Contenido de seguridad del software Fortify

Actualización 2 de 2023
viernes, 30 de junio 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 Fortify Static Code Analyzer (SCA) y Fortify WebInspect. En la actualidad, el contenido de seguridad del software Fortify admite 1552 categorías de vulnerabilidades en 31 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 2023.2.0), 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 1329 categorías únicas de vulnerabilidades en más de 31 lenguajes y abarca más de un millón de API distintas. En resumen, esta versión incluye lo siguiente:

Soporte para Dart (versión compatible: 2.19.6)[1]

El kit de desarrollo de software (SDK) de Dart, desarrollado por Google, proporciona un lenguaje de programación con un potente sistema de tipos, basado en clases y recolectado de elementos no utilizados para crear aplicaciones de escritorio, móviles y web. Dart ofrece versatilidad al permitir que las aplicaciones se compilen en código de máquina específico de la arquitectura, módulos portátiles o JavaScript, según el caso de uso previsto. Con Dart, los desarrolladores pueden crear aplicaciones con interfaces gráficas de usuario (GUI) complementarias, lo que las convierte en una opción flexible para crear una amplia gama de soluciones de software. Entre las categorías compatibles se incluyen:

- Access Control: Database
- Command Injection
- Denial of Service
- Denial of Service: Regular Expression
- Header Manipulation
- Insecure Transport
- Open Redirect
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Path Manipulation
- Privacy Violation
- Resource Injection
- Server-Side Request Forgery
- SQL Injection
- System Information Leak
- System Information Leak: Internal

Soporte inicial para Flutter (versión compatible: 3.7.11)[1]

Flutter, un SDK de interfaz de usuario (UI) de código abierto creado por Google, aprovecha el poder del lenguaje de programación Dart. Proporciona a los desarrolladores un conjunto integral de herramientas, bibliotecas y paquetes para facilitar la creación de aplicaciones multiplataforma. Con Flutter, los desarrolladores pueden crear aplicaciones móviles, web y de escritorio a partir de una base de código única, lo que simplifica el proceso de desarrollo y reduce el tiempo y el esfuerzo. Al aprovechar las capacidades de Flutter, los desarrolladores pueden crear aplicaciones visualmente atractivas y de alto rendimiento que se ejecutan sin problemas en múltiples plataformas. El soporte para Flutter incluye

[1] Requiere Fortify Static Code Analyzer 23.1.0. Para obtener los mejores resultados, use Fortify Static Code Analyzer 23.1.1.

seguimiento de entradas suministradas por el usuario, detección de todas las categorías admitidas para el lenguaje de programación Dart y las siguientes categorías específicamente para las GUI de Flutter:

- Privacy Violation: Shoulder Surfing
- System Information Leak: Internal

Android 13 (nivel de API: 33)

La plataforma Android es una pila de software de código abierto diseñada para dispositivos móviles. Un componente principal de Android es Java API Framework, 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 Java API Framework de Android. En esta versión se introducen cinco nuevas categorías de vulnerabilidades para las aplicaciones de Android:

- Privacy Violation: Android Insecure Indexing
- Privilege Management: Android Nearby Devices
- Privilege Management: Android Notifications
- Privilege Management: Android Read Aural Media
- Privilege Management: Android Read Visual Media

Se incluyen actualizaciones adicionales de Android para ofrecer la compatibilidad con la detección de categorías de vulnerabilidades existentes en los siguientes espacios de nombres:

- android.app
- android.content
- android.net
- android.os
- android.util
- java.nio
- java.security
- java.security.interfaces

Java SE JDK (versión compatible: 17)

Java Platform, Standard Edition (SE) Java Development Kit (JDK) es un paquete de desarrollo de software que contiene herramientas y bibliotecas utilizadas para desarrollar aplicaciones y componentes Java. Esta versión incluye soporte actualizado de las categorías de vulnerabilidades existentes en los siguientes espacios de nombres para las nuevas API introducidas en Java SE JDK 15, 16 y 17:

- java.io
- java.lang
- java.lang.reflect
- java.net
- java.nio.channels
- java.util
- java.util.random
- java.util.stream

La cobertura de escaneo mejorada puede incluir problemas adicionales identificados en las siguientes categorías:

- Insecure Randomness
- Aleatoriedad insegura: Hardcoded Seed
- Aleatoriedad insegura: Propagación controlada por el usuario
- Server-Side Request Forgery
- Setting Manipulation
- Unsafe Reflection

Actualizaciones de la biblioteca estándar de Kotlin (versión compatible: 1.7.21)

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 1.6 y 1.7 de Kotlin dirigidas a la máquina virtual de Java (JVM).

Actualización del escaneo de secretos

El escaneo de secretos es una técnica para buscar automáticamente secretos en el código fuente y los archivos de configuración. En este contexto, "secretos" se refiere a contraseñas, tokens de API, claves de encriptación y artefactos similares destinados a mantenerse en secreto. Esta versión incluye soporte actualizado para el análisis de secretos en las siguientes categorías:

- Credential Management: Hardcoded API Credentials
- Key Management: Hardcoded Encryption Key
- Password Management: Hardcoded Password

Además, el análisis de secretos en los scripts de PowerShell ahora es compatible con las siguientes categorías:

- Password Management: Hardcoded Password
- Privacy Violation

Infraestructura de la nube como código (IaC)

Infraestructura como código es el proceso de administrar y aprovisionar recursos informáticos a través de código en lugar de varios procesos manuales. La cobertura ampliada de tecnologías compatibles incluye configuraciones de Terraform para la implementación en Amazon Web Services (AWS) y Google Cloud Platform (GCP), así como configuraciones para AWS CloudFormation. Los problemas comunes relacionados con la configuración de los servicios mencionados ahora se notifican al desarrollador.

Configuraciones de AWS Terraform

Terraform es una herramienta IaC de código abierto para construir, cambiar y versionar la infraestructura de la nube. Utiliza su propio lenguaje declarativo conocido como HashiCorp Configuration Language (HCL). La infraestructura de la nube está codificada en archivos de configuración para describir el estado deseado. Los proveedores de Terraform son compatibles con la configuración y administración de la infraestructura de AWS. En esta versión, identificamos las siguientes categorías adicionales para las configuraciones de Terraform:

- AWS Terraform Misconfiguration: Aurora Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: CloudWatch Missing Customer-Managed Encryption Key

- AWS Terraform Misconfiguration: Database Migration Service Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: DocumentDB Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: ElastiCache Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: Improper API Gateway Access Control
- AWS Terraform Misconfiguration: Improper EC2 Network Access Control
- AWS Terraform Misconfiguration: Improper ECR Access Control
- AWS Terraform Misconfiguration: Improper EKS Network Access Control
- AWS Terraform Misconfiguration: Improper ElastiCache Network Access Control
- AWS Terraform Misconfiguration: Improper Lambda Access Control
- AWS Terraform Misconfiguration: Improper MSK Network Access Control
- AWS Terraform Misconfiguration: Improper Neptune Access Control
- AWS Terraform Misconfiguration: Improper RDS Network Access Control
- AWS Terraform Misconfiguration: Improper S3 Access Control
- AWS Terraform Misconfiguration: Improper VPC Network Access Control
- AWS Terraform Misconfiguration: Insecure API Gateway Storage
- AWS Terraform Misconfiguration: Insecure API Gateway Transport
- AWS Terraform Misconfiguration: Insecure App Sync Storage
- AWS Terraform Misconfiguration: Insecure Athena Storage
- AWS Terraform Misconfiguration: Insecure CloudFront Transport
- AWS Terraform Misconfiguration: Insecure DynamoDB Storage
- AWS Terraform Misconfiguration: Insecure EC2 Storage
- AWS Terraform Misconfiguration: Insecure ECR Storage
- AWS Terraform Misconfiguration: Insecure ECS Transport
- AWS Terraform Misconfiguration: Insecure EKS Storage
- AWS Terraform Misconfiguration: Insecure ElastiCache Storage
- AWS Terraform Misconfiguration: Insecure Glue Storage
- AWS Terraform Misconfiguration: Insecure Kinesis Storage
- AWS Terraform Misconfiguration: Insecure MQ Storage
- AWS Terraform Misconfiguration: Insecure OpenSearch Service Storage
- AWS Terraform Misconfiguration: Insecure OpenSearch Service Transport
- AWS Terraform Misconfiguration: Insecure RDS Transport
- AWS Terraform Misconfiguration: Insecure S3 Storage
- AWS Terraform Misconfiguration: Insecure SageMaker Storage
- AWS Terraform Misconfiguration: Insufficient API Gateway Logging
- AWS Terraform Misconfiguration: Insufficient Aurora Backup
- AWS Terraform Misconfiguration: Insufficient CloudFront Logging
- AWS Terraform Misconfiguration: Insufficient CloudTrail Logging
- AWS Terraform Misconfiguration: Insufficient EC2 Logging
- AWS Terraform Misconfiguration: Insufficient ELB Logging
- AWS Terraform Misconfiguration: Insufficient ElastiCache Backup
- AWS Terraform Misconfiguration: Insufficient ElastiCache Logging
- AWS Terraform Misconfiguration: Insufficient Global Accelerator Logging
- AWS Terraform Misconfiguration: Insufficient GuardDuty Monitoring
- AWS Terraform Misconfiguration: Insufficient Lambda Logging
- AWS Terraform Misconfiguration: Insufficient OpenSearch Service Logging
- AWS Terraform Misconfiguration: Insufficient RDS Backup
- AWS Terraform Misconfiguration: Insufficient Redshift Logging
- AWS Terraform Misconfiguration: Insufficient S3 Backup
- AWS Terraform Misconfiguration: MemoryDB Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: MQ Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: Neptune Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: RDS Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: Reduced CloudFront Availability

- AWS Terraform Misconfiguration: Reduced ELB Availability
- AWS Terraform Misconfiguration: Reduced StackSets Availability
- AWS Terraform Misconfiguration: Weak Cognito Authentication
- AWS Terraform Misconfiguration: Weak IAM Password Policy

Configuraciones de Terraform de GCP

Terraform es una herramienta de código abierto de infraestructura como código para construir, cambiar y versionar la infraestructura de la nube. Utiliza su propio lenguaje declarativo conocido como HashiCorp Configuration Language (HCL). La infraestructura de la nube está codificada en archivos de configuración para describir el estado deseado. Los proveedores de Terraform son compatibles con la configuración y administración de la infraestructura de GCP. En esta versión, identificamos las siguientes categorías de vulnerabilidades para las configuraciones de GCP Terraform:

- GCP Terraform Misconfiguration: Insufficient Cloud Load Balancing Logging
- GCP Terraform Misconfiguration: Insufficient Cloud NAT Logging
- GCP Terraform Misconfiguration: Insufficient Media CDN Logging
- GCP Terraform Misconfiguration: Insufficient Operations Suite Logging

Configuraciones de AWS CloudFormation

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. En esta versión, identificamos las siguientes categorías de vulnerabilidades para las configuraciones de AWS CloudFormation:

- AWS CloudFormation Misconfiguration: AmazonMQ Publicly Accessible
- AWS CloudFormation Misconfiguration: Backup Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: CloudTrail Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DataBrew Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DMS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DMS Publicly Accessible
- AWS CloudFormation Misconfiguration: DocDB Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DocDBElastic Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DynamoDB Backup Disabled
- AWS CloudFormation Misconfiguration: EC2 Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: ECR Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: EFS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: ElastiCache Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: FinSpace Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: FSx Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: ImageBuilder Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Improper Athena Access Control
- AWS CloudFormation Misconfiguration: Improper CodeStar Access Control
- AWS CloudFormation Misconfiguration: Improper Cognito Access Control
- AWS CloudFormation Misconfiguration: Improper ECS Network Access Control
- AWS CloudFormation Misconfiguration: Improper EMR Access Control
- AWS CloudFormation Misconfiguration: Improper KMS Access Control
- AWS CloudFormation Misconfiguration: Improper Lambda Network Access Control
- AWS CloudFormation Misconfiguration: Improper Lightsail Access Control
- AWS CloudFormation Misconfiguration: Improper M2 Access Control

- AWS CloudFormation Misconfiguration: Improper QLDB Access Control
- AWS CloudFormation Misconfiguration: Improper RDS Access Control
- AWS CloudFormation Misconfiguration: Improper Redshift Access Control
- AWS CloudFormation Misconfiguration: Improper S3 Access Control
- AWS CloudFormation Misconfiguration: Improper SageMaker Access Control
- AWS CloudFormation Misconfiguration: Improper SageMaker Network Access Control
- AWS CloudFormation Misconfiguration: Improper Serverless Network Access Control
- AWS CloudFormation Misconfiguration: Improper Transfer Network Access Control
- AWS CloudFormation Misconfiguration: Insecure API Gateway Transport
- AWS CloudFormation Misconfiguration: Insecure CloudFront Transport
- AWS CloudFormation Misconfiguration: Insecure DAX Storage
- AWS CloudFormation Misconfiguration: Insecure ECR Supply Chain
- AWS CloudFormation Misconfiguration: Insecure EFS Storage
- AWS CloudFormation Misconfiguration: Insecure ELB Transport
- AWS CloudFormation Misconfiguration: Insecure Elasticsearch Storage
- AWS CloudFormation Misconfiguration: Insecure Elasticsearch Transport
- AWS CloudFormation Misconfiguration: Insecure WorkSpaces Storage
- AWS CloudFormation Misconfiguration: Insufficient API Gateway Logging
- AWS CloudFormation Misconfiguration: Insufficient AppSync Logging
- AWS CloudFormation Misconfiguration: Insufficient CloudFront Logging
- AWS CloudFormation Misconfiguration: Insufficient CloudFront Monitoring
- AWS CloudFormation Misconfiguration: Insufficient CloudTrail Monitoring
- AWS CloudFormation Misconfiguration: Insufficient Config Monitoring
- AWS CloudFormation Misconfiguration: Insufficient ECR Monitoring
- AWS CloudFormation Misconfiguration: Insufficient ELB Logging
- AWS CloudFormation Misconfiguration: Insufficient ElasticLoadBalancing Logging
- AWS CloudFormation Misconfiguration: Insufficient Elasticsearch Logging
- AWS CloudFormation Misconfiguration: Insufficient GuardDuty Monitoring
- AWS CloudFormation Misconfiguration: Insufficient Lambda Logging
- AWS CloudFormation Misconfiguration: Insufficient MQ Logging
- AWS CloudFormation Misconfiguration: Insufficient MSK Logging
- AWS CloudFormation Misconfiguration: Insufficient OpenSearch Service Logging
- AWS CloudFormation Misconfiguration: Insufficient RDS Monitoring
- AWS CloudFormation Misconfiguration: Insufficient Route 53 Logging
- AWS CloudFormation Misconfiguration: Insufficient Serverless Logging
- AWS CloudFormation Misconfiguration: Insufficient Stack Monitoring
- AWS CloudFormation Misconfiguration: Kinesis Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Lambda Denial of Service
- AWS CloudFormation Misconfiguration: Location Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Logs Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: M2 Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: MemoryDB Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Neptune Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Privileged Batch Container
- AWS CloudFormation Misconfiguration: RDS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: RDS Publicly Accessible
- AWS CloudFormation Misconfiguration: Redshift Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Reduced EC2 Availability
- AWS CloudFormation Misconfiguration: Reduced ElastiCache Availability

- AWS CloudFormation Misconfiguration: Reduced Stack Availability
- AWS CloudFormation Misconfiguration: Rekognition Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: S3 Backup Disabled
- AWS CloudFormation Misconfiguration: SQS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: SageMaker Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Serverless Denial of Service
- AWS CloudFormation Misconfiguration: Timestream Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Weak API Gateway Authentication
- AWS CloudFormation Misconfiguration: Weak Certificate Manager Authentication
- AWS CloudFormation Misconfiguration: Weak IAM Authentication
- AWS CloudFormation Misconfiguration: Weak Lambda Authentication
- AWS CloudFormation Misconfiguration: Weak RDS Authentication

Actualización de expresiones regulares de gestión de contraseñas personalizable
Las expresiones regulares personalizables de administración de contraseñas para los scripts de Salesforce Apex, Dart y PowerShell ahora se pueden especificar mediante las siguientes propiedades:

- com.fortify.sca.rules.password_regex.apex
- com.fortify.sca.rules.password_regex.dart
- com.fortify.sca.rules.password_regex.powershell

Estas propiedades se pueden usar para anular las expresiones regulares predeterminadas que se usan para identificar contraseñas al escanear el código fuente de Salesforce Apex, el código fuente de Dart o los scripts de PowerShell.

OWASP Mobile Application Security Verification Standard (MASVS) v2.0.0

El estándar OWASP MASVS v2.0.0 se lanzó en abril de 2023 como parte del proyecto OWASP Mobile Application Security (MAS). Ofrece una línea de base para los requisitos de seguridad de las aplicaciones móviles y está diseñado para ser utilizado por arquitectos, desarrolladores y probadores de software móvil. OWASP MASVS 2.0 está destinado a centrarse en la seguridad de la aplicación de la aplicación móvil "cliente" que se ejecuta en el dispositivo móvil. Como tal, debe usarse en combinación con OWASP ASVS para evaluar los riesgos de seguridad de la aplicación del lado del servidor relacionados con los controles para puntos finales remotos. Para apoyar a nuestros clientes en el desarrollo de aplicaciones móviles seguras y la evaluación de aplicaciones móviles para la cobertura de control de seguridad y la mitigación de riesgos, se ha agregado una correlación de Fortify Taxonomy con OWASP MASVS v2.0.0.

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 la categoría "Access Control"

La categoría *Access Control* para Salesforce Apex se eliminó en esta versión. La falta de controles de seguridad a nivel de campo ahora se registra indirectamente a través de otras categorías, como *Access Control: Database* y *SOQL Injection*.

Obsolescencia de la categoría "Link Injection: Auto Dial"

La categoría *Link Injection: Auto Dial* se ha eliminado debido a que está desactualizada. La categoría se introdujo para abordar CVE-2017-2484, donde los atacantes pueden explotar la entrada de usuario no desinfectada en las aplicaciones de iOS para marcar automáticamente números de teléfono o llamadas de Facetime. Este exploit se solucionó en la actualización de iOS 10.3, por lo tanto, ya no es relevante para las aplicaciones de iOS actuales.

Asignaciones de estándares en desuso

Los siguientes estándares y mejores prácticas se han marcado como obsoletos, por lo que no se mostrarán de forma predeterminada:

- CWE Top 25 2019
- CWE Top 25 2020
- DISA STIG 4.9
- DISA STIG 4.10
- OWASP Top 10 2004
- OWASP Top 10 2007
- OWASP Top 10 2010
- SANS Top 25 2009
- SANS Top 25 2010
- WASC 24 + 2

Funciones dinámicas de PHP[2]

El último Fortify Static Code Analyzer incluye compatibilidad actualizada con PHP, lo que permite generar informes de problemas de *Dynamic Code Evaluation: Code Injection* con funciones dinámicas a las que hace referencia una entrada externa sin desinfectar.

Clase no segura de Java

Dentro de Java JDK hay una clase oculta para realizar acciones intrínsecamente inseguras que normalmente no están disponibles para los desarrolladores y que requiere reflexión para crear instancias. Ahora, al usar la clase `sun.misc.Unsafe` dentro de proyectos Java, los resultados del análisis informarán de cualquier uso, como *Often Misused: sun.misc.Unsafe.*

[2] Requiere SCA 23.1 y superior

Mejoras en falsos positivos

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

- *Access Control: Unenforced Sharing Rules* : se eliminaron los falsos positivos en activadores de Salesforce, páginas de Visualforce y componentes
- *Command Injection* : se eliminaron los falsos positivos al marcar expresiones regulares en JavaScript
- *Cookie Security: Cookie not Sent Over SSL* : se eliminaron los falsos positivos en Swift cuando se aplica la corrección recomendada
- *Credential Management: Hardcoded API Credentials* : se eliminaron los falsos positivos al identificar tokens de portador
- *Dead Code: Expression is Always false* : se eliminaron los falsos positivos cuando aparecían en instrucciones switch de Java
- *Dockerfile Misconfiguration: Dependency Confusion* : se eliminaron los falsos positivos en los comandos "apt" y "apt-get" dentro de los dockerfiles
- *Log Forging (debug)* : se eliminaron los falsos positivos en aplicaciones de Salesforce Apex al imprimir valores de encabezado de solicitud HTTP
- *Race Condition: Signal Handling* : se eliminaron los falsos positivos en C/C++ al invocar `sigaction()`
- *String Termination Error* : se eliminaron los falsos positivos al activar tipos primitivos en C++
- *Unused Method* : se eliminaron los falsos positivos en código Java donde el método es llamado por un método serializable implementado
- Se eliminaron los falsos positivos de flujo de datos en JavaScript que podrían haberse activado en valores booleanos

Cambios 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 darán como resultado categorías añadidas o eliminadas.

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

- *Azure Terraform Misconfiguration: Improper CosmosDB CORS Policy* ahora informa como *Azure Terraform Misconfiguration: Improper Cosmos DB CORS Policy*
- *Kubernetes Misconfiguration: Missing ServiceAccount Admission Controller* ahora informa como *Kubernetes Misconfiguration: Missing Service Account Admission Controller*
- *NoSQL Injection: CosmosDB* ahora informa como *NoSQL Injection: Cosmos DB*

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: Unpatched Application:

ZK Framework, una biblioteca Java de código abierto utilizada para crear aplicaciones móviles y web empresariales, contiene una vulnerabilidad de seguridad identificada por CVE-2022-36537. Los atacantes pueden aprovechar esta vulnerabilidad para recuperar el contenido de un archivo ubicado en el contexto web. La explotación exitosa permite a un atacante obtener información confidencial o apuntar a un punto final que de otro modo sería inalcanzable. Esta versión incluye una verificación para detectar esta vulnerabilidad en servidores de destino que usan las versiones de ZK Framework 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 lo siguiente:

Command Injection:

Las comprobaciones identificadas por ID 11722 y 11723 se añadieron para usar cargas útiles que admitan la función de pruebas de seguridad de aplicaciones fuera de banda (OAST)[3]. Reducen los falsos positivos y aumentan la precisión de los resultados del análisis de WebInspect.

Fortify Premium Content

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

OWASP MASVS v2.0.0

Para acompañar las nuevas correlaciones, esta versión también contiene un nuevo paquete de informes para Fortify Software Security Center compatible con OWASP MASVS v2.0.0 que se puede descargar de Fortify Customer Support Portal, en la sección Premium Content.

[3] Debido a que la verificación 11723 envía una cantidad significativa de solicitudes, se excluye de la política estándar. Utilice la política Todas las comprobaciones, personalice una política existente para incluir la comprobación o cree una política personalizada para ejecutar esta comprobación.

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.
Ahora hay disponible una nueva versión fuera de la nube del sitio de Fortify Taxonomy, consistente con el sitio en vivo anterior, para que los clientes la descarguen desde el portal de soporte de Fortify.

Comuníquese con el soporte técnico 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