Anuncio de publicación de Software Security Research

Contenido de seguridad del software Fortify

Actualización 2 de 2022

viernes, 24 de junio de 2022

Acerca de CyberRes Fortify Software Security Research

El equipo de Fortify Sofware 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 1.220 categorías de vulnerabilidad en 30 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 2022.2.0), Fortify WebInspect SecureBase (disponible mediante SmartUpdate) y Fortify Premium Content.

Fortify Secure Coding Rulepacks (SCA)

Con esta versión, Fortify Secure Coding Rulepacks detecta 1.000 categorías únicas de vulnerabilidades en 30 lenguajes de programación y abarca más de un millón de API distintas. En resumen, esta versión incluye lo siguiente:

Mejoras de .NET (versión compatible: 6.0)

.NET es una plataforma de programación general que permite a los programadores escribir código en lenguajes como C# y VB.NET con un conjunto estandarizado de API. Esta versión aumenta nuestra cobertura a la última versión de .NET para mejorar el flujo de datos, así como ampliar la cobertura de API para las siguientes categorías:

- Access Control: Database
- Path Manipulation
- Privacy Violation
- Server-Side Request Forgery
- SQL Injection
- System Information Leak: External
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Encryption: Insecure Mode of Operation

Mejoras de ASP.NET Core (versión compatible: 6.0)

ASP.NET Core es el marco web de referencia para usar con .NET. El marco incluye funcionalidades para crear muchos tipos de aplicaciones, entre las que se incluyen aplicaciones web MVC y API web. Esta versión amplía nuestra cobertura a la última versión de ASP.NET Core, que incluye las API mínimas, y expande nuestras categorías admitidas para incluir:

- .NET Attribute Misuse: Authorization Bypass
- ASP.NET Bad Practices: Compression Over Encrypted WebSocket Connection
- ASP.NET Middleware Out of Order: Default Cookie Configuration
- ASP.NET Middleware Out of Order: Insecure Transport
- ASP.NET Middleware Out of Order: Insufficient Logging
- ASP.NET Misconfiguration: Insecure Transport
- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute

Weak Cryptographic Implementation

Psychic Signatures (CVE-2022-21449) es una debilidad en la implementación de Java del algoritmo Elliptical Curve Digital Signature (ECDSA). Esta debilidad permite que un atacante obligue a la aplicación a aceptar una firma digital de ceros como válida. Las versiones vulnerables de Java incluyen: 15, 16, 17 y 18. Si se utiliza una versión vulnerable de Java, un atacante puede falsificar algunos tipos de certificados SSL, tokens web JSON firmados o incluso mensajes de autenticación WebAuthn. Esta versión permite informar sobre la *Weak Cryptographic Implementation* en Java.

Compatibilidad con Jakarta EE (versión admitida: 9.0.0)

Jakarta EE proporciona un conjunto de especificaciones neutral, abierto y completo en forma de un marco de código abierto que se utiliza para desarrollar aplicaciones Java nativas en la nube. Anteriormente se conocía como Java EE (o J2EE), que era uno de los marcos más reconocibles para Java del lado del servidor. Esta versión agrega mejoras a la cobertura existente de Java EE, que abarca 52 categorías de debilidad.

Mejoras en el escaneo de secretos

El escaneo de secretos es una técnica para buscar y detectar secretos en el código fuente y los archivos de configuración. A veces, los archivos de configuración que contienen contraseñas o tokens de API pueden filtrarse accidentalmente a los repositorios de código fuente. Esta versión incluye compatibilidad para formatos hash de contraseña comunes. La cobertura incluye la identificación de secretos y formatos hash de contraseñas comunes en archivos de configuración para productos, entre los que se incluyen los siguientes: OpenVPN, escritorio remoto de Windows, netrc, IntelliJ IDEA, DBeaver, FileZilla, Heroku y DigitalOcean doctl.
Se proporciona cobertura mejorada para las siguientes categorías:

- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key
- Password Management: Hardcoded Password
- Password Management: Password in Configuration File
- Password Management: Weak Cryptography

Mejoras de Express JS (versión compatible: 4.x)[1]

Express es un marco concebido para crear aplicaciones web con Node.js. Proporciona funcionalidades para el enrutamiento, manejo de errores, creación de plantillas, administración de middleware y utilidades relacionadas con HTTP.
En esta versión, mejoramos la compatibilidad con Express 4.x para las siguientes categorías:

- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute
- Insecure Transport
- Path Manipulation
- Privacy Violation
- Process Control
- Setting Manipulation
- System Information Leak: External

[1] Se requiere SCA versión 22.1.1

Handlebars de JavaScript (versión compatible: 4.7.7)

Handlebars es una biblioteca de JavaScript diseñada para crear plantillas web reutilizables. Estas plantillas son una combinación de HTML, texto y expresiones. Las expresiones se incrustan directamente en el código HTML y sirven como marcador de posición para el contenido que debe insertarse mediante el código, lo que hace que el documento sea fácilmente reutilizable.
En esta versión, agregamos compatibilidad para Handlebars 4.7.7, mejoramos la cobertura del flujo de datos y ampliamos la cobertura de la API para las siguientes categorías:

- Cross-Site Scripting: Handlebars Helper
- Handlebars Misconfiguration: Escaping Disabled
- Handlebars Misconfiguration: Prototypes Allowed
- Log Forging
- Log Forging (debug)
- Privacy Violation
- System Information Leak
- Template Injection

Moustache de JavaScript (versión compatible: 4.2.0)

Moustache es un sistema de plantillas sin lógica de código abierto que proporciona plantillas y vistas como base para crear plantillas dinámicas. Las plantillas contienen el formato de presentación y el código, mientras que las vistas contienen los datos que se incluirán en las plantillas.
En esta versión, hemos agregado compatibilidad para Moustache 4.2.0, para identificar las debilidades de *Inyección de plantilla*.

GraphQL.js (versión compatible: 16.5.0)

GraphQL.js es la implementación de referencia de JavaScript para GraphQL y se usa ampliamente en aplicaciones de JavaScript. Esta versión agrega compatibilidad inicial con el servidor GraphQL para detectar las siguientes categorías de debilidad en las API de GraphQL:

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- GraphQL Bad Practices: Introspection Enabled
- GraphQL Bad Practices: GraphiQL Enabled
- Privacy Violation
- System Information Leak: External

Graphene-Python (versión compatible: 3.0.0)

Python-Graphene es un marco de servidor GraphQL popular para aplicaciones de Python. Esta versión mejora la compatibilidad con servidores GraphQL de 2022.1.0 para detectar las siguientes categorías de debilidad en las API de GraphQL:

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation

- Cross-Site Scripting: Reflected
- Privacy Violation
- System Information Leak: External

Infraestructura como código (IaC) en la nube

Infraestructura como código (IaC) es el proceso de administrar y aprovisionar recursos informáticos a través de código en lugar de varios procesos manuales. Esta versión agrega compatibilidad ampliada para IaC. Las tecnologías compatibles incluyen configuraciones de Ansible para la implementación en Azure y AWS y configuraciones de Terraform para la implementación en Azure y GCP. Los problemas comunes relacionados con la configuración de los servicios mencionados ahora se informan al desarrollador.

Configuraciones de Terraform:

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 admiten la configuración y administración de la infraestructura de ***Microsoft Azure***. En esta versión, identificamos las siguientes categorías para las configuraciones de Terraform de los servicios de Microsoft Azure:

- Azure Terraform Misconfiguration: Insecure App Service Transport
- Azure Terraform Misconfiguration: Insecure CDN Endpoint Transport
- Azure Terraform Misconfiguration: Insecure Function App Transport
- Azure Terraform Misconfiguration: Insecure Logic App Transport
- Azure Terraform Misconfiguration: Insecure MariaDB Transport
- Azure Terraform Misconfiguration: Insecure MySQL Transport
- Azure Terraform Misconfiguration: Insecure Network Monitor Transport
- Azure Terraform Misconfiguration: Insecure PostgresSQL Transport
- Azure Terraform Misconfiguration: Insecure Redis Cache Transport
- Azure Terraform Misconfiguration: Insecure Spring Cloud Redis Transport
- Azure Terraform Misconfiguration: Insecure Spring Cloud Transport
- Azure Terraform Misconfiguration: Insecure Storage Account Transport

Los proveedores de Terraform son compatibles con la configuración y administración de la infraestructura de ***Google Cloud Platform (GCP)***. En esta versión, identificamos las siguientes categorías para las configuraciones de Google Cloud Platform Terraform:

- GCP Terraform Bad Practice: Overly Permissive Service Account
- GCP Terraform Misconfiguration: BigQuery Dataset Publicly Accessible
- GCP Terraform Misconfiguration: Cloud DNS DNSSEC Disabled
- GCP Terraform Misconfiguration: Cloud KMS CryptoKey Publicly Accessible
- GCP Terraform Misconfiguration: Cloud SQL Backup Disabled
- GCP Terraform Misconfiguration: Cloud Storage Bucket Publicly Accessible
- GCP Terraform Misconfiguration: Compute Engine Access Control
- GCP Terraform Misconfiguration: Compute Engine Default Service Account
- GCP Terraform Misconfiguration: Compute Engine Project-Wide SSH

- GCP Terraform Misconfiguration: Google Project Network Access Control
- GCP Terraform Misconfiguration: Insecure Cloud SQL Transport
- GCP Terraform Misconfiguration: Insecure Load Balancer Transport
- GCP Terraform Misconfiguration: Insufficient Cloud Storage Bucket Logging
- GCP Terraform Misconfiguration: Insufficient GKE Cluster Logging
- GCP Terraform Misconfiguration: Insufficient GKE Cluster Monitoring
- GCP Terraform Misconfiguration: Insufficient VPC Flow Logging
- GCP Terraform Misconfiguration: GKE Cluster Administrative Interface Access Control
- GCP Terraform Misconfiguration: GKE Cluster Certificate-Based Authentication
- GCP Terraform Misconfiguration: GKE Cluster Legacy Authorization
- GCP Terraform Misconfiguration: GKE Cluster HTTP Basic Authentication
- GCP Terraform Misconfiguration: GKE Container-Optimized OS Not In Use
- GCP Terraform Misconfiguration: GKE Node Auto-Upgrade Disabled
- GCP Terraform Misconfiguration: Weak Cryptographic Cloud DNS Signature
- GCP Terraform Misconfiguration: Weak GKE Cluster Network Management
- GCP Terraform Misconfiguration: Weak Key Management

Configuraciones de Ansible:

Ansible es una herramienta de automatización de código abierto que proporciona administración de configuración, implementación de aplicaciones, aprovisionamiento en la nube y orquestación de nodos en varios entornos.

Ansible incluye módulos que son compatibles con la configuración y administración de ***Amazon Web Services (AWS)***. En esta versión, identificamos las siguientes categorías para las configuraciones de AWS Ansible:

- AWS Ansible Misconfiguration: Amazon RDS Publicly Accessible
- AWS Ansible Misconfiguration: Insecure CloudFront Distribution Transport
- AWS Ansible Misconfiguration: Insufficient CloudTrail Logging

Ansible también incluye módulos que son compatibles con la configuración y administración de ***Servicios de computación en la nube de Microsoft Azure***. En esta versión, identificamos las siguientes categorías para las configuraciones de Microsoft Azure Ansible:

- Azure Ansible Misconfiguration: Overly Permissive Azure SQL Database Firewall

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:

Log4j (versión compatible: 2.17)

La compatibilidad con Log4j ahora incluye la detección de una nueva categoría, *Denial of Service: Stack Exhaustion*.

Oslo.config (versión compatible: 8.8.0)

La compatibilidad inicial para oslo.config para Python incluye la detección de una nueva categoría, *Privacy Violation: Unobfuscated Logging*.

Corrección de errores de Objective-C y mejoras de rendimiento

Los clientes que exploraron proyectos que incluyen archivos Objective-C usando los paquetes de reglas 2022R1 podrían haber encontrado los siguientes problemas:

- Durante la fase de exploración, podrían aparecer mensajes de error como "[error] Unexpected exception during dataflow analysis..." en los archivos de salida o de registro de SCA.
- Tiempo de exploración inusualmente largo en el análisis de flujo de datos, lo que podría provocar problemas de pérdida de flujo de datos.

Se proporcionó un paquete de reglas hotfix de Objective-C a los clientes afectados para abordar esos problemas. Esta versión oficial de R2 incluye la misma solución se incluye. Los clientes que usaban el paquete de reglas hotfix deben eliminar el paquete de reglas hotfix al actualizar a los paquetes de reglas de la versión R2.

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:

- *SQL injection: iBatis Data Map*: se evitan falsos positivos cuando se encuentran caracteres literales '$'
- *Password Management: Password in Configuration File*: se evitan los falsos positivos cuando el valor es un marcador de posición variable
- *ASP.NET MVC Bad Practices: Model With Required Non-Nullable Property*: se evitan falsos positivos en aplicaciones C# ASP.NET al usar el atributo [BindRequired]
- *Often Misused: Authentication*: reducción de falsos positivos en aplicaciones Java
- *XSS: Content Sniffing*: reducción de falsos positivos en aplicaciones Java Spring
- *Privacy Violation*: reducción de falsos positivos en aplicaciones .NET
- *SOQL Injection* y *SOSL Injection*: los problemas encontrados por el analizador semántico ahora se identificarán con Low Fortify Priority Order

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

OGNL Expression Injection: Double Evaluation

Una vulnerabilidad crítica de OGNL Expression Injection identificada por CVE-2022-26134 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 Server and Data Center son de 1.3.0 a 7.4.16, de 7.13.0 a 7.13.6, de 7.14.0 a 7.14.2, de 7.15.0 a 7.15.1, de 7.16.0 a 7.16.3, de 7.17.0 a 7.17.3 y 7.18.0. Esta versión incluye una comprobación que permite detectar esta vulnerabilidad en servidores de Confluence and Data Center.

Dynamic Code Evaluation: Code Injection

Se ha descubierto que Spring Framework de Pivotal es vulnerable a una vulnerabilidad de ejecución remota de código (RCE) identificada por CVE-2022-22965. Un atacante remoto puede proporcionar parámetros de solicitud especialmente diseñados que pueden conducir a la ejecución de código arbitrario. Esta versión incluye una comprobación que permite detectar esta vulnerabilidad en aplicaciones web con versiones afectadas de Spring Framework.

Insecure Deployment: OpenSSL

Se descubrió que OpenSSL, una biblioteca criptográfica popular ampliamente utilizada para ofrecer compatibilidad con conexiones SSL/TLS, es vulnerable a una vulnerabilidad de denegación de servicio (DoS) identificada por CVE-2022-0778. Es posible desencadenar un DoS de bucle infinito en el sistema afectado mediante la elaboración de un certificado que tenga parámetros de curva elíptica explícitos no válidos. Esta versión incluye una comprobación que permite detectar la vulnerabilidad CVE-2022-0778 en los servidores web de destino. Debido a que esta verificación tiene el potencial de causar una condición DoS en el sistema afectado que hace que no esté disponible para el servicio, esta verificación no se incluye en 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.

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 resultados comunicados en relación con lo siguiente:

Password Management: Weak Password Policy

Esta versión incluye mejoras menores para la verificación de la política de contraseñas, donde los campos de contraseña/nombre de usuario se reconocen con una precisión mejorada cuando el tipo de entrada es un cuadro de texto.

Fortify Premium Content

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

Fortify Taxonomy: errores en la seguridad del software

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

Comuníquese con el soporte técnico de Fortify

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

Comuníquese con SSR

Alexander M. Hoole
Director sénior del Equipo de investigación de seguridad para software
CyberRes Fortify
hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
Director del Equipo de investigación de seguridad para software
CyberRes Fortify
peter.blay@microfocus.com