Anuncio de publicación de Software Security Research

Contenido de Fortify Software Security

Actualización 4 de 2021

17 de diciembre de 2021

Acerca de CyberRes Fortify Software Security Research

Fortify Software Security Research transforma la investigación más avanzada en inteligencia de seguridad que impulsa la cartera de productos de Fortify, incluidos Fortify Static Code Analyzer (SCA), Fortify WebInspect y Fortify Application Defender. Actualmente, el contenido de CyberRes Fortify Software Security admite 1137 categorías de vulnerabilidad en 29 lenguajes de programación 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 2021.4.0), Fortify WebInspect SecureBase (disponible mediante SmartUpdate) y Fortify Premium Content.

CyberRes Fortify Secure Coding Rulepacks [SCA]

Con esta versión, Fortify Secure Coding Rulepacks detecta 917 categorías únicas de vulnerabilidades en 29 lenguajes de programación y abarca más de un millón de API distintas. En resumen, esta versión incluye lo siguiente:

Actualizaciones de .NET Core y ASP.NET (versión compatible: .NET Core 3.1)

Compatibilidad mejorada con diversos espacios de nombres de .NET Core y ASP.NET, entre los que se incluyen los siguientes:

- Microsoft.AspNetCore.Http
- Microsoft.AspNetCore.Mvc
- Microsoft.Extensions.Logging
- System
- System.IO
- System.Net
- System.Threading

La compatibilidad mejora la cobertura de las siguientes categorías:

- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Log Forging
- Log Forging (debug)
- Privacy Violation
- System Information Leak

Azure

Azure es la plataforma de computación pública en la nube de Microsoft que ofrece una serie de servicios en la nube, entre los que se incluyen computación, contenedores, Internet de las cosas, IA y aprendizaje automático.

En esta versión, ofrecemos compatibilidad inicial con un gran número de servicios clave de Azure: Functions, Identity y CosmosDB. A su vez, las siguientes tecnologías específicas de Azure ya son compatibles:

Azure Functions (versiones compatibles: Java 1.3.1, C# 3.x)

Fuctions es la solución computacional sin servidor de Microsoft Azure. Azure Functions proporciona una infraestructura continuamente actualizada para ejecutar su aplicación, construir API web, responder a cambios en las bases de datos y gestionar colas de mensajes. Esta actualización incluye compatibilidad inicial con los siguientes tipos de desencadenadores de C# y Java:

- Blob Trigger
- CosmosDB Trigger
- Event Trigger
- Http Trigger (as class library)
- Http Trigger (as C# isolated process)
- Queue Trigger
- ServiceBus Trigger

La compatibilidad de Azure Functions incluye las siguientes categorías:

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set
- Cookie Security: Overly Broad Path
- Cookie Security: Overly Broad Domain
- Cookie Security: Persistent Cookie
- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Denial Of Service
- Header Manipulation
- Header Manipulation: Cookies
- HTML5: Overly Permissive CORS Policy
- Privacy Violation
- Resource Injection
- Setting Manipulation
- System Information Leak: External

Azure Identity (versiones compatibles: C# 1.5.0, Java 1.4.1)

Azure Identity es el servicio de gestión de identidades y accesos basado en la nube de Microsoft. Proporciona autenticación y autorización a los recursos dentro de una organización. Esta actualización incluye compatibilidad inicial con los siguientes espacios de nombres:

C#

- Azure.Identity (version 1.5.0)

Java

- com.azure.identity (version 1.4.1)

La compatibilidad de Azure Identity incluye las siguientes categorías:

- Password Management
- Password Management: Empty/Hardcoded/Null Password
- Password Management: Weak Cryptography
- Resource Injection

Azure CosmosDB (versión compatible: 3.x)

Azure Cosmos DB es un servicio de base de datos multimodelo distribuido globalmente. Gracias a Azure Cosmos DB, puede almacenar y acceder a bases de datos de documentos, de valores clave, de columnas anchas y de gráficos mediante el uso de API y modelos de programación. Esta actualización incluye compatibilidad inicial con los siguientes espacios de nombres para C#:

- Microsoft.Azure.Cosmos
- Microsoft.Azure.Cosmos.Scripts
- Microsoft.Azure.Cosmos.Table

La compatibilidad de Azure Cosmos DB incluye las siguientes categorías:

- Denial of Service

- HTML5: Overly Permissive CORS Policy
- Insecure Transport
- NoSQL Injection: CosmosDB
- Resource Injection
- Setting Manipulation
- SQL Injection

AWS

Amazon Web Services (AWS) es una plataforma de computación pública en la nube que ofrece una serie de servicios en la nube, entre los que se incluyen computación, almacenamiento, redes, bases de datos, Internet de las cosas y aprendizaje automático.

En esta versión, ofrecemos compatibilidad inicial con un gran número de servicios clave de AWS: IAM, DynamoDB y RDS. Esta versión también añade compatibilidad inicial de Lambda con C# y compatibilidad actualizada con Java. A su vez, las siguientes tecnologías concretas de AWS ya son compatibles:

Actualizaciones de AWS Lambda (versiones compatibles: .NET AWS SDK 3.7.x, Java AWS SDK v2 2.17.x) [1]

Lambda es un servicio de computación, proporcionado por Amazon como parte de Amazon Web Services (AWS), que ejecuta códigos sin aprovisionar ni gestionar servidores. El servicio Lambda ejecuta códigos en respuesta a eventos y gestiona automáticamente los recursos informáticos requeridos por el código. Esta actualización incluye compatibilidad inicial con C# y compatibilidad adicional con Java. Esta actualización incluye compatibilidad con los siguientes espacios de nombres de C# y Java:

C#

- Amazon.Lambda
- Amazon.Lambda.APIGatewayEvents
- Amazon.Lambda.Core

Java

- com.amazonaws.services.lambda.runtime
- com.amazonaws.services.lambda.runtime.events

Esta actualización incluye compatibilidad adicional con los siguientes tipos de eventos:

- API Gateway Events (C#, Java)
- DynamoDB (Java)
- S3 Events (Java)
- Scheduled Events (Java)

La compatibilidad de AWS Lambda incluye las siguientes categorías:

[1] Para mejorar los análisis, incluya las plantillas YAML/JSON de AWS SAM o CloudFormation en la traducción.

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Header Manipulation
- Header Manipulation: Cookies
- Log Forging
- Privacy Violation
- System Information Leak: External
- System Information Leak: Internal

AWS IAM (versiones compatibles: .NET AWS SDK 3.7.x, Java AWS SDK v2 2.17.x)

AWS Identity and Access Management (IAM) es un servicio web que controla el acceso a los recursos de AWS. IAM puede utilizarse para controlar el uso autenticado y autorizado de los recursos de AWS. Esta actualización incluye compatibilidad con C# y Java. Esta actualización incluye compatibilidad con los siguientes espacios de nombres de C# y Java:

C#

- Amazon.IdentityManagement.Model

Java

- com.amazonaws.services.identitymanagement.model
- software.amazon.awssdk.services.iam.model

Además de identificar información confidencial, la compatibilidad de AWS IAM incluye las siguientes categorías:

- Password Management
- Password Management: Empty/Hardcoded/Null Password
- Password Management: Weak Cryptography

AWS DynamoDB (versiones compatibles: .NET AWS SDK 3.7.x, Java AWS SDK v2 2.17.x)

AWS DynamoDB es un servicio de bases de datos NoSQL totalmente administrado que admite estructuras de datos de valor clave y documentos. DynamoDB puede utilizarse para almacenar y recuperar datos y servir cantidades arbitrarias de tráfico de solicitudes. Esta actualización incluye compatibilidad inicial con C# y compatibilidad actualizada con Java. La compatibilidad incluye los siguientes espacios de nombres:

C#

- Amazon.DynamoDBv2.Model
- Amazon.DynamoDBv2.DataModel
- Amazon.DynamoDBv2.DocumentModel

Java

- com.amazonaws.services.lambda.runtime.events.models.dynamodb
- software.amazon.awssdk.enhanced.dynamodb
- software.amazon.awssdk.enhanced.dynamodb.model

La compatibilidad de AWS DynamoDB incluye las siguientes categorías:

- Access Control: Database

- NoSQL Injection: DynamoDB
- SQL Injection: PartiQL

API de datos de AWS Relational Database Service (RDS) para Aurora Serverless (versiones compatibles: .NET AWS SDK 3.7.x, Java AWS SDK v2 2.17.x)

Amazon Aurora es un motor de base de datos relacional compatible con MySQL y PostgreSQL que forma parte del servicio gestionado Amazon Relational Database Service (Amazon RDS). La API de datos de AWS RDS proporciona una interfaz de servicio web que permite a las aplicaciones acceder a sentencias SQL y ejecutarlas contra un clúster de bases de datos de Aurora Serverless. Esta actualización incluye compatibilidad con los siguientes espacios de nombres de C# y Java:

C#

- Amazon.RDSDataService.Model

Java

- software.amazon.awssdk.services.rdsdata.model (V2)

La compatibilidad de AWS RDS incluye las siguientes categorías:

- Access Control: Database
- Setting Manipulation
- SQL Injection

Secret Scanning

Compatibilidad con Secret Scanning. Secret Scanning es una técnica de búsqueda automática de secretos en archivos de texto. En este contexto, los "secretos" hacen referencia a contraseñas, tokens de API, claves de cifrado y elementos similares destinados a no ser revelados. El objetivo principal es encontrar secretos accidentalmente codificados en el código fuente y los archivos de configuración. Compatibilidad ampliada con todos los lenguajes y tipos de archivos adicionales mediante el nuevo análisis Regex[2]. Entre las categorías compatibles se incluyen:

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

Trojan Source

Trojan Source[3] es una categoría de vulnerabilidades publicada por Nick Boucher y Ross Anderson en su artículo *Trojan Source: Invisible Vulnerabilities*. Demuestran cinco formas distintas de utilizar los caracteres especiales Unicode para hacer que el código se muestre de una manera a simple vista para un desarrollador y funcione de una manera diferente cuando se ejecuta. Trojan Source debe considerarse un escenario de amenaza interna, puesto que un individuo malintencionado puede insertar a propósito los caracteres Unicode. Debido a la precisión de una de las categorías, incluimos compatibilidad de detección en el núcleo de Rulepacks para los siguientes lenguajes: C, C++, C#, Go, Java, JavaScript, Python y Rust. Las categorías compatibles incluyen:

[2] Se necesita Fortify Static Code Analyzer v21.2.0 o posterior.
[3] Se necesita Fortify Static Code Analyzer v21.2.0 o posterior.

- Encoding Confusion: BiDi Control Characters

Correlación de problemas estáticos/dinámicos[4]

Compatibilidad con la exportación de datos para permitir la correlación de los resultados de los análisis estáticos y dinámicos en Fortify Software Security Center (SSC) para proyectos de Java Spring. Entre las categorías compatibles se incluyen:

- Cross-Site Scripting: Content Sniffing
- Cross-Site Scripting: Inter Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- SQL Injection
- SQL Injection: Hibernate

Compatibilidad ampliada con COBOL de IBM Mainframe (versión compatible: 6.3)

Esta actualización incluye la detección de vulnerabilidades de desbordamiento de enteros en el código COBOL de IBM Mainframe.

Infraestructura como código en la nube

Compatibilidad con infraestructura como código (IaC, por sus siglas en inglés) en la nube. IaC es el proceso de gestión y aprovisionamiento de recursos informáticos mediante código, en lugar de emplear varios procesos manuales. Las tecnologías compatibles incluyen AWS, AWS CloudFormation, Azure ARM, Kubernetes K8S y Azure Kubernetes Service. Los problemas más comunes relacionados con la configuración de los servicios mencionados se comunican ahora al desarrollador. Entre estos servicios se incluyen:

- Access Control: Azure Blob Storage
- Access Control: Azure Container Registry
- Access Control: Azure Network Group
- Access Control: Azure SQL Database
- Access Control: Azure Storage
- Access Control: Cosmos DB
- Access Control: EC2
- Access Control: Kubernetes Admission Controller
- Access Control: Kubernetes Image Authorization Bypass
- Access Control: Overly Broad IAM Principal
- Access Control: Overly Permissive S3 Policy
- AKS Bad Practices: Missing Azure Monitor Integration
- Ansible Bad Practices: Missing CloudWatch Integration

[4] Se necesita Fortify Static Code Analyzer v21.2.0 o posterior. Permitir que la salida de correlación pase la propiedad 'com.fortify.sca.rules.enable_wi_correlation' a tiempo de escaneo. Esto se puede hacer con argumentos en la línea de comandos o modificando los archivos de propiedades de SCA.

- Ansible Bad Practices: Redshift Publicly Accessible
- Ansible Misconfiguration: Log Validation Disabled
- AWS CloudFormation Bad Practices: Missing CloudWatch Integration
- AWS CloudFormation Bad Practices: Redshift Publicly Accessible
- AWS CloudFormation Bad Practices: User-Bound IAM Policy
- AWS CloudFormation Misconfiguration: API Gateway Unauthenticated Access
- AWS CloudFormation Misconfiguration: Insecure Transport
- AWS CloudFormation Misconfiguration: Insufficient CloudTrail Logging
- AWS CloudFormation Misconfiguration: Insufficient DocumentDB Logging
- AWS CloudFormation Misconfiguration: Insufficient Neptune Logging
- AWS CloudFormation Misconfiguration: Insufficient RedShift Logging
- AWS CloudFormation Misconfiguration: Insufficient S3 Logging
- AWS CloudFormation Misconfiguration: Log Validation Disabled
- AWS CloudFormation Misconfiguration: root User Access Key
- AWS CloudFormation Misconfiguration: Unrestricted Lambda Principal
- Azure Monitor Misconfiguration: Insufficient Logging
- Azure Resource Manager Bad Practices: Cross-Tenant Replication
- Azure Resource Manager Bad Practices: Remote Debugging Enabled
- Azure Resource Manager Bad Practices: SSH Password Authentication
- Azure Resource Manager Misconfiguration: Insecure Transport
- Azure Resource Manager Misconfiguration: Overly Permissive CORS Policy
- Azure Resource Manager Misconfiguration: Security Alert Disabled
- Azure SQL Database Misconfiguration: Insufficient Logging
- Insecure SSL: Inadequate Certificate Verification
- Insecure Storage: Missing DocumentDB Encryption
- Insecure Storage: Missing EBS Encryption
- Insecure Storage: Missing Elasticache Encryption
- Insecure Storage: Missing Neptune Encryption
- Insecure Storage: Missing RDS Encryption
- Insecure Storage: Missing Redshift Encryption
- Insecure Storage: Missing S3 Encryption
- Insecure Storage: Missing SNS Topic Encryption
- Insecure Transport: Azure Storage
- Insecure Transport: Database
- Insecure Transport: Missing Elasticache Encryption
- Key Management: Excessive Expiration
- Kubernetes Bad Practices: API Server Publicly Accessible
- Kubernetes Bad Practices: Default Namespace
- Kubernetes Bad Practices: Host Write Access
- Kubernetes Bad Practices: Missing API Server Authorization
- Kubernetes Bad Practices: Missing Kubelet Authorization
- Kubernetes Bad Practices: Missing Node Authorization
- Kubernetes Bad Practices: Missing RBAC Authorization
- Kubernetes Bad Practices: NamespaceLifecycle Enforcement Disabled
- Kubernetes Bad Practices: readOnlyPort Enabled
- Kubernetes Bad Practices: Static Authentication Token

- Kubernetes Bad Practices: Unconfigured API Server Logging
- Kubernetes Misconfiguration: API Server Anonymous Access
- Kubernetes Misconfiguration: API Server Logging Disabled
- Kubernetes Misconfiguration: HTTP Basic Authentication
- Kubernetes Misconfiguration: Insecure Transport
- Kubernetes Misconfiguration: Kubelet Anonymous Access
- Kubernetes Misconfiguration: Missing Garbage Collection Threshold
- Kubernetes Misconfiguration: Missing Kubelet Client Certificate
- Kubernetes Misconfiguration: Overly Permissive Capabilities
- Kubernetes Misconfiguration: Privileged Container
- Kubernetes Misconfiguration: Server Identity Verification Disabled
- Kubernetes Misconfiguration: Unbound Controller Manager
- Kubernetes Misconfiguration: Unbound Scheduler
- Poor Logging Practice: Excessive Cloud Log Retention
- Poor Logging Practice: Insufficient Cloud Log Retention
- Poor Logging Practice: Insufficient Cloud Log Rotation
- Poor Logging Practice: Insufficient Cloud Log Size
- Privacy Violation: Exposed Default Value
- Privilege Management: Overly Broad Access Policy
- Privilege Management: Overly Permissive Role
- System Information Leak: Kubernetes Profiler

OWASP Top 10 2021

El Top 10 de 2021 de Open Web Application Security Project (OWASP) proporciona un poderoso documento de concienciación sobre la seguridad de las aplicaciones web, centrado en informar al público general sobre las consecuencias de los riesgos de seguridad de las aplicaciones web más comunes y críticos. OWASP Top 10 representa un amplio acuerdo sobre cuáles son los fallos de seguridad más críticos de las aplicaciones web, con un consenso extraído de la recopilación de datos y los resultados de una encuesta. Para proporcionar asistencia a nuestros clientes que desean mitigar el riesgo de las aplicaciones web, se agregó una correlación de la taxonomía de Micro Focus Fortify con OWASP Top 10 2021, que se publicó recientemente.

Otras erratas

En esta versión, seguimos invirtiendo recursos para garantizar la reducción del número de falsos positivos y para mejorar la capacidad de auditoría de los problemas por parte de los clientes. Los clientes también verán cambios en los problemas comunicados en relación con lo siguiente:

Desuso de versiones de Fortify Static Code Analyzer anteriores a 18.x:

Como se comunicó en el anuncio del lanzamiento de 2021.3, esa fue la última versión de Rulepacks compatible con versiones de Fortify Static Code Analyzer anteriores a 18.x. En esta actualización, las versiones de Fortify Static Code Analyzer anteriores a 18.x no cargarán la instancia de Rulepacks. Se deberá cambiar a una versión inferior de Rulepacks o actualizar la versión de SCA. En las versiones futuras, continuaremos admitiendo las cuatro últimas versiones principales de Fortify Static Code Analyzer.

Mejoras para PHP

Se ha mejorado la compatibilidad con la identificación de contraseñas y claves de cifrado en Key Management: categorías de claves de cifrado vacías/codificadas/nulas.

Mejoras de Python

Se ha mejorado la compatibilidad con el módulo *subprocess*, lo que ha permitido mejorar la detección de problemas, como Command Injection.

Mejoras en falsos positivos:

Se ha seguido trabajando con gran esfuerzo para eliminar los falsos positivos en esta versión. Además de las otras mejoras, los clientes disfrutarán de una eliminación adicional de falsos positivos en las áreas siguientes:

- Problemas derivados de los actores de Akka en proyectos de Scala cuando la aplicación no utiliza Play.
- Problemas de Cross-site Scripting en JavaScript cuando solo se puede obtener un control parcial sobre las URL.
- Problemas de Password Management en archivos JSON al referirse a la localización de cadenas
- Problemas de flujo de datos en proyectos de Java y .NET derivados de métodos HTTP.

CyberRes 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:

Discovery API

Esta versión incluye una comprobación para Discovery API. La comprobación de Discovery API se marca cuando WebInspect detecta una definición de API en la especificación de Swagger(spec) en la ubicación especificada por el usuario proporcionada a través de la entrada de comprobación. Estos archivos de especificación pueden no estar directamente referenciados en ninguna página y, por lo tanto, no se detectan en el rastreo. Además de comprobar las especificaciones de Swagger, en las ubicaciones especificadas por el usuario, también se marcarán y comprobarán las definiciones encontradas durante la exploración que no se hayan especificado explícitamente junto con la entrada de comprobación. Aunque estos hallazgos no indican necesariamente una vulnerabilidad de la seguridad, aumentan los recursos que son potencialmente vulnerables a los ataques.

Compatibilidad de vulnerabilidades

OGNL Expression Injection: evaluación doble

CVE-2021-26084 ha identificado una vulnerabilidad grave de OGNL Expression Injection que afecta al servidor de Confluence y al centro de datos de Atlassian. Esta vulnerabilidad permite a un atacante sin identificar ejecutar códigos arbitrarios en aplicaciones vulnerables. Las versiones de los servidores de Atlassian afectadas son las anteriores a la versión 6.13.23, de la versión 6.14.0 a las versiones anteriores a 7.4.11, de la versión 7.5.0 a las versiones anteriores a 7.11.6, y de la versión 7.12.0 a las versiones anteriores a 7.12.5. Esta versión incluye una comprobación que permite detectar esta vulnerabilidad en los servidores de Atlassian afectados.

Directory Traversal

El servidor HTTP de Apache es vulnerable a los ataques de Directory Traversal identificados por CVE-2021-41773 y CVE-2021-42013. Las vulnerabilidades permiten a un atacante manipular direcciones URL que asignan las direcciones a archivos fuera de los directorios configurados por directivas con forma de alias. Los atacantes podrían recuperar el contenido de los archivos en el servidor, lo que conllevaría la divulgación de datos confidenciales, la recuperación potencial de la lógica de negocio de propiedad y, para algunas configuraciones, la ejecución remota de los códigos. Estos problemas solo afectan a las versiones de servidores HTTP de Apache 2.4.49 y 2.4.50. Esta versión incluye una comprobación que permite detectar estas vulnerabilidades en los servidores HTTP de Apache.

Path Manipulation: caracteres especiales

Una vulnerabilidad de Path Manipulation, identificada por CVE-2021-28164, afecta a Eclipse Jetty. El modo de cumplimiento por defecto en las versiones afectadas permite que las peticiones con URI que contienen segmentos con caracteres especiales accedan a recursos protegidos en el directorio WEB-INF. Esto puede revelar información confidencial sobre la implementación de una aplicación web y saltarse determinadas restricciones de seguridad. Esta versión incluye una comprobación que permite detectar instancias de Jetty vulnerables.

Dynamic Code Evaluation: deserialización de XStream no segura

XStream es una herramienta de uso popular para convertir datos entre objetos de Java y XML. El flujo procesado en el momento de la conversión contiene información de tipo para recrear los objetos anteriormente escritos. Un atacante puede manipular el flujo de entrada procesado y reemplazar o insertar objetos, lo que da como resultado la ejecución de un código arbitrario cargado desde un servidor remoto. Esta versión incluye una comprobación que permite detectar la última vulnerabilidad de CVE-2021-39149 sobre la vulnerabilidad de deserialización de XStream no segura en servidores web objetivo.

Path Manipulation: caracteres especiales

Los caracteres de control, como 0x09, no deben ser permitidos en una ruta URL y los clientes deben codificarlos en porcentaje. El rastreo inconsistente de estos caracteres de control entre el proxy y el servidor *back-end* podría introducir varias amenazas. Esta versión incluye una comprobación para detectar si algunos caracteres de control comunes podrían insertarse en la ruta de la URL y tener un impacto negativo en el servidor web *back-end*.

Informes de cumplimiento

OWASP Top 10 2021

El Top 10 de 2021 de Open Web Application Security Project (OWASP) proporciona un poderoso documento de concienciación sobre la seguridad de las aplicaciones web, centrado en informar al público general sobre las consecuencias de los riesgos de seguridad de las aplicaciones web más comunes y críticos. OWASP Top 10 representa un amplio acuerdo sobre cuáles son los fallos de seguridad más críticos de las aplicaciones web, con un consenso extraído de la recopilación de datos y los resultados de una encuesta. Esta actualización de SecureBase incluye una nueva plantilla de informe de cumplimiento que proporciona una correlación de categorías de OWASP Top 10 2021 con comprobaciones de WebInspect.

Actualizaciones de directivas

OWASP Top 10 2021

Se ha incorporado una directiva personalizada a la lista de directivas admitidas en WebInspect SecureBase para incluir las comprobaciones pertinentes para OWASP Top 10 2021. Esta directiva contiene un subconjunto de las comprobaciones de WebInspect disponibles, con el fin de ayudar a los clientes a ejecutar exploraciones de WebInspect específicamente orientadas al cumplimiento.

Otras erratas

En esta versión, seguimos invirtiendo recursos para garantizar la reducción del número de falsos positivos y para mejorar la capacidad de auditoría de los problemas por parte de los clientes. Los clientes también verán cambios en los problemas comunicados en relación con lo siguiente:

Mejoras en la comprobación SSL

Se ha mejorado la comprobación de la lista de cifrado de SSL para reflejar que la siguiente configuración no es compatible con la confidencialidad directa total: TLS_DH_RSA_WITH_AES_128_GCM_SHA256.

CyberRes Fortify Premium Content

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

OWASP Top 10 2021

Para acompañar a las nuevas correlaciones, esta versión también contiene un nuevo paquete de informes con compatibilidad para OWASP Top 10 2021 que se puede descargar en Fortify Customer Support Portal, en la sección Premium Content.

Taxonomía de CyberRes Fortify: Errores en la seguridad del software

El sitio Taxonomía de Fortify, que contiene descripciones de la compatibilidad con las nuevas categorías añadidas, está disponible en https://vulncat.fortify.com. Los clientes que busquen el sitio antiguo con la última actualización compatible pueden encontrarlo en CyberRes Fortify Support Portal.

Póngase en contacto con el soporte técnico de Fortify

CyberRes Fortify
http://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

Póngase en contacto con SSR

Alexander M. Hoole
Director sénior de Software Security Research
CyberRes Fortify
hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
Director de Software Security Research
CyberRes Fortify
peter.blay@microfocus.com