Contenido de seguridad del software Fortify

Actualización 4 de 2023
viernes, 15 de diciembre de 2023

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 (SCA) y OpenText™ Fortify WebInspect. En la actualidad, el contenido de seguridad del software Fortify admite 1.657 categorías de vulnerabilidades en 33 lenguajes y abarca más de un millón de API distintas.

Copyright © 2023 Open Text. Todos los derechos reservados. Marcas propiedad de Open Text.

Fortify Software Security Research (SSR) se complace en anunciar la disponibilidad inmediata de actualizaciones para Fortify Secure Coding Rulepacks (en inglés, versión 2023.4.0), 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 1.432 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 Python (versión compatible: 3.12)

Python es un potente lenguaje de programación de uso general con tipos dinámicos y estructuras de datos eficientes de alto nivel. Admite múltiples paradigmas de programación, inclusive la programación estructurada, la orientada a objetos y la funcional. Esta versión aumenta nuestra cobertura hasta la última versión de Python expandiendo nuestra compatibilidad con los cambios en la API de la biblioteca estándar de Python. Se ha actualizado la cobertura de reglas existentes para los siguientes módulos:

- os
- pathlib
- tomllib

Soporte mejorado para Django (versión compatible: 4.2)

Django es un marco web escrito en Python que está 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 las versiones: 4.0, 4.1 y 4.2.

La cobertura mejorada incluye los siguientes espacios de nombres: *asyncio, django.core.cache.backends.base.BaseCache, django.db.models.Model,* y *django.middleware.security.SecurityMiddleware*. Además, hemos mejorado la cobertura de las categorías de vulnerabilidades, que incluye lo siguiente:

- Header Manipulation
- Insecure Cross-Origin Opener Policy
- Resource Injection
- Setting Manipulation

PyCryptodome y PyCrypto (versión compatible: 3.19.0)

PyCryptodome es un paquete de Python autónomo que proporciona una colección completa de algoritmos y protocolos criptográficos. Sirve como una versión extendida y mantenida más activamente de la biblioteca PyCrypto. PyCryptodome está diseñado para ofrecer una amplia gama de funcionalidades criptográficas, lo que lo convierte en una opción versátil para los desarrolladores que necesitan implementar comunicaciones seguras, protección de datos y operaciones criptográficas en sus aplicaciones Python.

La cobertura inicial de las categorías de vulnerabilidades incluye lo siguiente:

- Key Management: Empty Encryption Key
- Key Management: Empty PBE Password
- Key Management: Hardcoded Encryption Key
- Key Management: Hardcoded HMAC Key
- Key Management: Hardcoded PBE Password
- Key Management: Unencrypted Private Key
- Password Management: Hardcoded Password
- Password Management: Lack of Key Derivation Function
- Password Management: Password in Comment
- Weak Cryptographic Hash
- Weak Cryptographic Hash: Hardcoded PBE Salt
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Cryptographic Hash: Predictable Salt
- Weak Cryptographic Signature: Insufficient Key Size
- Weak Encryption
- Weak Encryption: Insecure Initialization Vector
- Weak Encryption: Insecure Mode of Operation
- Weak Encryption: Insufficient Key Size
- Weak Encryption: Stream Cipher
- Weak Encryption: User-Controlled Key Size

Detección de riesgos derivados de modelos de aprendizaje automático (ML) e inteligencia artificial (IA)

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. El soporte inicial de Fortify cubre proyectos de Python que consumen API OpenAI, Amazon Web Services (AWS), SageMaker o LangChain. El soporte detecta debilidades resultantes de la confianza implícita en las respuestas de las API del modelo AI/ML, además de las siguientes características únicas:

Soporte inicial para la API Python OpenAI (versión compatible: 1.3.8)

La biblioteca de Python de OpenAI permite a los desarrolladores acceder cómodamente a la API REST de OpenAI para interactuar con modelos OpenAI como GPT-4 y DALL-E. La API de OpenAI permite que una aplicación envíe solicitudes a los modelos de OpenAI y reciba las respuestas generadas, así como también ajustar los modelos existentes. El módulo Python de OpenAI admite la capacidad de enviar y recibir solicitudes asincrónicas y sincrónicas impulsadas por *httpx*. El soporte incluye la identificación de resultados potencialmente peligrosos del modelo, así como la siguiente categoría nueva:

- Cross-Site Scripting: AI

Soporte inicial para Python AWS SageMaker (Boto3) (versión compatible: 1.33.9)

AWS SageMaker es una oferta incluida en el amplio conjunto de servicios de Amazon AWS. AWS SageMaker proporciona un amplio conjunto de herramientas para respaldar una amplia variedad de proyectos de aprendizaje automático, desde el entrenamiento de modelos personalizados hasta la

configuración de canales de desarrollo completos compatibles con MLOps. El SDK de Amazon para Python (Boto3) permite la comunicación con una amplia variedad de ofertas de AWS, incluido AWS SageMaker. El soporte incluye la identificación de resultados potencialmente peligrosos del modelo, así como la siguiente categoría nueva:

- Cross-Site Scripting: AI

Soporte inicial para Python LangChain (versión compatible: 0.0.338)[1]

LangChain es un popular marco de orquestación de código abierto para el desarrollo de aplicaciones que utilizan modelos de lenguaje grandes (LLM). LangChain ofrece herramientas y API que facilitan la creación de aplicaciones basadas en LLM, como chatbots y agentes virtuales. Están disponibles como bibliotecas basadas en Python y JavaScript. El soporte incluye la identificación de resultados potencialmente peligrosos del modelo, la detección de *Path Manipulation*, así como la siguiente categoría nueva:

- Cross-Site Scripting: AI

Soporte de .NET 8 (versión compatible: 8.0.0)

Como sucesor de .NET 7, .NET 8 es un marco de desarrollo multiplataforma, gratuito y de código abierto que permite a los programadores escribir aplicaciones en diferentes lenguajes como C# y VB con un conjunto estandarizado de API. Esta versión aumenta nuestra cobertura a la última versión de .NET para mejorar la detección de vulnerabilidades en API nuevas y existentes.

La cobertura ampliada incluye los siguientes espacios de nombres:

- System.Collections.Frozen
- System.Net.Http.Json
- System
- System.Security
- System.Text
- System.Text.Unicode
- System.Net.Http

Java Simplified Encryption (Jasypt) (versión compatible: 1.9.3)

Java Simplified Encryption (Jasypt) es una pequeña biblioteca de Java que se utiliza para realizar cifrado basado en contraseñas, así como para crear resúmenes de contraseñas para almacenamiento. Tiene integración con marcos Java populares como Spring, Wicket e Hibernate.

La cobertura inicial de las categorías de vulnerabilidades incluye lo siguiente:

- Insecure Randomness
- Key Management: Empty PBE Password
- Key Management: Hardcoded PBE Password
- Key Management: Null PBE Password
- Password Management: Lack of Key Derivation Function
- Privacy Violation: Heap Inspection

[1] LangChain todavía es muy nuevo. Se debe evaluar cuidadosamente la seguridad antes del uso en producción.

- Setting Manipulation
- 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: User-Controlled PBE Salt
- Weak Encryption
- Weak Encryption: Insecure Mode of Operation

ECMAScript 2023

ECMAScript 2023, también conocido como ES2023 o ES14, es la última versión del ECMAScript estándar para el lenguaje JavaScript. Las características clave de ES2023 incluyen nuevas funciones de matriz que permiten cambiarlas copiando y buscando desde el final. La compatibilidad con ES2023 amplía la cobertura de todas las categorías de vulnerabilidad de JavaScript relevantes a la última versión del ECMAScript estándar.

Contaminación del prototipo

Contaminación del prototipo es una vulnerabilidad en aplicaciones JavaScript que permite a usuarios malintencionados eludir o afectar la lógica empresarial, además de ejecutar potencialmente su propio código.

Esta actualización de Rulepack detecta si un atacante puede contaminar el prototipo de un objeto en los siguientes paquetes NPM:

- assign-deep
- deap
- deep-extend
- defaults-deep
- dot-prop
- hoek
- lodash
- merge
- merge-deep
- merge-objects
- merge-options
- merge-recursive
- mixin-deep
- object-path
- pathval

Configuraciones de Kubernetes

Kubernetes es una solución de gestión de contenedores de código abierto para automatizar la implementación, el escalado y la gestión de aplicaciones en contenedores. Proporciona abstracciones de infraestructura centradas en contenedores que eliminan las dependencias de la infraestructura subyacente, lo que permite implementaciones portátiles y simplifica la gestión de sistemas distribuidos complejos. La cobertura mejorada de las categorías de vulnerabilidades incluye lo siguiente:

- Kubernetes Misconfiguration: Improper API Server Network Access Control
- Kubernetes Misconfiguration: Improper CronJob Access Control
- Kubernetes Misconfiguration: Improper DaemonSet Access Control
- Kubernetes Misconfiguration: Improper Deployment Access Control
- Kubernetes Misconfiguration: Improper Job Access Control
- Kubernetes Misconfiguration: Improper Pod Access Control
- Kubernetes Misconfiguration: Improper RBAC Access Control
- Kubernetes Misconfiguration: Improper ReplicaSet Access Control
- Kubernetes Misconfiguration: Improper Replication Controller Access Control
- Kubernetes Misconfiguration: Improper StatefulSet Access Control
- Kubernetes Misconfiguration: Insecure Secret Transport
- Kubernetes Misconfiguration: Insufficient Kubelet Logging
- Kubernetes Misconfiguration: Scheduler System Information Leak
- Kubernetes Misconfiguration: Uncontrolled Kubelet Resource Consumption
- Kubernetes Terraform Misconfiguration: Improper Daemon Set Access Control
- Kubernetes Terraform Misconfiguration: Improper Deployment Access Control
- Kubernetes Terraform Misconfiguration: Improper Job Access Control
- Kubernetes Terraform Misconfiguration: Improper Pod Access Control
- Kubernetes Terraform Misconfiguration: Improper Pod Network Access Control
- Kubernetes Terraform Misconfiguration: Improper RBAC Access Control
- Kubernetes Terraform Misconfiguration: Improper Replication Controller Access Control
- Kubernetes Terraform Misconfiguration: Improper Stateful Set Access Control
- Kubernetes Terraform Misconfiguration: Insecure Secret Transport

DISA STIG 5.3

Para ofrecer asistencia a nuestros clientes federales en lo que respecta al cumplimiento, se ha agregado una correlación de Fortify Taxonomy con la versión 5.3 de la STIG de seguridad y desarrollo de aplicaciones de la Agencia de sistemas de información de defensa (DISA) estadounidense.

OWASP Mobile Top 10 Risks 2023

Open Worldwide Application Security Project (OWASP) Mobile Top 10 Risks 2023 tiene como objetivo crear conciencia sobre los riesgos de seguridad móvil y educar a quienes participan en el desarrollo y mantenimiento de aplicaciones móviles. Para proporcionar soporte a los clientes que desean mitigar el riesgo de las aplicaciones web, se ha agregado a la versión inicial una correlación de Fortify Taxonomy con OWASP Mobile Top 10 2023.

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:

Obsolescencia de las versiones de Fortify Static Code Analyzer anteriores a 20.x

Como se anunció en la presentación del lanzamiento de 2023.3, esa fue la última versión de Rulepacks compatible con versiones de Static Code Analyzer anteriores a 20.x. En esta versión,

las versiones de Static Code Analyzer anteriores a 20.x no cargarán las instancias 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 últimas cuatro versiones principales de Static Code Analyzer.

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 Misconfiguration: Persistent Authentication* : falsos positivos eliminados en aplicaciones ASP.NET que utilizan servicios de autenticación de formularios
- *Credential Management: Hardcoded API Credentials:* falsos positivos eliminados del análisis secreto relacionado con tokens de portador HTTP
- *Credential Management: Hardcoded API Credentials* : nuevos problemas detectados para las claves API de Avature
- *Cross-Site Request Forgery* : nuevos problemas detectados en aplicaciones NodeJS que utilizan el marco JavaScript `Express.js`
- *Cross-Site Scripting* : nuevos problemas detectados en aplicaciones Go que utilizan el paquete `html/template`
- *Cross-Site Scripting: Reflected:* falsos positivos eliminados en aplicaciones ASP.NET que utilizan la clase `ListControl`
- *Denial of Service: Format String*: asignaciones incorrectas a las categorías de OWASP Top 10
- *Insecure Transport:* falsos positivos eliminados en aplicaciones ASP.NET relacionadas con métodos de controlador que manejan datos de usuarios privados
- *Insecure Transport: Mail Transmission:* falsos positivos eliminados de las aplicaciones Python que utilizan la clase `smtplib.SMTP`
- *Key Management: Hardcoded Encryption Key:* falsos positivos eliminados en aplicaciones Java que utilizan la clase `RSAKeyGenParameterSpec`
- *Link Injection: Missing Validation:* falsos positivos eliminados en aplicaciones Swift y Objective-C que utilizan el protocolo `WKNavigationDelegate`[2]
- *Mass Assignment: Insecure Binder Configuration:* falsos positivos eliminados de las aplicaciones Java que utilizan las API de Jakarta EE
- *Password Management: Password in Configuration File:* falsos positivos eliminados en los archivos de configuración
- *Path Manipulation* : nuevos problemas detectados en aplicaciones PHP con la carga de archivos
- *SQL Injection*: nuevos problemas detectados en aplicaciones NodeJS que utilizan la base de datos marsdb
- *SQL Injection: MyBatis Mapper*: nuevos problemas detectados en los archivos XML del mapeador MyBatis
- *String Termination Error*: falsos positivos eliminados en aplicaciones C/C++ que usan `printf()` y sus variantes
- *System Information Leak: Incomplete Servlet Error Handling:* falsos positivos eliminados en aplicaciones Java
- *Weak Encryption: Insecure Initialization Vector:* falsos positivos eliminados en aplicaciones Python que utilizan la biblioteca `Pycryptodome`
- *Unreleased Resource: Streams*: falsos negativos identificados en aplicaciones Java que utilizan las API `java.nio.file`
- Varios falsos positivos de flujo de datos en aplicaciones de Visualforce relacionados con la información del perfil del usuario

[2] Requiere Fortify Source Code Analyzer 23.1 o posterior

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 dos categorías:

Categoría eliminada	Categoría añadida
Azure ARM Misconfiguration: Insecure DataBricks Storage	Azure ARM Misconfiguration: Insecure Databricks Storage
Azure ARM Misconfiguration: Insecure Redis Enterprise Transport	Azure ARM Misconfiguration: Insecure Redis Transport

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

Access Control: Interfaz administrativa

Esta versión incluye una verificación para detectar una configuración insegura de Spring Cloud Gateway cuando el punto final del actuador de la puerta de enlace está habilitado, expuesto y no protegido. En este caso, los atacantes pueden crear nuevas rutas y obtener acceso a activos internos o confidenciales en nombre de la aplicación. Esto podría provocar el robo de claves de metadatos de la nube, la exposición de aplicaciones internas o ataques de denegación de servicio (DoS).

Expression Language Injection: Spring

Las versiones de Spring Cloud Gateway 3.1.0, de la 3.0.0 a la 3.0.6 y las anteriores a la 3.0.0 contienen una vulnerabilidad de seguridad identificada por CVE-2022-22947. Esta vulnerabilidad permite un ataque de inyección de código cuando el punto final del actuador de la puerta de enlace está habilitado, expuesto y no es seguro. Esta versión incluye una verificación para detectar si existe esta vulnerabilidad en el servidor de destino que usa las versiones de Spring Cloud Gateway afectadas.

Insecure Deployment: Unpatched Application

Las versiones 2023.05.3 y anteriores del servidor TeamCity On-Premises son propensas a una omisión de autenticación, lo que permite a un atacante no autenticado obtener la ejecución remota de código (RCE) en el servidor. Esta vulnerabilidad ha sido identificada por CVE-2023-42793. Esta versión incluye una comprobación que permite detectar esta vulnerabilidad en los servidores de destino.

Descubrimiento de información: API indocumentada

La documentación limitada o no documentada para los puntos finales de API puede proporcionar a los atacantes una superficie de ataque que no está suficientemente probada para detectar vulnerabilidades de seguridad. Un atacante podría realizar un reconocimiento para descubrir puntos finales obsoletos, sin parches y sin mantenimiento y obtener acceso a información confidencial o funcionalidad peligrosa. Esta versión incluye una verificación que tiene como objetivo descubrir puntos finales de API versionados a los que se puede acceder, pero que no están definidos en el documento de especificación de API.

Informes de cumplimiento

DISA STIG 5.3

Para ofrecer asistencia a las necesidades de nuestros clientes federales en lo que respecta al cumplimiento, esta versión contiene una correlación de las comprobaciones de WebInspect con la versión más reciente (5.3) de la STIG para la seguridad y el desarrollo de aplicaciones de la Agencia de sistemas de información de defensa estadounidense (DISA).

Actualizaciones de directivas

DISA STIG 5.3

Se incorporó una directiva personalizada a la lista de directivas admitidas en WebInspect SecureBase para incluir las comprobaciones pertinentes para DISA STIG 5.3.

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 Transport: Secuencia de renegociación SSLv3/TLS

TLS 1.3 no admite la renegociación. Esta versión incluye mejoras en la verificación de la inyección de la secuencia de renegociación para reducir los falsos positivos y mejorar la precisión de los resultados.

HTML5: Cross-Site Scripting Protection

El encabezado X-XSS-Protection está obsoleto en todos los navegadores modernos. En esta versión, hemos dejado de utilizar las comprobaciones de encabezados X-XSS-Protection faltantes o mal configuradas.

Fortify Premium Content

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

DISA STIG 5.3 y OWASP Mobile Top 10 2023

Para acompañar las nuevas correlaciones, esta versión también contiene un nuevo paquete de informes para OpenText™ Fortify Software Security Center compatible con DISA STIG 5.3 y OWASP Mobile Top 10 2023, que se puede descargar de Fortify Customer Support Portal, en la sección Premium Content.

Fortify Taxonomy: errores en la seguridad del software

El sitio de 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 de Fortify

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

© Copyright 2023 Open Text or one of its affiliates. The information contained herein is subject to change without notice. The only warranties for Open Text products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein.