Anuncio de publicación de Software Security Research

Contenido de seguridad del software Fortify

Actualización 3 de 2022

viernes, 30 de septiembre de 2022

Acerca de CyberRes 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 1.244 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 2022.3.0), 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 1024 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:

Actualizaciones de ASP.NET Core (versión compatible: 6.0)[1]

En el patrón Modelo-Vista-Controlador (MVC), las vistas son archivos *.cshtml* que utilizan el lenguaje de programación C# integrado en el marcado Razor. El marcado Razor es un código que interactúa con el marcado HTML para producir una página web enviada al cliente. Las vistas manejan la presentación de datos de la aplicación y la interacción del usuario. Con la versión 22.2.0 y posteriores de Fortify Static Code Analyzer, las reglas ahora admiten la búsqueda de problemas en las vistas.
El soporte incluye la cobertura de las siguientes categorías de debilidad:

- ASP.NET MVC Bad Practices: Form Without AntiForgery Token
- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Open Redirect
- Privacy Violation
- System Information Leak

Entity Framework Core (versión compatible: 6.0)

Entity Framework (EF) Core es una tecnología de acceso a datos de código abierto para aplicaciones .NET. EF Core permite a los desarrolladores asignar objetos .NET a esquemas de base de datos e invocar operaciones de base de datos a través de API estándar y consultas LINQ. El soporte incluye la cobertura de las siguientes categorías de debilidad:

- Access Control: Database
- ASP.NET Bad Practices: Leftover Debug Code
- Connection String Parameter Pollution
- Insecure Transport: Database
- Password Management: Hardcoded Password
- Setting Manipulation
- SQL injection
- System Information Leak: Overly Broad SQL Logging

---

[1] Requiere la versión 22.2.0 o posterior de Fortify Static Code Analyzer.

GitHub Actions

GitHub Actions es una plataforma de integración continua y entrega continua (CI/CD) que permite la automatización de canales de compilación, prueba e implementación. Han salido a la luz debilidades recientes que dan como resultado vectores de ataque de inyección de comandos en una variedad de sistemas. Esta versión incluye cobertura para detectar instancias comunes de esta debilidad de inyección de comandos en la siguiente categoría:

- Command Injection: GitHub Actions

React (versión compatible: 18.2)[2]

React, o ReactJS, es una biblioteca JavaScript de código abierto para crear interfaces de usuario basadas en componentes. Si bien no se admiten nuevas categorías de debilidad en esta versión, la cobertura se ha rediseñado para que React sea más precisa y reduzca los falsos positivos.

React Native (versión compatible: 0.70)[2]

React Native es un marco de interfaz de usuario de código abierto para desarrollar interfaces de usuario multiplataforma en JavaScript y JSX. React Native permite a los desarrolladores escribir aplicaciones móviles que son renderizadas por las API de renderizado nativas de las plataformas de destino para producir una experiencia de usuario depurada y coherente. Además de las categorías de debilidad compatibles con React, se agregan las siguientes categorías de debilidad para React Native:

- Open Redirect
- Privacy Violation
- System Information Leak: Internal

React Native Async Storage (versión compatible: 1.17)[2]

Async Storage es una biblioteca de almacenamiento de valores clave, asíncrona y sin cifrar para React Native basada en el *react-native-async-storageproyecto* de la comunidad. Async Storage proporciona una abstracción sobre los mecanismos de almacenamiento nativos específicos de la plataforma iOS y Android. El soporte permite el flujo de datos a través de Async Storage y la generación de informes de las categorías de debilidades específicas de la plataforma/biblioteca y de JavaScript.

Mejoras en el escaneo de secretos

El escaneo de secretos es el concepto de encontrar secretos en varios códigos fuente y archivos de configuración. Fortify Static Code Analyzer aplica la cobertura de escaneo de secretos a todos los tipos de archivos, lo que permite encontrar secretos específicos independientemente del lenguaje del código. Se agregó soporte para los siguientes secretos, los cuales se reportan como *Password Management: Hardcoded Password* o *Administración de credenciales: Hardcoded API Credentials*:

- Tokens de autenticación básica HTTP
- JWT (JSON Web Tokens)
- Tokens de acceso NPM (Node Package Manager)
- Claves API de Postman
- Token de API de PyPI

---

[2] Requiere la versión 22.2.0 o posterior de Fortify Static Code Analyzer.

Compatibilidad inicial con gRPC para Java y Go (versión compatible: 1.49.0)

Google Remote Procedure Call (gRPC) es un moderno marco RPC de alto rendimiento de código abierto multientorno y multilenguaje. gRPC conecta servicios con soporte para equilibrio de carga, seguimiento y autenticación. A diferencia de JSON tradicional sobre HTTP, gRPC se basa en HTTP2 y normalmente usa el formato de búfer de protocolo binario (protobuf) para los mensajes. Para proyectos de gRPC, los usuarios deben incluir el código generado a partir de las definiciones de archivos .proto durante la fase de traducción de Fortify Static Code Analyzer.

Se agregó soporte para Go gRPC v1.49.0 para cubrir las siguientes categorías de debilidad:

- Header Manipulation
- Privacy Violation
- System Information Leak: External

Se agregó soporte para Java gRPC v1.49.0 para cubrir las siguientes categorías de debilidad:

- Denial of Service
- gRPC Metadata Manipulation
- Insecure Transport
- Insecure Transport: gRPC Server Credentials
- Insecure Transport: gRPC Channel Credentials
- Privacy Violation
- Resource Injection
- System Information Leak: External

Compatibilidad inicial con Flask (versión compatible: 2.2.x)

Flask es un marco web escrito en Python. Inicialmente un contenedor para las bibliotecas *Werkzeug* y *Jinja*, Flask se ha convertido en uno de los marcos de aplicaciones web de Python más populares. Para complementar nuestro soporte de Google Cloud Functions para Python, esta versión contiene soporte solo para los objetos Flask Response.
El soporte incluye la cobertura de las siguientes categorías de debilidad:

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set
- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Broad Domain
- Cookie Security: Overly Broad Path
- Cookie Security: Overly Permissive SameSite Attribute
- Cookie Security: Persistent Cookie
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Header Manipulation
- Header Manipulation: Cookies
- HTML5: Misconfigured Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- HTML5: Overly Permissive CORS Policy
- HTML5: Unenforced Content Security Policy
- Open Redirect

- Privacy Violation
- System Information Leak: External

Google Cloud Functions (versión compatible: 403.0.0)

Google Cloud Functions es un entorno de ejecución sin servidor para crear y conectar servicios en la nube. Puede ejecutar código en respuesta a eventos predefinidos, como llamadas a API, transacciones de base de datos, carga de archivos en Cloud Storage o un mensaje entrante sobre un tema de Pub/Sub.
Cloud Functions ofrece dos versiones del producto: Cloud Functions (1.ª generación), la versión original, y Cloud Functions (2.ª generación), una nueva versión basada en *Cloud Run* y *Eventarc* para proporcionar un conjunto de funciones mejoradas. Esta versión incluye soporte para Google Cloud Functions en Python y soporte actualizado para Google Cloud Functions en Java.

Las categorías de debilidades compatibles con Python incluyen aquellas compatibles con las API de Flask, junto con las siguientes:

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

Para Google Cloud Functions en Python, los usuarios deben incluir el archivo de compilación en la nube JSON o YAML. Alternativamente, los usuarios pueden configurar las siguientes propiedades en el momento del escaneo:

- *com.fortify.sca.rules.GCPFunctionName* debe establecerse como nombre de la función.
- *com.fortify.sca.rules.GCPHttpTrigger* debe establecerse en `true` si el tipo de desencadenador es HTTP y en `false` para otros tipos de desencadenadores.

La compatibilidad con reglas actualizadas para las funciones Java de Google Cloud de 2.ª generación identifica las fuentes de entradas peligrosas que se originan en las solicitudes de CloudEvents.

Compatibilidad inicial con Apollo Server (versión compatible: 3.6.8)

Apollo Server es un servidor GraphQL de código abierto que se utiliza en aplicaciones de JavaScript para crear API de GraphQL. Esta versión agrega compatibilidad inicial con el servidor GraphQL para Apollo Server, incluida la detección de las siguientes categorías de debilidad en las API de GraphQL desarrolladas con Apollo Server:

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

Infraestructura como código (IaC)

IaC es el proceso de administrar y aprovisionar recursos informáticos a través de código en lugar de varios procesos manuales. Las tecnologías compatibles incluyen configuraciones de Terraform para la implementación en GCP, OpenAPI Specification y MuleSoft. Los problemas comunes relacionados con la configuración de estos servicios ahora se notifican al desarrollador.

Configuraciones de Terraform en Google Cloud Platform (GCP)

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 GCP. Esta versión incluye la cobertura de las siguientes categorías de debilidad para las configuraciones de Terraform en GCP:

- GCP Terraform Misconfiguration: Cloud SQL Database Publicly Accessible
- GCP Terraform Misconfiguration: Cloud Storage Bucket Uniform Access Disabled
- GCP Terraform Misconfiguration: Compute Engine IP Forwarding Enabled
- GCP Terraform Misconfiguration: Compute Engine Serial Console Enabled
- GCP Terraform Misconfiguration: Compute Engine Shielded VM Option Disabled
- GCP Terraform Misconfiguration: GKE Cluster Node Auto-Repair Disabled
- GCP Terraform Misconfiguration: GKE Cluster Publicly Accessible
- GCP Terraform Misconfiguration: Overly Permissive Role
- GCP Terraform Misconfiguration: Permissive Firewall

Especificación OpenAPI

La especificación OpenAPI define una descripción estándar e independiente del lenguaje de programación para las API HTTP. Los documentos de OpenAPI que se ajustan a la especificación de OpenAPI se pueden representar en formato JSON o YAML. Este estándar define las capacidades de un servicio sin acceso a la implementación, documentación o inspección de la red. Esta versión incluye cobertura de las siguientes categorías de debilidad para las configuraciones de OpenAPI:

- Error de configuración de OpenAPI: Credential Leakage
- Error de configuración de OpenAPI: Empty Global Security Requirement
- Error de configuración de OpenAPI: Empty Operation Security Requirement
- Error de configuración de OpenAPI: Insecure Transport
- Error de configuración de OpenAPI: Missing Error Handling
- Error de configuración de OpenAPI: Missing Global Security Requirement
- Error de configuración de OpenAPI: Missing Operation Security Requirement
- Error de configuración de OpenAPI: Missing Security Schemes
- Error de configuración de OpenAPI: Optional Global Security Requirement
- Error de configuración de OpenAPI: Optional Operation Security Requirement
- Error de configuración de OpenAPI: Weak Authentication

Mule

Mule Runtime, a menudo denominado simplemente Mule, es un bus de servicios empresariales y un marco de integración proporcionado por MuleSoft. Mule permite integraciones de sistemas existentes como servicios web, HTTP, conectividad de bases de datos Java (JDBC), etc. Mule permite que diferentes aplicaciones se comuniquen entre sí, actuando como un sistema de tránsito entre aplicaciones dentro de una red empresarial o a través de Internet. Esta versión incluye cobertura de las siguientes categorías de debilidad para las configuraciones de Mule:

- Mule Misconfiguration: Hardcoded Password
- Mule Misconfiguration: Insecure Database Transport
- Mule Misconfiguration: Insecure Transport
- Mule Misconfiguration: Server Identity Verification Disabled

Top 25 de CWE 2022

La Common Weakness Enumeration (CWE™) Top 25 (enumeración de las 25 principales debilidades comunes) se introdujo en 2019 y remplaza la SANS Top 25. La CWE Top 25 de 2022 se publicó en junio y se determinó mediante una fórmula heurística que normaliza la frecuencia y la gravedad de las vulnerabilidades comunicadas a la base de datos nacional de vulnerabilidades (NVD) en los últimos dos años. Para ofrecer soporte a nuestros clientes que deseen dar prioridad en sus auditorías a las vulnerabilidades críticas más registradas en la NVD, se agregó una correlación de CyberRes Fortify Taxonomy a la CWE Top 25 de 2022.

Otras erratas

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

Obsolescencia de las versiones de Fortify Static Code Analyzer anteriores a 19.x

Como se observó con la versión 2021.4, continuamos admitiendo las últimas cuatro versiones principales de Fortify Static Code Analyzer. Por lo tanto, esta será la última versión de los paquetes de reglas compatibles con las versiones de Fortify Static Code Analyzer anteriores a la 19.x. Para la próxima versión, las versiones de Fortify Static Code Analyzer anteriores a la 19.x no cargarán los paquetes de reglas más recientes. Se deberá cambiar a una versión inferior de Rulepacks o actualizar la versión de Fortify Static Code Analyzer. En las versiones futuras, continuaremos admitiendo las últimas cuatro versiones principales de Fortify Static Code Analyzer.

Cambio de nombre de las categorías de debilidades de la infraestructura como código (IaC)

A medida que el soporte para detectar configuraciones incorrectas y malas prácticas relacionadas con la IaC continúa madurando, nuestro próximo lanzamiento de contenido de seguridad incluirá cambios en el nombre de categoría de un subconjunto de categorías de debilidad (actualización 4 de 2022). Cuando se producen cambios en el nombre de la categoría de debilidad, los resultados del escaneo al fusionar escaneos anteriores con nuevos escaneos darán como resultado categorías añadidas o eliminadas.

Refactorización de metadatos de orden de prioridad de Fortify para categorías de debilidad

A medida que el ámbito de la seguridad de las aplicaciones sigue evolucionando, también lo hacen nuestro conocimiento y entendimiento colectivos del impacto de las categorías de debilidad en la confidencialidad, la integridad y la disponibilidad. Nuestro próximo lanzamiento de contenido de seguridad incluirá cambios en los campos de metadatos de debilidad "precisión" e "impacto" para un subconjunto de categorías de debilidad (actualización 4 de 2022). Cuando se producen cambios en los campos de metadatos de debilidad, es posible que los resultados de escaneos futuros tengan problemas que aparezcan en diferentes carpetas de conjuntos de filtros (p. ej., crítico, alto, medio, bajo). Las actualizaciones iniciales provocarán que algunos problemas pasen de las carpetas superiores de Fortify Priority Order (FPO) a las carpetas inferiores de FPO. Los clientes deben estar preparados para saber cómo puede afectar este cambio a los conjuntos de filtros y las plantillas existentes.

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:

- *Cross-Site Request Forgery*: falsos positivos eliminados en aplicaciones .NET que utilizan versiones de .NET Framework posteriores a la 4.5.2
- *JavaScript Hijacking*: problemas (consulte la sección a continuación)

- *Key Management*: se reducen los falsos positivos en los escaneos de JavaScript
- *Key Management*: reducción de falsos positivos que afectan principalmente a proyectos SAPUI5
- *Key Management*: los problemas basados en comparaciones produjeron muchos falsos positivos y se eliminaron
- *Password Management: Hardcoded/Empty/Null Password*: se evitan falsos positivos para expresiones condicionales de C#
- *Password Management*: se reducen los falsos positivos de los archivos NPM, Yarn y Bower
- *Privacy Violation: Autocomplete*: se reducen los falsos positivos al establecer nuevas contraseñas
- *Setting Manipulation*: se reducen los falsos positivos al borrar las variables de entorno
- *Weak Cryptographic Signature*: se evitan los falsos positivos en el paquete java.security
- *XML Entity Expansion Injection*: se reducen los falsos positivos en programas Java que utilizan transformadores JAXP

JavaScript Hijacking Eliminación

Las siguientes categorías ya no son relevantes en ECMAScript moderno, por lo que se han eliminado:

- JavaScript Hijacking
- JavaScript Hijacking: Constructor Poisoning
- JavaScript Hijacking: Vulnerable Framework

Como resultado, todos los problemas de las categorías anteriores se eliminarán de los resultados del escaneo.

Cambios de categoría

Junto con las eliminaciones de falsos positivos, identificamos algunos lugares en los que las categorías deberían haberse unificado o estaban mal etiquetadas. Cuando se producen cambios en el nombre de la categoría de debilidad, los resultados del escaneo al fusionar escaneos anteriores con nuevos escaneos darán como resultado categorías añadidas o eliminadas.

- *Insecure SSL: Android Hostname Verification Disabled* ahora se notifica como *Insecure SSL: Server Identity Verification Disabled*
- En Dockerfiles, *Password Management:* los problemas *Hardcoded Password* ahora se notifican como *Password Management: Password in Configuration Files*
- En .NET, algunas instancias de *Setting Manipulation* al establecer una cadena de conexión de base de datos ahora se notifican como *Connection String Parameter Pollution*

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

dotCMS es un sistema de administración de contenido que brinda la capacidad de crear y reutilizar contenido, imágenes y activos en una ubicación centralizada. La API de ContentResource es susceptible a una vulnerabilidad de ejecución remota de código (RCE) identificada por CVE-2022-26352. El nombre del archivo utilizado para almacenar el contenido se crea a partir de la entrada del usuario proporcionada en la solicitud de varias partes y dotCMS no lo desinfecta.

Permite que un atacante cargue archivos arbitrarios en el sistema, lo que resulta en RCE. Esta versión incluye una verificación para detectar esta vulnerabilidad en un servidor de destino que ejecuta versiones dotCMS afectadas.

Insecure Deployment: Unpatched Application

Apache APISIX es una puerta de enlace API de código abierto que proporciona funciones de gestión de tráfico, como equilibrio de carga, upstream dinámico, etc. Esta puerta de enlace API es susceptible a una vulnerabilidad RCE identificada por CVE-2022-24112. Un atacante puede eludir las restricciones de IP en Apache APISIX a través del complemento de solicitud por lotes. Si APISIX usa una clave de administración predeterminada, con la API de administración habilitada y sin un puerto de administración personalizado asignado, un atacante puede invocar la API de administración a través del complemento de solicitudes por lotes, lo que resulta en RCE. Esta versión incluye una verificación para detectar esta vulnerabilidad en un servidor de destino que ejecuta versiones Apache APISIX afectadas.

Dynamic Code Evaluation: JNDI Reference Injection[3]

Java Naming and Directory Interface (JNDI) es una API de Java que permite a los clientes descubrir y buscar datos y objetos por nombre. Estos objetos se pueden almacenar y recuperar a través de diferentes nombres o servicios de directorio, como la invocación de métodos remotos (RMI), la arquitectura de agente de solicitud de objetos comunes (CORBA), el protocolo ligero de acceso a directorios (LDAP) o el servicio de nombres de dominio (DNS). Si los atacantes obtienen el control del argumento de una operación de búsqueda JNDI, podrían apuntar la búsqueda a un servicio de nombres o de directorio bajo su control y devolver una referencia JNDI que utiliza una fábrica remota para la creación de instancias de objetos. Este ataque puede permitir la ejecución de código remoto arbitrario en el servidor de destino que realiza la operación de búsqueda. Esta versión incluye una comprobación que permite detectar esta vulnerabilidad en los servidores web de destino.

Dynamic Code Evaluation: Unsafe Deserialization[3]

CVE-2022-21445 identificó una vulnerabilidad de deserialización insegura de Java de preautorización en componentes ADF Faces de las versiones 12.2.1.3.0 y 12.2.1.4.0 de Oracle Fusion Middleware Afecta a todas las aplicaciones que dependen de los componentes ADF Faces, incluidos Business Intelligence, Enterprise Manager, Identity Management, SOA Suite, WebCenter Portal, Application Testing Suite y Transportation Management. Este problema permite a los atacantes ejecutar código arbitrario en el servidor, abusar de la lógica de la aplicación o montar ataques de denegación de servicio (DoS). Esta versión incluye una comprobación que permite detectar esta vulnerabilidad en los servidores web de destino.

Informes de cumplimiento

Top 25 de CWE 2022

La Common Weakness Enumeration (CWE™) Top 25 (enumeración de las 25 principales debilidades comunes) se introdujo en 2019 y remplaza la SANS Top 25. La CWE Top 25 de 2022 se publicó en junio y se determinó mediante una fórmula heurística que normaliza la frecuencia y la gravedad de las vulnerabilidades comunicadas a la base de datos nacional de vulnerabilidades (NVD) en los últimos dos años.

---

[3] Requiere funciones OAST que están disponibles en el parche WebInspect 21.2.0.117 o posterior.

La actualización de SecureBase incluye las verificaciones que realizan asignaciones de manera directa a la categoría identificada en CWE Top 25, o bien a un ID de CWE relacionado con uno de los incluidos en el Top 25 a través de una relación “ChildOf”.

Actualizaciones de directivas

2022 CWE Top 25

Se incorporó una directiva personalizada a la lista de directivas admitidas en WebInspect SecureBase para incluir las comprobaciones pertinentes para 2022 CWE Top 25.

Otras erratas

En esta versión, seguimos invirtiendo 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:

Dynamic Code Evaluation: Unsafe Deserialization[4]

La comprobación identificada por ID 11504 se modificó para usar cargas útiles que admitan la función OAST. La mejora de esta comprobación reduce los falsos positivos y aumenta la eficiencia y la precisión de sus resultados.

Fortify Premium Content

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

Top 25 de CWE 2022

Para acompañar las nuevas correlaciones, esta versión también contiene un nuevo paquete de informes para Fortify Software Security Center compatible con 2022 CWE Top 25, que se puede descargar de Fortify Customer Support Portal, en la sección Premium Content.

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.

[4] Requiere funciones OAST que están disponibles en el parche WebInspect 21.2.0.117 o posterior.

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