Contenido de seguridad del software Fortify

Actualización 2 de 2024
viernes, 28 de junio de 2024

Acerca de OpenText Fortify Software Security Research

El equipo de Fortify Software Security Research transforma la investigación más avanzada en inteligencia de seguridad que impulsa la cartera de productos de Fortify, que incluye OpenText™ Fortify Static Code Analyzer y OpenText™ Fortify WebInspect. En la actualidad, el contenido de seguridad del software Fortify admite 1.660 categorías de vulnerabilidades en 33 lenguajes 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 2024.2.0), Fortify WebInspect SecureBase (disponible mediante SmartUpdate) y Fortify Premium Content.

Fortify Secure Coding Rulepacks [Fortify Static Code Analyzer]

Con esta versión, Fortify Secure Coding Rulepacks detecta 1.435 categorías únicas de vulnerabilidades en más de 33 lenguajes y abarca más de un millón de API distintas. En resumen, esta versión incluye lo siguiente:

Soporte mejorado para Node.js (versión compatible: 21.x)[1]

Node.js es un entorno de ejecución de JavaScript multiplataforma que permite a los desarrolladores crear servidores, aplicaciones web, herramientas de línea de comandos y mucho más. Esta versión contiene actualizaciones importantes de nuestro soporte con Node.js para los siguientes módulos en Node.js 21.x:

- async_hooks
- buffer
- child_process
- crypto
- dgram
- dns
- fs
- http
- https
- net
- os
- path
- process
- punycode
- querystring
- stream
- string_decoder
- timers
- tls
- url
- util
- v8
- vm
- worker_threads
- zlib

Estas actualizaciones mejoran la detección de problemas para las siguientes categorías de vulnerabilidades:

- Command Injection
- Dynamic Code Evaluation: Code Injection
- Header Manipulation

[1] Requiere la versión 24.2 o posterior de Fortify Static Code Analyzer.

- Insecure Transport: Weak SSL Cipher
- Insecure Transport: Weak SSL Protocol
- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- System Information Leak
- System Information Leak: External

Además, en esta versión se introducen las siguientes categorías de vulnerabilidades para las aplicaciones de Node.js:

- DNS Spoofing
- Dynamic Code Evaluation: Script Injection
- Insecure Transport: Insufficient Diffie Hellman Strength
- Key Management: Empty HMAC Key
- Key Management: Empty PBE Password
- Key Management: Hardcoded HMAC Key
- Key Management: Hardcoded PBE Password
- Weak Cryptographic Hash
- Weak Cryptographic Hash: Empty PBE Salt
- Weak Cryptographic Hash: Hardcoded PBE Salt
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Cryptographic Hash: Predictable Salt
- Weak Cryptographic Hash: User-Controlled PBE Salt
- Weak Encryption
- Weak Encryption: Insecure Initialization Vector
- Weak Encryption: Insecure Mode of Operation
- Weak Encryption: Stream Cipher

Soporte mejorado para Java (versión compatible: 21)

Java 21 es la última versión de soporte a largo plazo (LTS) para la plataforma Java. Incluye mejoras a las API existentes, pero también incluye una cantidad significativa de características nuevas. A continuación se incluyen algunas de las más importantes: Función y memoria externas, colecciones secuenciadas, encapsulación de claves, subprocesos virtuales, concurrencia estructurada, variables sin nombre y valores con alcance. Algunas de estas funciones aún se encuentran en estado de vista previa, pero se consideran lo suficientemente desarrolladas como para incluir cobertura. Entre las categorías actualizadas se incluyen las siguientes:

- Process Control
- Unreleased Resource
- Weak Encryption
- Weak Cryptographic Hash

Además, se admiten las siguientes categorías nuevas:

- Restricted Method
- Weak Cryptographic Signature: XML Signature Secure Validation Disabled

Soporte MyBatis mejorado (versión compatible: 3.5. x)

MyBatis es un asignador SQL que se utiliza para acoplar objetos en una base de datos relacional con objetos en una aplicación orientada a objetos. Este marco combina procedimientos almacenados y declaraciones SQL utilizando descriptores XML o anotaciones de código para facilitar el proceso de desarrollo y la comunicación de la base de datos. El soporte para MyBatis se actualizó a la versión 3.5.16. Las mejoras incluyen el soporte actualizado para las siguientes categorías de vulnerabilidades:

- Dynamic Code Evaluation: Unsafe Deserialization
- SQL Injection
- System Information Leak
- Unreleased Resource: Database
- Unsafe Reflection

Soporte inicial de MyBatis-Plus (versión compatible: 3.5.x)

MyBatis-Plus se basa en el marco MyBatis existente para simplificar el desarrollo al proporcionar funciones listas para usar que resultan útiles y eficientes más allá de las que se encuentran en el marco original. Se proporciona soporte inicial para MyBatis - Plus 3.5.x. Se proporciona soporte de categoría inicial para *Inyección SQL*.

Detección de riesgos originados por modelos de inteligencia artificial (IA) y aprendizaje automático (ML)

Con el uso de la IA generativa y los grandes modelos de lenguaje (LLM) que están cambiando rápidamente el espacio de soluciones de la industria del software, se están presentando nuevos riesgos. Esta versión mejora la cobertura para proyectos que consumen API de OpenAI (Python y JavaScript), TensorFlow (Python) o Anthropic Claude (Python y JavaScript). El soporte detecta vulnerabilidades resultantes de la confianza implícita en las respuestas de las API del modelo AI/ML, además de las siguientes características:

Soporte mejorado para OpenAI (versión compatible: 1.14.x [Python], 4.33.x [JavaScript])

Las bibliotecas OpenAI para Python, TypeScript y JavaScript proporcionan herramientas integrales para integrar capacidades avanzadas de IA en diversas aplicaciones. Estas bibliotecas admiten una variedad de funcionalidades, incluido el procesamiento del lenguaje natural, la generación de texto y la IA conversacional. Con API intuitivas y fáciles de usar, los desarrolladores pueden integrar sin problemas los modelos de IA de última generación de OpenAI en sus proyectos, lo que mejora la interactividad y la inteligencia en entornos Python, TypeScript y JavaScript. El soporte mejorado amplía la cobertura para *Cross-Site Scripting: AI* y añade dos nuevas categorías de vulnerabilidades:

- Cross-Site Scripting: DOM AI
- Prompt Injection

TensorFlow (versión compatible: 2.16.x)

TensorFlow, un marco líder de aprendizaje automático de código abierto de Google, ofrece un potente conjunto de herramientas para crear e implementar modelos de aprendizaje automático. Con bibliotecas integradas y modelos previamente entrenados, simplifica la creación de aplicaciones de aprendizaje profundo. TensorFlow es escalable para una colección diversa de proyectos, que van desde prototipos de investigación hasta sistemas de producción a gran escala. La cobertura inicial incluye soporte con las dos siguientes categorías:

- Path Manipulation
- Privacy Violation
- System Information Leak: Internal

Además, el soporte añade la nueva categoría de vulnerabilidad:

- Dynamic Code Evaluation: Unsafe TensorFlow Deserialization

Anthropic Claude SDK (versión compatible: 0.21.3 [Python], 0.20.5 [JavaScript])

Las bibliotecas de Anthropic Claude para Python y JavaScript proporcionan herramientas integrales para integrar Claude, un sofisticado modelo de lenguaje de IA, en aplicaciones. La cobertura inicial incluye soporte para *Cross-Site Scripting: AI* y añade dos nuevas categorías de vulnerabilidades:

- Cross-Site Scripting: DOM AI
- Prompt Injection

Soporte Django mejorado (versión compatible: 5.0.x)

Django es un marco web escrito en Python que ha sido diseñado para facilitar el desarrollo web rápido y seguro. La velocidad y la seguridad del desarrollo se logran gracias al alto nivel de abstracción del marco, donde se utilizan construcciones y generación de código para reducir drásticamente el código boilerplate. En esta versión, hemos actualizado nuestra cobertura existente de Django para admitir versiones hasta la versión 5.0.x.

Estas actualizaciones mejoran la detección de problemas para las siguientes categorías de vulnerabilidades:

- Access Control: Database
- Cookie Security: CSRF Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set on CSRF Cookie
- Cookie Security: HTTPOnly not Set on Session Cookie
- Cookie Security: Session Cookie not Sent Over SSL
- Cross-Frame Scripting
- Cross-Site Request Forgery
- HTML5: Cross-Site Scripting Protection
- HTML5: MIME Sniffing
- HTML5: Misconfigured Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- Insecure Transport
- Insecure Transport: HSTS Does Not Include Subdomains
- Insecure Transport: HSTS not Set
- Insecure Transport: Insufficient HSTS Expiration Time
- Privacy Violation: BREACH
- SQL Injection

Soporte inicial de Paramiko (versión compatible: 3.4.x)

Paramiko es una biblioteca de Python para conectarse a máquinas mediante SSH. Paramiko proporciona un conjunto de funcionalidades para abstraer los métodos criptográficos del desarrollador. Esto proporciona funciones de alto nivel similares a la programación de sockets y otorga a los desarrolladores acceso a métodos de nivel inferior para la configuración de microgestión de una conexión SSH. El soporte inicial cubre las siguientes categorías de vulnerabilidades:

- Command Injection
- Insecure Transport: Cipher Suite Downgrade
- Insecure Transport: Weak SSL Cipher
- Password Management: Hardcoded Password
- SSH Misconfiguration: Missing Authentication

Soporte mejorado para PHP (versión compatible: 8.3)

PHP es un lenguaje de programación de uso general ampliamente utilizado que se utiliza con mayor frecuencia para el desarrollo web. Esta versión actualiza el soporte para PHP hasta la versión 8.3. En particular, la versión incluye soporte mejorado para las siguientes extensiones:

- DOM (versión compatible: 8.3)

  La extensión DOM de PHP permite operaciones en documentos XML y HTML en PHP mediante el uso de un modelo de objetos de documento. El soporte ampliado para esta biblioteca incluye soporte mejorado de flujo de datos para operaciones DOM, así como cobertura adicional para identificar vulnerabilidades de *Manipulación de configuración*.

- JSON (versión compatible: 8.3)

  La extensión JSON de PHP permite el uso de un analizador JSON escrito y autorizado bajo la licencia PHP. El soporte inicial de esta extensión incluye soporte de flujo de datos para las funciones de la extensión.

- OpenSSL (versión compatible: 8.3)

  La extensión OpenSSL de PHP implementa características de la biblioteca OpenSSL para varias operaciones criptográficas. El soporte ampliado para esta biblioteca incluye soporte mejorado de flujo de datos para pares de claves criptográficas.

- Simdjson (versión compatible: 8.3)

  La extensión Simdjson de PHP implementa los enlaces específicos de PHP del proyecto simdjson para proporcionar una decodificación JSON rápida. El soporte inicial incluye la siguiente categoría nueva para PHP:

  - JSON Path Manipulation

Soporte mejorado para iOS (versión compatible: 17)[2]

El SDK de iOS y IPadOS de Apple proporciona una recopilación de sistemas que permiten a los desarrolladores crear aplicaciones móviles para dispositivos iPhone y iPad de Apple. Esta versión contiene actualizaciones graduales de nuestro soporte de iOS SDK con Swift y Objective-C. Reglas nuevas y actualizadas amplían nuestra cobertura de los siguientes marcos en iOS 17:

- CryptoKit

[2] Las API de iOS 17 requieren Xcode 15 o superior, que a su vez requiere Fortify Static Code Analyzer 23.2 o posterior. Sin embargo, es posible que haya advertencias del compilador al utilizar Source Code Analyzer 23.2 para crear aplicaciones que utilicen las API de iOS 17. Se recomienda Fortify Static Code Analyzer 24.2 o posterior para garantizar una compilación y un análisis válidos.

- Foundation
- Network
- os
- System
- SwiftUI
- UIKit

Estas actualizaciones mejoran la detección de problemas para las siguientes categorías de vulnerabilidades:

- Insecure Transport
- Path Manipulation
- Privacy Violation
- Privacy Violation: Health Information
- System Information Leak: External
- System Information Leak: Internal
- Unreleased Resource: Synchronization
- Unsafe Reflection
- Weak Cryptographic Hash
- Weak Cryptographic Hash: User-Controlled Salt
- Weak Encryption: User-Controlled Key Size

Soporte mejorado de MISRA C 2012

MISRA es una organización de estándares que crea y mantiene varios estándares para el desarrollo de aplicaciones utilizadas en entornos críticos para la seguridad que requieren alta integridad o alta confiabilidad en el software. Esta versión incluye soporte para dos nuevas categorías que se corresponden en gran medida con dos reglas directrices obligatorias en el estándar MISRA C 2012:

- Undefined Behavior: File Pointer Dereference
- Undefined Behavior: File Pointer Use After Close

Actualización de propiedades de expresión regular de contraseña

Las propiedades de expresión regular de contraseña, introducidas en Fortify Static Code Analyzer versión 23.1, son propiedades personalizables que contienen expresiones regulares que dictan cómo las reglas de Fortify coinciden con los identificadores de contraseña en varios idiomas. En esta versión, ampliamos el valor predeterminado de la propiedad com.fortify.sca.rules.password_regex.global para reconocer identificadores de contraseña que incluyan la palabra "secreto". Además, añadimos nuevas reglas para utilizar las propiedades de expresión regular de la contraseña al analizar cadenas JSON generadas de forma dinámica. Como resultado, los clientes pueden esperar una detección mejorada en las siguientes categorías en todos los idiomas:

- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Privacy Violation

Soporte mejorado para Golang (versión compatible: hasta la 1.21)

Go, también conocido como Golang, es un lenguaje de programación compilado de tipo estático creado en Google. Se conoce por su simplicidad, eficiencia y gran compatibilidad con la competencia, lo que lo hace ideal para crear servicios web escalables, canales de datos y sistemas distribuidos. Esta versión incluye la detección de vulnerabilidades *Unreleased Resource* e introduce una nueva detección *Inyección SQL* para proyectos que utilizan GORM v2.

Mejoras de la API de WordPress (versión compatible: hasta 6.5) (recuento de API: 2)

La interfaz de programación de aplicaciones (API) de WordPress se puede dividir en múltiples secciones/temas de API, cada una de las cuales cubre las funciones involucradas y el uso de un conjunto determinado de funcionalidades. Juntas forman lo que podría llamarse la API de WordPress, que es la interfaz de plugin/tema/complemento creada por todo el proyecto de WordPress. Esta versión añade un soporte inicial para identificar problemas en las siguientes API:

- REST API
- Shortcode API

Otras erratas

En esta versión, seguimos invirtiendo recursos para garantizar la reducción del número de falsos positivos, lograr una mejor consistencia 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:

Reducción de falsos positivos y otras mejoras notables en la detección

Se ha seguido trabajando con el fin de eliminar los falsos positivos en esta versión. Los clientes pueden esperar una mayor eliminación de falsos positivos y otras mejoras notables relacionadas con las siguientes áreas:

- *ASP.NET MVC Bad Practices: Optional Submodel With Required Property*: se han reducido los falsos positivos en las aplicaciones ASP.NET
- *Insecure Transport: Mail Transmission*: reducción de falsos positivos en aplicaciones Java
- *Password Management: Hardcoded Password*: reducción de falsos positivos en archivos JSON/YAML
- *Unreleased Resource: Streams*: reducción de falsos positivos en aplicaciones Java
- *Password Management: Hardcoded Password*: nuevos problemas detectados en aplicaciones Python relacionados con tipos de diccionario
- *Password Management: Hardcoded Password*: nuevos problemas detectados en aplicaciones ASP.NET relacionados con cadenas interpoladas
- Se eliminaron muchos falsos positivos que provenían de las propiedades integradas del sistema JDK.

Cambios de nombre de categoría

Cuando se producen cambios en el nombre de la categoría de vulnerabilidad, los resultados del análisis al fusionar escaneos anteriores con nuevos escaneos podrían dar como resultado categorías añadidas o eliminadas.

Para mejorar la coherencia, se han cambiado los nombres de las siguientes tres categorías:

Nombre de la categoría 2024 R1	Nombre de la categoría 2024 R2
Access Control: gRPC Authentication Bypass	Access Control: gRPC Fail Open
AWS CloudFormation Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key	AWS CloudFormation Misconfiguration: SecretsManager Missing Customer-Managed Encryption Key
AWS Terraform Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key	AWS Terraform Misconfiguration: SecretsManager Missing Customer-Managed Encryption Key

Identificador de correlación de control DISA (CCI) versión 2

La CCI de la Agencia de Sistemas de Información de Defensa (DISA) es un documento que cierra la brecha entre la orientación de ciberseguridad de alto y bajo nivel al proporcionar un conjunto de identificadores estándar combinados con declaraciones singulares y procesables. El STIG de desarrollo y seguridad de aplicaciones de DISA está estrechamente relacionado con el CCI de DISA, en el que un único control STIG puede aplicarse a uno o más CCI. Esta versión equipara los CCI asignados con las actualizaciones recientes de las asignaciones STIG con la taxonomía Fortify durante las versiones anteriores.

Publicación especial de NIST 800-53, revisiones 4 y 5

La publicación especial 800-53 del National Institute of Standards and Technology (NIST) es un documento que proporciona un catálogo de controles de seguridad y privacidad para sistemas de información que el campo de la ciberseguridad en general puede aprovechar para brindar orientación sobre cómo proteger los sistemas. La publicación especial NIST 800-53 está estrechamente relacionada con DISA CCI, en la que un único CCI puede aplicarse a uno o más controles NIST 800-53. Esta versión equipara los controles NIST 800-53 asignados con las actualizaciones recientes de las asignaciones de DISA CCI con la taxonomía Fortify.

OWASP Mobile Top 10 2023

Como ya se ha anunciado, en la próxima versión de Fortify Software Security Content, el mapeo OWASP Mobile Top 10 2023 ha quedado obsoleto y solo permanece el OWASP Mobile Top 10 2024 actualizado.

Alinear las versiones de contenido de seguridad del software con el control de versiones de OpenText

La próxima versión contendrá un cambio en las versiones del contenido de seguridad. Esta será la última versión de actualización de contenido de seguridad de OpenText Fortify que sigue la convención de nomenclatura de la "Actualización 2 de 2024". Para alinearse con los estándares de control de versiones de OpenText, las versiones están programadas una por trimestre cada año y están numeradas según el año y el trimestre; por lo tanto, la próxima versión de OpenText™ Fortify™ Software Security Content será la 24.4, lo que indica una versión en el primer mes del 4.º trimestre de 2024.

Fortify SecureBase [Fortify WebInspect]

Fortify SecureBase combina las comprobaciones para miles de vulnerabilidades con las directivas que guían a los clientes en las siguientes actualizaciones disponibles inmediatamente con SmartUpdate.

Compatibilidad de vulnerabilidades

Denial of Service: GraphQL

El lenguaje de consulta GraphQL para API proporciona un tiempo de ejecución para consultar datos existentes. El esquema GraphQL es un modelo que consta de objetos de datos, sus campos y tipos, y sus relaciones con otros objetos de datos. Las referencias entre diferentes objetos de datos pueden crear un ciclo. Un atacante puede desencadenar un uso excesivo de CPU y memoria al crear una consulta cíclica costosa y anidada maliciosa para provocar una denegación de servicio (DoS). Esta versión incluye una comprobación que permite detectar referencias circulares en el esquema de GraphQL.

Access Control: Authorization Bypass (CVE-2024-27198)

CVE-2024-27198 ha sido identificada como una vulnerabilidad crítica en el software JetBrains y representa una importante amenaza a la seguridad. Esta vulnerabilidad resalta los riesgos asociados con mecanismos de autenticación insuficientes, que pueden permitir a atacantes no autenticados obtener un control administrativo sobre los sistemas afectados. La última versión incluye una comprobación que permite detectar esta vulnerabilidad en los servidores de destino.

Directory Traversal (CVE-2024-27199)

Las versiones del servidor JetBrains TeamCity On-Premises anteriores a la 2023.11.4 son vulnerables a un fallo de recorrido de ruta, identificado como CVE-2024-27199. Los atacantes pueden utilizar este fallo para eludir los controles de autenticación y amenazar significativamente la integridad y confidencialidad del sistema. La última versión incluye una comprobación que permite detectar esta vulnerabilidad en los servidores de destino.

Dynamic Code Evaluation: Deserialización no segura (CVE-2023-26360)

Las versiones 2018 Update 15 y anteriores de Adobe ColdFusion, así como 2021 Update 5 y anteriores, se ven afectadas por una vulnerabilidad de evaluación de código dinámico, identificada por CVE -2023-26360. Esta vulnerabilidad podría resultar en la ejecución de código arbitrario en el contexto del usuario actual. La explotación de este problema no requiere la interacción del usuario. Esta versión incluye una comprobación que permite detectar esta vulnerabilidad en los servidores de destino.

Insecure Deployment: Unpatched Application (CVE-2024-32962)

CVE-2024-32962 es una vulnerabilidad crítica asociada con xml-crypto, una biblioteca de cifrado y firma digital XML para Node.js. Esta vulnerabilidad se introdujo en la versión 4.0.0 y se solucionó en la versión 6.0.0. La vulnerabilidad surge porque, en las versiones afectadas, la configuración predeterminada no comprueba la autorización del firmante. Un atacante puede aprovechar esta situación modificando un documento XML y reemplazando la firma existente por una generada con una clave privada maliciosa, adjuntando el certificado correspondiente al elemento <KeyInfo/>. Esta versión incluye una verificación para detectar esta vulnerabilidad en servidores de destino que usan las versiones xml -crypto afectadas.

Otras erratas

En esta versión hemos invertido recursos para reducir aún más el número de falsos positivos y para mejorar la capacidad de auditar problemas por parte de los clientes. Los clientes también verán cambios en los resultados comunicados en relación con las siguientes áreas:

Insecure Deployment: OpenSSL

Esta versión incluye mejoras en la verificación OpenSSL ChangeCipherSpec Man-in-the-Middle (MitM) para reducir los falsos positivos y mejorar la precisión de los resultados.

Fortify Premium Content

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

Fortify Taxonomy: errores en la seguridad del software

El sitio Fortify Taxonomy, que contiene descripciones de la compatibilidad con las nuevas categorías añadidas, está disponible en https://vulncat.fortify.com.

Comuníquese con el servicio de atención al cliente

OpenText Fortify
https://softwaresupport.softwaregrp.com/
+1 (800) 509-1800

Comuníquese con SSR

Alexander M. Hoole
Director sénior del equipo de Software Security Research
OpenText Fortify
hoole@opentext.com
+1 (650) 427-9973

Peter Blay
Director del Equipo de Software Security Research
OpenText Fortify
pblay@opentext.com
+1 (669) 309-1634