciones de Java Spring.
- *ASP.NET MVC Bad Practices: Controller Not Restricted to POST* ahora considera seguros algunos verbos adicionales (PATCH, DELETE, PUT).

Correcciones de errores en iOS:
Debido a las mejoras en el análisis, era necesario actualizar las reglas. Esto puede hacer que los usuarios experimenten mejoras en los siguientes tipos de debilidades:

- Intercepción de entrada: Extensiones de teclado permitidas
- Privacy Violation: HTTP Get
- Privacy Violation: Almacenamiento en caché de teclado
- Privacy Violation: Almacenamiento en caché de pantalla
- Privacy Violation: Shoulder Surfing

Se han hecho también actualizaciones secundarias en algunos marcos para mejorar la precisión: Foundation, UIKit, WebKit, HealthKit, WatchKit, MessageUI, CoreLocation, CoreData.

Categorías eliminadas:
La siguiente categoría se ha eliminado en esta versión para aumentar la relevancia de los resultados:

- Privilege Management: Red Android

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

OGNL Expression Injection: Struts 2

Las vulnerabilidades críticas de OGNL Expression Language Injection identificadas mediante CVE-2019-0231 y CVE-2020-17530 afectan a las versiones 2.0 a 2.5.25 de Struts. La explotación de estas vulnerabilidades puede conllevar una ejecución arbitraria de código remoto en el servidor. Esta versión incluye una comprobación que permite detectar estas vulnerabilidades en aplicaciones web que usan Struts 2.

Detección de WAF[2]

Esta versión incluye una comprobación de "Detección de WAF", que arroja resultados informativos cuando se detecta un firewall de aplicación web durante un análisis. Estos resultados indican que la calidad del análisis puede verse comprometida si las solicitudes de análisis están bloqueadas antes de llegar a la aplicación.

Hacker Level Insights[2]

Hacker Level Insights ofrece a los desarrolladores y profesionales de la seguridad contexto en relación con la postura global de seguridad de su aplicación. Esta versión incluye una comprobación que señala las bibliotecas que se han detectado en la aplicación durante el análisis. Aunque estos resultados no representan necesariamente una vulnerabilidad de la seguridad, es importante destacar que los atacantes suelen llevar a cabo un reconocimiento de este tipo de objetivos para intentar identificar debilidades conocidas o patrones.

Actualizaciones de directivas

[2] Se requiere WebInspect 21.1 o una versión posterior.

SP 800-53 Rev. 5 del NIST

Se incorporó una directiva personalizada a la lista de directivas admitidas en WebInspect SecureBase para incluir las comprobaciones pertinentes para NIST SP 800-53 Rev. 5.

CWE Top 25 de 2020

Se incorporó una directiva personalizada a la lista de directivas admitidas en WebInspect SecureBase para incluir las comprobaciones pertinentes para CWE Top 25 2020.

DISA STIG 5.1

Se incorporó una directiva personalizada a la lista de directivas admitidas en WebInspect SecureBase para incluir las comprobaciones pertinentes para DISA STIG 5.1.

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:

Envenenamiento de la memoria caché web
Esta versión incluye una comprobación actualizada del *envenenamiento de la caché web: encabezados no codificados*. Los usuarios ya pueden añadir encabezados personalizados que sospechen que forman parte de la clave de la caché.

Accionadores de SpringBoot no seguros
Esta versión incluye una verificación actualizada para detectar accionadores de Spring Boot de información confidencial, disponible para usuarios sin privilegios, que ofrece resultados más precisos.

Mejoras para XSS
Esta versión incluye mejoras en la comprobación de ataques de XSS para Vue 3 y Angular JS 1.5.9 y superior.

Micro Focus Fortify Premium Content

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

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

26 de marzo de 2021