Micro Focus

Contenido de seguridad del software Fortify

Actualización 1 de 2020

27 de marzo 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 1019 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 2020.1.0), 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 810 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 para la biblioteca estándar GoLang[1]

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 nombre de bibliotecas estándar y admite 53 tipos de debilidades, incluidas las siguientes 19 categorías adicionales:

- Denial of Service: Regular Expression
- Formula Injection
- Insecure Randomness
- JSON Injection
- Key Management: Empty HMAC Key
- Key Management: Hardcoded HMAC Key
- Log Forging
- Log Forging (debug)
- Resource Injection
- Weak Cryptographic Hash
- Weak Cryptographic Hash: Hardcoded Salt
- Weak Cryptographic Hash: User-Controlled Salt
- Weak Cryptographic Signature: Insufficient Key Size
- Weak Cryptographic Signature: User-Controlled Key Size
- Weak Encryption: Inadequate RSA Padding
- Weak Encryption: Insecure Initialization Vector
- Weak Encryption: Stream Cipher
- Weak Encryption: User-Controlled Key Size
- XML Injection

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:

- En JavaScript, las instancias de “Cross-Site Scripting: DOM” que habían sido identificadas con mayor precisión como XSS automático se han modificado a la nueva subcategoría “Cross-Site Scripting: Self” y ahora se identifican con una prioridad inferior.

[1] Se recomienda SCA v20.1.0 o posterior para resultados de análisis óptimos.

- En Java, debido a mejoras en el motor de modelado, se produjo un aumento inadvertido en la cantidad de falsos positivos de Dead Code, particularmente en relación con las condiciones “if”. Se mejoraron las reglas para eliminar una cantidad significativa de problemas no válidos.
- Se resolvieron problemas de rendimiento poco frecuentes relacionados con aplicaciones JSP y Spring MVC.
- Se realizaron actualizaciones a metadatos externos para correlación con Common Weakness Enumeration (CWE™) mejorado con Micro Focus Fortify: Taxonomía de errores de seguridad de software (también denominado 7 Pernicious Kingdoms). Entre las mejoras se encuentran la alineación de 41 Id. de CWE adicionales en las 935 categorías de la taxonomía de errores de seguridad de software, lo que produce actualizaciones en las asignaciones de CWE y CWE Top 25 2019. Necesariamente, todas las capacidades de generación de informes o filtros “Group By” de CWE se verán afectadas. Los Id. de CWE adicionales incluyen lo siguiente:

  CWE-88, CWE-97, CWE-119, CWE-147, CWE-192, CWE-203, CWE-212, CWE-266, CWE-267, CWE-276, CWE-279, CWE-280, CWE-346, CWE-347, CWE-436, CWE-506, CWE-527, CWE-529, CWE-530, CWE-531, CWE-536, CWE-540, CWE-541, CWE-548, CWE-550, CWE-705, CWE-775, CWE-799, CWE-917, CWE-921, CWE-923, CWE-925, CWE-926, CWE-937, CWE-942, CWE-1004, CWE-1021, CWE-1069, CWE-1173, CWE-1188, CWE-1236.

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

Inclusión de archivos peligrosos: Local

Una vulnerabilidad grave que afecta a Tomcat aprovecha la funcionalidad del protocolo AJP para acceder a archivos en el lado del servidor y permitir que un atacante lea o incluya cualquier archivo en directorios de webapps de Apache Tomcat. Esta vulnerabilidad se denomina GhostCat y se la identifica mediante el nombre CVE-2020-1938. Además, esto podría permitir un ataque mediante ejecución de código arbitrario. Este problema afecta a Apache Tomcat 9.x (anterior a 9.0.31), 8.x (anterior a 8.5.51), 7.x (anterior a 7.0.100) y a todas las versiones anteriores. Esta actualización de SecureBase incluye una comprobación que permite detectar esta vulnerabilidad.

Asignaciones de Common Weakness Enumeration (CWE™)

Common Weakness Enumeration (CWE™) es una taxonomía de errores de software que pueden producir vulnerabilidades en el software. La taxonomía es una manera de consolidar la salida de varias metodologías en la evaluación de riesgos y vulnerabilidades de software durante distintas etapas de SDLC. En esta versión, Securebase incluye asignaciones actualizadas de verificaciones a actualizaciones recientes de CWE. CWE es una taxonomía jerárquica. Las verificaciones se asignan al subnodo más cercano que coincide con el propósito de la verificación.

Informe de cumplimiento

Common Weakness Enumeration (CWE™) Top 25

Los 25 errores de software más peligrosos de Common Weakness Enumeration (CWE™) (CWE Top 25) es un listado creado por MITRE. El listado incluye las 25 categorías más comunes de debilidades de software que pueden producir vulnerabilidades en software. Esta actualización de Securebase incluye asignaciones para estas categorías de CWE. Hemos incluido 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

Common Weakness Enumeration (CWE™)

Los 25 errores de software más peligrosos de Common Weakness Enumeration (CWE™) (CWE Top 25) es un listado creado por MITRE. El listado incluye las 25 categorías más comunes de debilidades de software que pueden producir vulnerabilidades en software. Esta versión incluye una directiva que contiene el listado de verificaciones para evaluar las vulnerabilidades asignadas en CWE Top 25.

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 corrección de un error en la verificación HTTP Request Smuggling reduce los falsos positivos relacionados con búsquedas con el Id. de verificación 11621. La verificación ya no considerará a HTTP 405 como una verificación válida de la vulnerabilidad.
- El contenido del informe Insecure Transport: Weak SSL Cipher ahora incluye un ejemplo para excluir cifrados de modo CBC mediante la inclusión de !SHA246 y !SHA384 en la cadena de configuración. Sin embargo, recomendamos consultar al administrador de servidores para crear una configuración que seleccione un conjunto de cifrados robustos de lista blanca.
- Se realiza una corrección adicional en la detección de Insecure Transport: Weak SSL Cipher para mejorar la detección de configuración en casos donde la verificación no pudo identificar cifrados correctos si el servidor admitía únicamente TLS1.2 y cifrados más robustos.

Micro Focus Fortify Premium Content

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

OWASP Application Security Verification Standard (ASVS)

Application Security Verification Standard (ASVS) es un listado de requisitos de seguridad y pruebas de aplicaciones que deben realizarse durante la configuración y el ciclo de vida de desarrollo de software (SDLC) para desarrollar software seguro. Hemos creado asignaciones de verificaciones de Securebase y reglas de SCA a los requisitos aplicables del estándar. Sin embargo, durante el proceso de creación de correlaciones con nuestros productos, detectamos instancias donde las asignaciones de CWE proporcionadas por el estándar pueden mejorarse aún más para estar alineados con mayor precisión con las verificaciones de Securebase y las reglas de SCA. Mientras trabajamos en estas mejoras, podemos poner estos artefactos a disposición de clientes interesados para su evaluación y colaboración. En caso de estar interesado, utilice el contacto de SSR que aparece abajo para obtener la plantilla de cumplimiento y la directiva de WebInspect, o un paquete de propagación de SSC.

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

27 de marzo de 2020