Contenido de Fortify Software Security

Actualización 3 de 2021
24 de septiembre de 2021

Acerca de CyberRes Fortify Software Security Research

Fortify Software Security Research transforma la investigación más avanzada en inteligencia de seguridad que impulsa la cartera de productos de Fortify, incluidos Fortify Static Code Analyzer, Fortify WebInspect y Fortify Application Defender. Actualmente, el contenido de CyberRes Fortify Software Security admite 1051 categorías de vulnerabilidad en 27 lenguajes de programación y abarca más de un millón de API distintas.

Fortify Software Security Research (SSR) se complace en anunciar la disponibilidad inmediata de actualizaciones para Fortify Secure Coding Rulepacks (en inglés, versión 2021.3.0), Fortify WebInspect SecureBase (disponible mediante SmartUpdate) y Fortify Premium Content.

CyberRes Fortify Secure Coding Rulepacks [Static Code Analyzer]

Con esta versión, Fortify Secure Coding Rulepacks detecta 831 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:

Actualizaciones de la biblioteca estándar de Golang (versión: 1.16)

Compatibilidad expandida para la biblioteca estándar 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 espacios de nombres de biblioteca estándar y aumenta la compatibilidad con las siguientes categorías nuevas:

- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute
- Go Bad Practices: Leftover Debug Code
- Insecure Randomness: Propagación en código fuente
- Insecure Randomness: Propagación controlada por el usuario
- El contenido del informe Insecure Transport: Ataques de degradado de conjuntos de cifrado
- El contenido del informe Insecure Transport: Weak SSL Protocol
- Often Misused: Privilege Management
- Firma criptográfica débil

Actualizaciones de Android 11 (nivel de API: 30)

La plataforma Android es una pila de software de código abierto diseñada para dispositivos móviles. Uno de los principales componentes de Android es el framework de la API de Java, que expone las funciones de Android a los desarrolladores de aplicaciones. Esta versión amplía la detección de vulnerabilidades en aplicaciones nativas de Android escritas en Java o Kotlin que aprovechan el framework de la API de Java de Android. Los usuarios obtendrán mejores resultados gracias a las actualizaciones del modelado de aplicaciones Android y la cobertura de la API. Esta versión también incluye nuevas vulnerabilidades en la gestión de permisos, que proporcionan orientación para los permisos peligrosos de Android:

- Privilege Management: Reconocimiento de actividad de Android
- Privilege Management: Calendario de Android
- Privilege Management: Historial de llamadas de Android
- Privilege Management: Cámara de Android
- Privilege Management: Contactos de Android
- Privilege Management: Micrófono de Android
- Privilege Management: Sensores de Android

Actualizaciones de la biblioteca estándar de iOS (versión: iOS 14)

Esta versión actualiza la compatibilidad con las API de la biblioteca de iOS 14 tanto para Swift como para Objective-C. Las actualizaciones se centran en los siguientes frameworks:

- UIKit
- UserNotification
- SwiftUI
- MessageUI

Los usuarios verán mejoras en las categorías de IPC no segura, inyección de enlaces, Path Manipulation, Privacy Violation, Shoulder Surfing y System Information Leak.

Actualizaciones de Micro Focus Visual COBOL (versión: 7.0)

Con la versión 7 de Micro Focus Visual COBOL, se ha ampliado la compatibilidad y se han añadido las dos vulnerabilidades siguientes:

- Integer Overflow
- Race Condition: Acceso al sistema de archivos

Compatibilidad con SAPUI5/OpenUI5[1] (versión: 1.93)

SAPUI5 es un framework de JavaScript de lado del cliente, creado por SAP, que comparte un conjunto de bibliotecas de control principales con OpenUI5 de código abierto. Esta versión ofrece compatibilidad inicial de identificación de vulnerabilidades para las siguientes categorías:

- Cross-Site Scripting: DOM
- Cross-Site Scripting: Control SAPUI5
- Cross-Site Scripting: Self
- Privacy Violation
- SAPUI5 Misconfiguration: Unsanitized Editor
- System Information Leak: External

Compatibilidad con JSON[2]

JavaScript Object Notation (JSON) es un formato ligero de intercambio de datos. Esta versión ofrece una mejor compatibilidad para identificar vulnerabilidades en JSON para las siguientes categorías:

- Password Management: Empty Password
- Password Management: contraseña codificada de forma rígida
- Password Management: Null Password
- Password Management: Password in Comment[3]

[1] Se han mejorado los resultados al utilizar Static Code Analyzer v21.2.0 o una versión superior.
[2] Requiere Static Code Analyzer v21.1.0 y el indicador: '-Dcom.fortify.sca.use.json-analyzer=true'.
[3] Se necesita Static Code Analyzer v21.2.0 o una versión superior. No se necesita ningún indicador a partir de Static Code Analyzer v21.2.0.

Actualizaciones de la biblioteca estándar de Kotlin (versión: 1.4.30)

Kotlin es un lenguaje de propósito general con un sistema de tipos estático que ofrece interoperabilidad con Java. Esta versión incluye una mejor compatibilidad con las nuevas API de la biblioteca estándar introducidas en Kotlin 1.4 dirigidas a la máquina virtual Java (JVM).

ECMAScript 2021 (versión: ECMA-262)

Compatibilidad con las nuevas API introducidas en ECMAScript 2021. ECMAScript es un lenguaje de programación de propósito general, definido por la especificación del lenguaje ECMAScript, más conocido por estar integrado en todos los navegadores web modernos. Sin embargo, cada vez es más común su uso para construir servidores web, aplicaciones móviles y otros tipos de aplicaciones tradicionales. Los clientes verán una mejora en el flujo de datos al analizar las aplicaciones dirigidas al último estándar ECMAScript.

Common Weakness Enumeration (CWE™) Top 25 de 2021

Las 25 debilidades de software más peligrosas (CWE Top 25) de Common Weakness Enumeration (CWE™) se introdujeron en 2019 y reemplazaron a SANS Top 25. La lista CWE Top 25 de 2021 se publicó en julio y se determinó mediante una fórmula heurística que normaliza la frecuencia y la gravedad de las vulnerabilidades comunicadas a la base de datos de vulnerabilidades de EE. UU. (NVD) en los últimos dos años. Para ayudar a los clientes que deseen dar prioridad en sus auditorías a las vulnerabilidades críticas más comunes de la NVD, se ha añadido una correlación de la taxonomía de CyberRes Fortify a la lista CWE Top 25 de 2021.

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 Static Code Analyzer anteriores a 18.x:

Como se observó con la versión 2020.4, todavía admitimos las cuatro últimas versiones principales de Static Code Analyzer. Por lo tanto, esta será la última versión de Rulepacks compatible con versiones de Static Code Analyzer anteriores a 18.x. En la próxima actualización, las versiones de Static Code Analyzer anteriores a 18.x no cargarán la instancia más reciente de Rulepacks. Se deberá cambiar a una versión inferior de Rulepacks o actualizar la versión de Static Code Analyzer.
En las versiones futuras, continuaremos admitiendo las cuatro últimas versiones principales de Static Code Analyzer.

Mejoras de Java J2EE:

Se ha mejorado la compatibilidad con las API de javax.servlet en las categorías de *Privacy Violation* y *System Information Leak*.

Servicios vinculados de Android:

Con nuestra asistencia continua para Android, esta versión incluye cobertura para los servicios vinculados de Android. Los clientes pueden tener incidencias nuevas en el flujo de datos debido a los parámetros del método de servicio vinculado de Android. Esto puede introducir rastreos de flujo de datos duplicados cuando los métodos se llaman dentro del servicio vinculado.

Weak Cryptographic Hash en Node.js:

Identifica los usos de los hashes criptográficos débiles en las aplicaciones Node.js.

La asignación OWASP ASVS 4.0 ahora admite los niveles

Para ayudar a los clientes que deseen tener la posibilidad de consultar los problemas que infringen los Niveles para la Verificación de Seguridad en Aplicaciones (L1, L2 y L3) de OWASP Application Security Verification Standard (ASVS), el último contenido de seguridad ha añadido estos niveles a los nombres de asignación. Ahora los clientes pueden buscar dentro de la agrupación OWASP ASVS 4.0 las palabras clave *L1*, *L2* y *L3* relacionadas, así como diseñar conjuntos de filtros y plantillas de filtros relacionados para su uso en AuditWorkbench y Software Security Center (SSC).

Mejoras en falsos positivos:

Se ha seguido trabajando para eliminar los falsos positivos en esta versión. Además de las otras mejoras, los clientes disfrutarán de una eliminación adicional de falsos positivos en las áreas siguientes:

- Falsos positivos de *Cross-Site Scripting* en código jQuery
- *Privacy Violation: Shoulder Surfing* en aplicaciones .NET con el atributo JsonIgnore
- Más consistencia en la reducción de incidencias de *Path Manipulation* de Fortify Priority Order donde solo se puede controlar un número
- Ya no identificamos las contraseñas en Swift cuando forman parte de una enumeración
- *Falta validación de XML* en .NET
- *Falta comprobación de parámetro cero* en proyectos Java

CyberRes 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

Insecure Deployment: HTTP Request Smuggling

El contrabando de HTTP2 en texto sin cifrar, o el contrabando h2c, es una alternativa al contrabando tradicional de solicitudes HTTP que abusa de los elementos frontend que no reconocen h2c, como los servidores proxy, para crear un túnel hacia los sistemas backend. Un atacante puede utilizar este túnel para traficar solicitudes adicionales al servidor de backend sin que el servidor de frontend las detecte. Esto puede dar a los atacantes la posibilidad de eludir los controles de autorización en los frontend y acceder a recursos restringidos en los sistemas backend. Esta versión incluye una comprobación para detectar configuraciones que se pueden utilizar para ataques de contrabando h2c.

Access Control: falta comprobación de autorización

GraphQL Introspection permite consultar el servidor para obtener información sobre un esquema subyacente. Introspection ofrece detalles sobre elementos como consultas, tipos y campos. GraphQL Introspection suele estar activado por defecto. Un atacante sin la debida autorización puede hacer un mal uso de esta información para ataques como SQL Injection y ataques por lotes. Esta versión incluye una verificación para detectar extremos GraphQL que tienen la introspección habilitada.

NoSQL Injection: MongoDB

Las vulnerabilidades de inyección de scripts NoSQL permiten a los atacantes inyectar consultas maliciosas en la base de datos. MongoDB es una de las bases de datos NoSQL y su documentación indica que permite que las aplicaciones ejecuten operaciones de JavaScript. NoSQL Injection es muy peligrosa, ya que un atacante sin autentificar puede extraer datos o ejecutar código JavaScript. Esto puede dar lugar a la ejecución remota de código, al compromiso de la confidencialidad y la integridad de los datos de la aplicación y a ataques Denial of Service (DoS). Esta versión incluye una comprobación que permite detectar la inyección de scripts NoSQL en MongoDB.

Dynamic Code Evaluation: Unsafe Deserialization

CVE-2021-35464 ha identificado una vulnerabilidad de deserialización Java insegura de preautorización en el servidor ForgeRock AM anterior a la versión 7.0 y el servidor OpenAM anterior a la versión 14.6.4. Esta vulnerabilidad permite a los atacantes elaborar un objeto serializado malicioso en el parámetro jato.pageSession y enviarlo al extremo "/ccversion/Version" mediante una única solicitud. La vulnerabilidad existe debido al uso de una biblioteca Java de terceros insegura en la aplicación. Este problema normalmente permite a los atacantes ejecutar código arbitrario en el servidor, abusar de la lógica de la aplicación o realizar ataques Denial of Service (DoS). Esta versión incluye una comprobación que permite detectar esta vulnerabilidad en servidores web objetivo.

Cross-Site Scripting: DOM[4]

Los ataques Cross-Site Scripting ocurren cuando las páginas web generadas dinámicamente muestran los datos del usuario, como la información de inicio de sesión, que no se ha validado correctamente, lo que permite a los atacantes incrustar scripts maliciosos en la página generada y, luego, ejecutar el script en la máquina de cualquier usuario que vea el sitio. En el caso del XSS basado en el modelo de objetos del documento (DOM), el contenido malicioso se ejecuta como parte de la manipulación del DOM. Si tienen éxito, las vulnerabilidades de Cross-Site Scripting basadas en DOM pueden aprovecharse para manipular o robar cookies, crear solicitudes que se pueden confundir con las de un usuario válido, comprometer información confidencial o ejecutar código malicioso en los sistemas del usuario final. Esta versión contiene una nueva comprobación para detectar XSS basado en DOM en fragmentos URI del lado del cliente.

Web Server Misconfiguration: Insecure Mapping Directives

Configurar Nginx para ejecutar PHP en el servidor web a veces requiere pasar cada URI que termina en .php al intérprete de PHP del backend (como FastCGI). Nginx, con esta configuración insegura de PHP, considerará las carpetas en la ruta de la URL como el archivo de destino que se debe ejecutar si la ruta completa solicitada no lleva a un archivo real existente. Esta configuración incorrecta permite al atacante ejecutar código PHP arbitrario en cualquier tipo de archivo, como un archivo de imagen, si se puede cargar en el servidor web y acceder a él. Esta versión incluye una comprobación que permite detectar esta vulnerabilidad en servidores web objetivo.

[4] Requiere WI v21.2.0 o una versión superior.

Integer Overflow

Las versiones de Nginx desde la 0.5.6 hasta la 1.13.2 son susceptibles a una vulnerabilidad de desbordamiento de enteros identificada por CVE-2017-7529. Este problema existe en el módulo de filtro de rango de Nginx y permite a un atacante adquirir información potencialmente sensible mediante el envío de una solicitud especialmente diseñada. Esta versión incluye una comprobación que permite detectar la vulnerabilidad CVE-2017-7529 en servidores web objetivo.

Informes de cumplimiento

Common Weakness Enumeration (CWE™) Top 25 de 2021

Las 25 debilidades de software más peligrosas (CWE Top 25) de Common Weakness Enumeration (CWE™) se introdujeron en 2019 y reemplazaron a SANS Top 25. La lista CWE Top 25 de 2021 se publicó en julio y se determina mediante una fórmula heurística que normaliza la frecuencia y la gravedad de las vulnerabilidades comunicadas a la base de datos de vulnerabilidades de EE. UU. (NVD) en los últimos dos años. Esta actualización de SecureBase incluye asignaciones para estas categorías de CWE. Esta actualización incluye 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”.

Actualizaciones de directivas

CWE Top 25 de 2021

Se incorporó una directiva personalizada a la lista de directivas admitidas en WebInspect SecureBase para incluir las comprobaciones pertinentes para CWE Top 25 2021.

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:

LDAP Injection

Esta versión mejora la comprobación de LDAP Injection para reducir los falsos positivos y mejorar la precisión de sus resultados.

CyberRes Fortify Premium Content

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

Top 25 de CWE 2021

Para acompañar las nuevas correlaciones, esta versión también contiene un nuevo paquete de informes para Fortify Software Security Center compatible con el Top 25 de CWE de 2021 que se puede descargar de Fortify Customer Support Portal, en la sección Premium Content.

Taxonomía de CyberRes 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 CyberRes Fortify Support Portal.

Póngase en contacto con el soporte técnico de Fortify

CyberRes Fortify
http://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

Póngase en contacto con SSR

Alexander M. Hoole
Director sénior de Software Security Research
CyberRes Fortify hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
Director de Software Security Research
CyberRes Fortify
peter.blay@microfocus.com