Contenido de seguridad del software Fortify

Actualización 1 de 2024
29 de marzo 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 (SCA) y OpenText™ Fortify WebInspect. En la actualidad, el contenido de seguridad del software Fortify admite 1654 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 2024.1.0), 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 1429 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 Angular (versión compatible: 16.0.0)

Angular es un marco de desarrollo de aplicaciones web de código abierto, gratuito y basado en TypeScript que se especializa en la creación de SPA (aplicaciones de una sola página) y se utiliza principalmente en la interfaz para manipular datos de forma dinámica y eficiente. Se ha ampliado el soporte para Angular desde la versión 11.2.4 hasta Angular 16.0.0 (solo soporte inicial). Los resultados de Angular se han mejorado para que los clientes puedan esperar mejores resultados en categorías como *Cross-Site Request Forgery*, *Privacy Violation* y *System Information Leak*. Se ha ampliado la cobertura para el documento DOM de JavaScript, así como para los siguientes módulos:

- @angular/common/http
- @angular/core
- @angular/platform-browser

Soporte mejorado para PHP (versión compatible: 8.2)

PHP es un lenguaje de programación de uso general ampliamente utilizado que se utiliza con mayor frecuencia para el desarrollo web. La última versión de SSR actualiza el soporte para PHP hasta la versión 8.2. En particular, la versión incluye soporte inicial para las siguientes extensiones base PHP adicionales:

- Sodium (versión compatible: 8.3.1)

  La extensión PHP Sodium es una implementación de la biblioteca Libsodium. Sodium proporciona capacidades de cifrado, descifrado, firmas, hash de contraseñas y otras operaciones criptográficas. Los clientes pueden encontrar problemas adicionales relacionados con el cifrado y las firmas digitales, además de cambios en torno a problemas de Privacy Violation.

- Zip (versión compatible: 1.22.3)

  La extensión PHP Zip es una implementación de la biblioteca Linzip. Zip proporciona capacidad para la creación, modificación y lectura de archivos zip, una estructura común utilizada para realizar la agrupación y compresión de archivos/datos. El soporte inicial de la extensión incluye cobertura de la clase ZipArchive específica del flujo de datos del sistema de archivos básico y expansión de la cobertura de PHP para las siguientes categorías:

  - Key Management: Empty PBE Password
  - Path Manipulation: Zip Entry Overwrite

Soporte mejorado para Golang (versión compatible: 1.21)[1]

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. Go combina los beneficios de rendimiento de los lenguajes compilados con la facilidad de programación que se ve en los lenguajes interpretados. Su sintaxis concisa y su potente biblioteca estándar permiten a los desarrolladores escribir código sólido de forma rápida. Se amplía la cobertura para los siguientes paquetes:

- context
- crypto/ecdh
- html/template
- net
- reflect
- Runtime
- time

Infraestructura de la nube como código (IaC)[2]

Soporte ampliado para infraestructura como código en la nube. Infraestructura como código es el proceso de administrar y aprovisionar recursos informáticos a través de código en lugar de varios procesos manuales. Los problemas comunes relacionados con la configuración de los servicios mencionados ahora se notifican al desarrollador. A partir de Fortify Static Code Analyzer 24.2, los problemas de configuración de Azure ARM y AWS CloudFormation se informan mediante nuevas técnicas. Esto da como resultado una serie de problemas agregados y eliminados al fusionar FPR generados con versiones anteriores de Fortify Static Code Analyzer. Con Fortify Static Code Analyzer 24.2 y las versiones posteriores, se requieren los Rulepacks 2024.1 para evitar problemas de IaC duplicados.

Configuraciones de Azure Resource Manager (ARM)

ARM es el servicio de implementación y administración de Azure. ARM proporciona una capa de administración que le permite crear, actualizar y eliminar recursos en su cuenta de Azure.

Configuraciones de CloudFormation de Amazon Web Services (AWS)

CloudFormation es un servicio proporcionado por Amazon que se utiliza para automatizar el aprovisionamiento y la configuración de los recursos de AWS. CloudFormation permite a los usuarios administrar los recursos de AWS mediante una plantilla JSON o YAML. Al utilizar estas plantillas, los usuarios pueden crear, eliminar y modificar colecciones de recursos, denominadas pila, como una sola unidad. En esta versión, identificamos las siguientes categorías de vulnerabilidades adicionales para las configuraciones de AWS CloudFormation:

- AWS CloudFormation Misconfiguration: Insecure SageMaker Transport
- AWS CloudFormation Misconfiguration: SageMaker Network Isolation Disabled
- AWS CloudFormation Misconfiguration: Weak SecretsManager Generated Password

[1] Para obtener resultados óptimos, actualice a Fortify Static Code Analyzer 24.2 o posterior.
[2] Requiere la versión 24.2 o posterior de Fortify Static Code Analyzer.

Soporte Kotlin mejorado (versión compatible: 1.9.2)[3]

Kotlin es un lenguaje con un sistema de tipos estático de uso general que ofrece interoperabilidad con Java. Esta versión incluye soporte actualizado para las nuevas API de biblioteca estándar introducidas en las versiones 1.7.2, 1.8 y 1.9 de Kotlin dirigidas a los espacios de nombres de Kotlin: *jvm.optional*, *math*, *io.path*, *coroutines.cancellation* y *kotlinx.serialization.json*. Es posible que se detecten problemas adicionales en las categorías existentes, que incluyen:

- Denial of Service: Regular Expression
- Path Manipulation
- Privacy Violation
- System Information Leak

Mejoras en JavaScript/TypeScript Node.js[4]

Nuestras reglas de Node.js se han actualizado para beneficiarse de la resolución de tipos cuando se utiliza Fortify Static Code Analyzer 24.2. Los cambios dan como resultado una reducción de los falsos positivos, una mejora de los positivos reales y resultados más precisos en las aplicaciones Node.js en la mayoría de las categorías. Más específicamente, los clientes pueden esperar resultados mejorados relacionados con los siguientes módulos de Node.js:

- child_process
- dgram
- dns
- fs
- http
- https
- net
- querystring
- tls
- url
- util
- v8

También se incluye soporte parcial inicial para los siguientes paquetes de NPM:

- Bluebird
- child-process-promise

Soporte mejorado de DISA STIG 5.3

Para ofrecer asistencia a nuestros clientes federales en lo que respecta al cumplimiento, se ha actualizado 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 para incluir los siguientes 45 ID de STIG adicionales: APSC-DV-000010, APSC-DV-000210, APSC-DV-000230, APSC-DV-000240, APSC-DV-000330, APSC-DV-000380, APSC-DV-000390, APSC- DV-000400, APSC-DV-000410, APSC-DV-000430, APSC-DV-000450, APSC-DV-000580, APSC-DV-000590, APSC-DV-000710, APSC-DV-001120, APSC-DV-001130, APSC-DV-001280, APSC-DV-001290, APSC-DV-001300, APSC-DV-001310, APSC-DV-001320, APSC-DV-001330,

[3] La compatibilidad con Kotlin 1.9 requiere Fortify Static Code Analyzer 24.2 o posterior.

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

APSC-DV-001410, APSC-DV-001520, APSC-DV-001530, APSC-DV-001540, APSC-DV-001610, APSC-DV-001760, APSC-DV-001770, APSC-DV-001780, APSC-DV-001790, APSC-DV-001795, APSC-DV-001820, APSC-DV-001970, APSC-DV-002290, APSC-DV-002310, APSC-DV-002320, APSC-DV-002410, APSC-DV-002530, APSC-DV-002890, APSC-DV-002950, APSC-DV-002960, APSC-DV-003100, APSC-DV-003310 y APSC-DV-003320.

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:

- *Access Control: Anonymous LDAP Bind* – falsos positivos eliminados en aplicaciones C/C++.
- *Command Injection* – nuevos problemas detectados en aplicaciones C/C++ que utilizan la variante de Windows de las funciones de la biblioteca de tiempo de ejecución de C
- *Credential Management: Hardcoded API Credentials* – falsos positivos eliminados en archivos YAML
- *Dockerfile Misconfiguration: Dependency Confusion* – falsos positivos eliminados en Dockerfiles que involucran npm
- *Dynamic Code Evaluation: Code Injection* – nuevos problemas detectados en aplicaciones ASP.NET que usan las API de Azure Cosmos DB
- *GCP Terraform Misconfiguration: Insecure Supply Chain* – falsos positivos eliminados en los archivos de configuración de AWS Terraform
- *Insecure SSL: Server Identity Verification Disabled* – nuevos problemas detectados en aplicaciones Python que utilizan la biblioteca `Solicitudes`
- *Mass Assignment: Insecure Binder Configuration* – falsos positivos eliminados en aplicaciones ASP.NET MVC
- *Mass Assignment: Request Parameters Bound into Persisted Objects* – falsos positivos eliminados de las aplicaciones Spring
- *Password Management: Hardcoded Password* – nuevos problemas detectados en las cadenas de conexión ODBC
- *Poor Style: Identifier Contains Dollar Symbol ($)* – falsos positivos eliminados en aplicaciones Java
- *Privacy Violation* – nuevos problemas detectados en aplicaciones ASP.NET que utilizan Razor Pages
- *Privacy Violation* – nuevos problemas detectados en aplicaciones Dart/Flutter
- *Privacy Violation* – nuevos problemas detectados en aplicaciones JavaScript que utilizan el middleware `csurf` junto con la biblioteca ExpressJS
- *String Termination Error* – nuevos problemas detectados en aplicaciones C/C++
- *System Information Leak: External* – nuevos problemas detectados en aplicaciones ASP.NET que utilizan Razor Pages
- *System Information Leak: External* – nuevos problemas detectados en aplicaciones C/C++
- *Weak Encryption: Inadequate RSA Padding* – falsos positivos eliminados en aplicaciones PHP que usan OpenSSL
- Se eliminaron varios falsos positivos del flujo de datos en aplicaciones Python Django

- Se detectaron varios problemas nuevos de flujo de datos en aplicaciones Java Spring
- Varios problemas de flujo de datos que aparecen desde el punto de entrada main() en los análisis de Java se pueden mostrar como nuevos y eliminados. Esto también elimina duplicados y rastros incorrectos encontrados en aplicaciones Kotlin y Scala.

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 cuatro categorías:

Nombre de la categoría 2023 R4	Nombre de la categoría 2024 R1
Insecure Cross-Origin Opener Policy	HTML5: Insecure Cross-Origin Opener Policy
Insecure Transport: Client Identity Verification Disabled	Insecure SSL: verificación de la identidad del servidor deshabilitada
Kubernetes Terraform Misconfiguration: Improper Daemon Set Access Control	Kubernetes Terraform Misconfiguration: Improper DaemonSet Access Control
Kubernetes Terraform Misconfiguration: Improper Stateful Set Access Control	Kubernetes Terraform Misconfiguration: Improper StatefulSet Access Control

Desuso de la categoría "Header Checking Disabled"

La categoría se ha eliminado para evitar confusión con otras categorías con nombres similares. Las reglas anteriores en esta categoría ahora se informan en:

- ASP.NET Misconfiguration: Header Checking Disabled
- ASP.NET Misconfiguration: Unsafe Header Parsing

Desuso de ciertas categorías de "Dead Code"

Las siguientes categorías de "Dead Code" se han eliminado de los paquetes de reglas estándar:

- Dead Code: Empty Try Block
- Dead Code: Expression is Always false
- Dead Code: Expression is Always true
- Dead Code: Unused Field
- Dead Code: Unused Method
- Dead Code: Unused Parameter

Para los clientes que quieran seguir viendo estas vulnerabilidades detectadas, las reglas se pueden descargar desde el portal de soporte de Fortify en un paquete de reglas separado.

Cambio de nombre y obsolescencia de OWASP Mobile Top 10 2023

Tras el lanzamiento de los “OWASP Top 10 Mobile Risks – Initial Release 2023” en septiembre de 2023, el proyecto se finalizó y pasó a llamarse “OWASP Top 10 Mobile Risks – Final Release 2024”

en enero de 2024. Como resultado, esta versión incluye un mapeo adicional y renombrado para “OWASP Mobile Top 10 Risks 2024”. Las asignaciones en sí no tienen cambios funcionales.

En la próxima versión de Fortify Software Security Content, el mapeo OWASP Mobile Top 10 2023 quedará obsoleto y solo permanecerá el OWASP Mobile Top 10 2024 actualizado.

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

Insecure Deployment: Unpatched Application (CVE-2024-23897)

Jenkins es un servidor de automatización basado en Java que se utiliza para crear, probar e implementar software. La interfaz de línea de comandos (CLI) de Jenkins es una característica integrada de Jenkins que proporciona una forma de interactuar con el servidor Jenkins y está habilitada de forma predeterminada. Una vulnerabilidad crítica de lectura de archivos identificada por CVE-2024-23897 permite capacidades de lectura de archivos arbitrarias en Jenkins. Esta vulnerabilidad está presente en la biblioteca args4j que se utiliza para analizar los argumentos de los comandos y las opciones proporcionadas a la CLI. El analizador de comandos tiene una característica que reemplaza el carácter de arroba (@) seguido de una ruta de archivo en un argumento con el contenido del archivo especificado. Las versiones afectadas de Jenkins incluyen la 2.441 y anteriores y la LTS 2.426.2 y anteriores. Esta versión incluye una comprobación que permite detectar CVE-2024-23897 en un servidor de destino.

Insecure Deployment: Unpatched Application (CVE-2023-22515)

Atlassian Confluence Data Center y Confluence Server son soluciones autoadministradas conocidas por brindar a las organizaciones las mejores prácticas de colaboración. Una vulnerabilidad crítica de control de acceso interrumpido identificada por CVE-2023-22515 permite a actores malintencionados crear cuentas de administrador no autorizadas, lo que les otorga acceso sin restricciones a la plataforma Confluence. Incluso cuando los atacantes carecen de autenticación, pueden aprovechar CVE-2023-22515 para establecer cuentas de administrador no autorizadas y obtener acceso a instancias de Confluence. Los atacantes también pueden manipular la configuración de los servidores de Confluence para sugerir que el proceso de configuración no ha finalizado. Las versiones afectadas de Confluence Server y Confluence Data Center son 8.0.0- 8.0.4, 8.1.0-8.1.4, 8.2.0-8.2.3, 8.3.0-8.3.2, 8.4.0-8.4.2 y 8.5.0-8.5.1. Esta versión incluye una comprobación para detectar CVE-2023-22515 en un servidor de destino.

Insecure Deployment: Unpatched Application (CVE-2023-22518)

Una vulnerabilidad crítica de autorización inadecuada identificada por CVE-2023-22518 afecta a Atlassian Confluence Data Center y Confluence Server. Esta vulnerabilidad permite a un atacante no autenticado restablecer Confluence y crear una cuenta de administrador de instancia de

Confluence. Al utilizar esta cuenta, un atacante puede realizar todas las acciones administrativas que están disponibles para un administrador de instancia de Confluence, lo que provoca una pérdida total de confidencialidad, integridad y disponibilidad. Las versiones afectadas de Confluence Server y Confluence Data Center son todas las versiones anteriores a la 7.19.16 y las versiones 8.3.4, 8.4.4, 8.5.3 y 8.6.1. Esta versión incluye una comprobación que permite detectar CVE-2023-22518 en un servidor de destino.

OGNL Expression Injection: Double Evaluation (CVE-2023-22527)

Una vulnerabilidad crítica de OGNL Expression Injection identificada por CVE-2023-22527 afecta a Atlassian Confluence Server and Data Center. Esta vulnerabilidad permite que un atacante no autenticado ejecute código arbitrario en aplicaciones vulnerables. Las versiones afectadas de Confluence Data Center y Confluence Server son 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x y 8.5.0-8.5.3. Esta versión incluye una comprobación que permite detectar esta vulnerabilidad en los servidores de Atlassian afectados.

Informes de cumplimiento

DISA STIG 5.3 mejorado

Para ofrecer asistencia a nuestros clientes federales en lo que respecta al cumplimiento, se ha actualizado 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 para incluir los siguientes 8 ID de STIG adicionales: APSC-DV-000210, APSC-DV-000230, APSC-DV-000240, APSC-DV-000450, APSC-DV-001280, APSC-DV-001300, APSC-DV-002530 y APSC-DV-003320.

Actualizaciones de directivas

DISA STIG 5.3 mejorado

La política de DISA STIG 5.3 se actualiza para incluir controles adicionales relevantes 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:

Inyección de XPath

Esta versión incluye mejoras en la verificación de *XPath Injection* 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.

OWASP Mobile Top 10 2024

Para acompañar el cambio de nombre de las correlaciones de OWASP Mobile Top 10 Risks 2024, esta versión también contiene un nuevo paquete de informes para OpenText™ Fortify Software Security Center compatible con OWASP Mobile Top 10 2024 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