Anúncio da versão do Software Security Research

Conteúdo de Segurança de Software do Fortify

Atualização 3 de 2022

sexta-feira, 30 de setembro de 2022

Sobre o CyberRes Fortify Software Security Research

A equipe do Fortify Software Security Research traduz pesquisas de ponta em inteligência de segurança que potencializa o portfólio de produtos Fortify, incluindo o Fortify Static Code Analyzer (SCA) e o Fortify WebInspect. Atualmente, o conteúdo de segurança de software do Fortify oferece suporte a 1.244 categorias de vulnerabilidade em 30 linguagens e se estende por mais de um milhão de APIs individuais.

O Fortify Software Security Research (SSR) tem o prazer de anunciar a disponibilidade imediata de atualizações para Fortify Secure Coding Rulepacks (idioma inglês, versão 2022.3.0), Fortify WebInspect SecureBase (disponível via SmartUpdate) e Fortify Premium Content.

Fortify Secure Coding Rulepacks [Fortify Static Code Analyzer]

Nesta versão, o Fortify Secure Coding Rulepacks detecta 1.024 categorias únicas de vulnerabilidades em 30 linguagens de programação e abrange mais de um milhão de APIs individuais. Em resumo, essa versão inclui o seguinte:

Atualizações do ASP.NET Core (versão com suporte: 6.0)[1]

No padrão Model-View-Controller (MVC), as exibições são arquivos *.cshtml* que usam a linguagem de programação C# incorporada na marcação Razor. A marcação Razor é um código que interage com a marcação HTML para produzir uma página da Web enviada ao cliente. As exibições tratam da apresentação de dados do aplicativo e da interação do usuário. Usando o Fortify Static Code Analyzer versão 22.2.0 e posterior, as regras agora oferecem suporte à localização de problemas nas exibições.

O suporte inclui cobertura das seguintes categorias de vulnerabilidades:

- 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 (versão com suporte: 6.0)

O Entity Framework (EF) Core é uma tecnologia de acesso a dados de código aberto para aplicativos .NET. O EF Core permite que os desenvolvedores mapeiem objetos .NET para esquemas de banco de dados e invoquem operações de banco de dados por meio de APIs padrão e consultas LINQ. O suporte inclui cobertura das seguintes categorias de vulnerabilidades:

- 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] Requer o Fortify Static Code Analyzer versão 22.2.0 ou posterior.

GitHub Actions

O GitHub Actions é uma plataforma de integração contínua e entrega contínua (CI/CD) que permite a automação de pipelines de compilação, teste e implantação. Vulnerabilidades recentes vieram à tona, resultando em vetores de ataque de injeção de comando em uma variedade de sistemas. Essa versão inclui cobertura para detectar instâncias comuns dessa vulnerabilidade de injeção de comando na seguinte categoria:

- Command Injection: GitHub Actions

React (versão com suporte: 18.2)[2]

React, ou ReactJS, é uma biblioteca JavaScript de código aberto para criar interfaces de usuário baseadas em componentes. Embora nenhuma nova categoria de vulnerabilidade tenha suporte nessa versão, a cobertura foi refatorada para que o React seja mais preciso e reduza os falsos positivos.

React Native (versão com suporte: 0.70)[2]

O React Native é uma estrutura de interface do usuário de código aberto para desenvolver interfaces de usuário multiplataforma em JavaScript e JSX. O React Native permite que os desenvolvedores escrevam aplicativos móveis que são renderizados pelas APIs de renderização nativas das plataformas de destino para produzir uma experiência de usuário polida e consistente. Além das categorias de vulnerabilidades com suporte pelo React, as seguintes categorias de vulnerabilidades são adicionadas ao React Native:

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

React Native Async Storage (versão com suporte: 1.17)[2]

O Async Storage é uma biblioteca de armazenamento de chave-valor não criptografada e assíncrona para React Native com base no projeto *react-native-async-storage* da comunidade. O Async Storage fornece uma abstração sobre os mecanismos de armazenamento específicos da plataforma nativa iOS e Android. O suporte permite o fluxo de dados por meio do Async Storage e os relatórios das categorias de vulnerabilidades existentes específicas do JavaScript e da plataforma/biblioteca.

Melhorias no Secret Scanning

O secret scanning é o conceito de encontrar segredos em vários códigos-fonte e arquivos de configuração. O Fortify Static Code Analyzer aplica a cobertura do secret scanning a todos os tipos de arquivo, o que permite encontrar segredos específicos, independentemente da linguagem do código. O suporte para os segredos a seguir foi adicionado e é relatado como *Password Management: Hardcoded Password* ou *Credential Management: Hardcoded API Credentials*:

- Tokens de autenticação HTTP Basic
- JWT (JSON Web Tokens)
- Tokens de acesso NPM (Node Package Manager)
- Chaves da API Postman
- Token da API PyPI

---

[2] Requer o Fortify Static Code Analyzer versão 22.2.0 ou posterior.

Suporte inicial a gRPC para Java e Go (versão com suporte: 1.49.0)

O Google Remote Procedure Call (gRPC) é uma estrutura RPC de alto desempenho de código aberto multiambiente e multilíngue moderna. O gRPC conecta serviços com suporte para balanceamento de carga, rastreamento e autenticação. Ao contrário do JSON-over-HTTP tradicional, o gRPC é baseado em HTTP2 e normalmente usa o formato binário Protocol Buffers (protobuf) para mensagens. Para projetos do gRPC, os usuários devem incluir o código gerado com base nas definições do arquivo .proto durante a fase de tradução do Fortify Static Code Analyzer.

Foi adicionado suporte para Go gRPC v1.49.0 para abranger as seguintes categorias de vulnerabilidades:

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

Foi adicionado suporte para Java gRPC v1.49.0 para abranger as seguintes categorias de vulnerabilidades:

- 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

Suporte inicial ao Flask (versão com suporte: 2.2.x)

Flask é um framework para web escrito em Python. Inicialmente um wrapper para as bibliotecas *Werkzeug* e *Jinja*, o Flask se tornou um dos frameworks de aplicativos web Python mais populares. Para complementar nosso suporte do Google Cloud Functions para Python, essa versão contém suporte apenas para os objetos Flask Response.
O suporte inclui cobertura das seguintes categorias de vulnerabilidades:

- 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 (versão com suporte: 403.0.0)

O Google Cloud Functions é um ambiente de execução sem servidor para criar e conectar serviços em nuvem. Ele pode executar código em resposta a eventos predefinidos, como chamadas de API, transações de banco de dados, upload de arquivos para o Cloud Storage ou uma mensagem recebida em um tópico Pub/Sub.
O Cloud Functions oferece duas versões de produto: Cloud Functions (1ª geração), a versão original, e Cloud Functions (2ª geração), uma nova versão criada no *Cloud Run* e *Eventarc* para fornecer um conjunto de recursos aprimorado. Essa versão inclui suporte para o Google Cloud Functions em Python e suporte atualizado para o Google Cloud Functions em Java.

As categorias de vulnerabilidades compatíveis com Python incluem aquelas compatíveis com APIs do Flask, juntamente com o seguinte:

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

Para o Python Google Cloud Functions, os usuários devem incluir o arquivo de compilação da nuvem JSON ou YAML. Como alternativa, os usuários podem definir as seguintes propriedades no momento da verificação:

- *com.fortify.sca.rules.GCPFunctionName* deve ser definido com o nome da função.
- *com.fortify.sca.rules.GCPHttpTrigger* deve ser definido como `true` se o tipo de gatilho é HTTP, `false` para outros tipos de gatilho.

O suporte de regras atualizado para o Java Google Cloud Functions de 2ª geração identifica fontes de entrada perigosas originadas de solicitações do CloudEvents.

Suporte inicial ao Apollo Server (versão com suporte: 3.6.8)

O Apollo Server é um servidor GraphQL de código aberto usado em aplicativos JavaScript para criar APIs GraphQL. Essa versão adiciona suporte inicial do servidor GraphQL para o Apollo Server, incluindo a detecção das seguintes categorias de vulnerabilidade nas APIs GraphQL desenvolvidas com o 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

Infraestrutura como código (IaC)

IaC é o processo de gerenciamento e provisionamento de recursos de computador por meio de código, em vez de vários processos manuais. As tecnologias com suporte incluem configurações do Terraform para implantação no GCP, especificação OpenAPI e MuleSoft. Problemas comuns relacionados à configuração desses serviços mencionados agora são relatados ao desenvolvedor.

Configurações do Terraform do Google Cloud Platform (GCP)

Terraform é uma ferramenta de IaC de código aberto para criar, alterar e controlar a versão da infraestrutura da nuvem. Ele usa sua própria linguagem declarativa conhecida como HashiCorp Configuration Language (HCL). A infraestrutura da nuvem é codificada em arquivos de configuração para descrever o estado desejado. Os provedores do Terraform oferecem suporte à configuração e gerenciamento da infraestrutura do GCP. Esta versão inclui a cobertura das seguintes categorias de vulnerabilidades para configurações do GCP Terraform:

- 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

Especificação OpenAPI

A especificação OpenAPI define uma descrição padrão independente de linguagem de programação para APIs HTTP. Os documentos OpenAPI que estão em conformidade com a especificação OpenAPI podem ser representados em um formato JSON ou YAML. Esse padrão define os recursos de um serviço sem acesso à implementação, documentação ou por meio de inspeção de rede. Essa versão inclui a cobertura das seguintes categorias de vulnerabilidades para configurações do OpenAPI:

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

Mule

O Mule Runtime, muitas vezes referido simplesmente como Mule, é um barramento de serviço corporativo e uma estrutura de integração fornecida pela MuleSoft. O Mule permite integrações de sistemas existentes, como serviços Web, HTTP, Java Database Connectivity (JDBC) e muito mais. O Mule permite que diferentes aplicativos se comuniquem, atuando como um sistema de trânsito entre aplicativos em uma rede corporativa ou pela Internet. Essa versão inclui a cobertura das seguintes categorias de vulnerabilidades para configurações do Mule:

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

2022 CWE Top 25

O Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) foi introduzido em 2019 e substitui o SANS Top 25. Lançado em junho, o 2022 CWE Top 25 foi determinado usando uma fórmula heurística que normaliza a frequência e a gravidade das vulnerabilidades relatadas ao National Vulnerability Database (NVD) nos últimos dois anos. Para dar suporte a nossos clientes que desejam priorizar suas auditorias em torno das vulnerabilidades críticas mais comumente relatadas no NVD, foi adicionada uma correlação do CyberRes Fortify Taxonomy com o 2022 CWE Top 25.

Erratas diversas

Nesta versão, continuamos a investir recursos para garantir que possamos reduzir o número de problemas de falsos positivos, refatorar para consistência e melhorar a capacidade dos clientes de auditar problemas. Os clientes também podem esperar alterações nos problemas relatados relacionadas ao seguinte:

Descontinuação das versões do Fortify Static Code Analyzer anteriores à 19.x

Conforme observado na versão 2021.4, continuamos a oferecer suporte às últimas quatro versões principais do Fortify Static Code Analyzer. Portanto, essa será a última versão do Rulepacks que oferece suporte a versões do Fortify Static Code Analyzer anteriores à 19.x. No próximo lançamento, as versões do Fortify Static Code Analyzer anteriores à 19.x não vão mais carregar o Rulepacks mais recente. Será necessário fazer o downgrade do Rulepacks ou o upgrade da versão do Fortify Static Code Analyzer. Nas versões futuras, vamos continuar a oferecer suporte para as últimas quatro versões principais do Fortify Static Code Analyzer.

Renomeação das categorias de vulnerabilidade da Infraestrutura como Código (IaC)

À medida que o suporte para detectar configurações incorretas e práticas ruins relacionadas ao IaC continuar a amadurecer, nossa próxima versão de conteúdo de segurança incluirá alterações no nome da categoria para um subconjunto das categorias de vulnerabilidade (2022 Update 4). Quando ocorrerem alterações no nome da categoria de vulnerabilidade, os resultados da varredura ao mesclar verificações anteriores com novas verificações resultarão em categorias adicionadas/removidas.

Refatoração de metadados de ordem prioritária do Fortify para categorias de vulnerabilidade

À medida que o domínio de segurança de aplicativos continua a amadurecer, nosso conhecimento coletivo e compreensão do impacto das categorias de vulnerabilidade na confidencialidade, integridade e disponibilidade evoluem. Nossa próxima versão de conteúdo de segurança incluirá alterações nos campos de metadados de vulnerabilidades "precisão" e "impacto" para um subconjunto de categorias de vulnerabilidades (2022 Update 4). Quando ocorrem alterações no campo de metadados de vulnerabilidades, os resultados da verificação futura podem apresentar problemas em diferentes pastas do conjunto de filtros (por exemplo, crítica, alta, média, baixa). As atualizações iniciais farão com que alguns problemas sejam movidos de pastas de Ordem de Prioridade da Fortify (FPO) mais altas para pastas de FPO mais baixas. Os clientes devem estar preparados para como essa mudança pode afetar os conjuntos de filtros e modelos existentes.

Melhorias em falsos positivos

O trabalho continuou com o esforço para remover falsos positivos nessa versão. Além de outras melhorias, os clientes podem esperar uma maior remoção de falsos positivos nas seguintes áreas:

- *Cross-Site Request Forgery* — falsos positivos removidos em aplicativos .NET usando versões do .NET Framework posteriores à 4.5.2
- *JavaScript Hijacking* — problemas (consulte a seção abaixo)

- *Key Management* — falsos positivos reduzidos nas verificações de JavaScript
- *Key Management* — redução de falsos positivos que afetam principalmente projetos SAPUI5
- *Key Management* — problemas baseados em comparações produziam muitos falsos positivos e foram removidos
- *Password Management: Hardcoded/Empty/Null Password* — falsos positivos evitados para instruções condicionais C#
- *Password Management* — falsos positivos reduzidos de arquivos do NPM, Yarn e Bower
- *Privacy Violation: Autocomplete* — falsos positivos reduzidos com a definição de novas senhas
- *Setting Manipulation* — falsos positivos reduzidos com a limpeza de variáveis de ambiente
- *Weak Cryptographic Signature* — falsos positivos evitados no pacote java.security
- *XML Entity Expansion Injection* — falsos positivos reduzidos em programas Java usando transformadores JAXP

Remoção de JavaScript Hijacking

As categorias a seguir não são mais relevantes no ECMAScript moderno e foram removidas:

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

Como resultado, todos os problemas das categorias acima serão removidos dos resultados da verificação.

Mudanças de categoria

Junto com remoções de falsos positivos, identificamos alguns lugares em que as categorias deveriam ter sido unificadas ou foram rotuladas incorretamente. Quando ocorrerem alterações no nome da categoria de vulnerabilidade, os resultados da varredura ao mesclar verificações anteriores com novas verificações resultarão em categorias adicionadas/removidas.

- *Insecure SSL: Android Hostname Verification Disabled* agora é relatada como *Insecure SSL: Server Identity Verification Disabled*
- No Dockerfiles, *Password Management:* Os problemas de *Hardcoded Password* agora são relatados como *Password Management: Password in Configuration Files*
- No .NET, algumas instâncias de *Setting Manipulation* na definição de uma cadeia de conexão de banco de dados agora são relatadas como *Connection String Parameter Pollution*

Fortify SecureBase [Fortify WebInspect]

O Fortify SecureBase combina verificações de milhares de vulnerabilidades com políticas que orientam os usuários nas seguintes atualizações disponíveis imediatamente pelo SmartUpdate:

Suporte a vulnerabilidades

Insecure Deployment: Unpatched Application

dotCMS é um sistema de gerenciamento de conteúdo que oferece a capacidade de criar e reutilizar conteúdo, imagens e ativos em um local centralizado. A API ContentResource é suscetível a uma vulnerabilidade de execução remota de código (RCE) identificada por CVE-2022-26352. O nome do arquivo usado para armazenar o conteúdo é criado com base na entrada do usuário fornecida na solicitação de várias partes e não é sanitizado pelo dotCMS.

Ele permite que um invasor faça upload de arquivos arbitrários para o sistema, resultando em RCE. Essa versão inclui uma verificação para detectar essa vulnerabilidade em um servidor de destino que executa as versões afetadas do dotCMS.

Insecure Deployment: Unpatched Application

Apache APISIX é um gateway de API de código aberto que fornece recursos de gerenciamento de tráfego, como balanceamento de carga, upstream dinâmico e muito mais. Esse gateway de API é suscetível a uma vulnerabilidade RCE identificada por CVE-2022-24112. Um invasor pode ignorar as restrições de IP no Apache APISIX por meio do plug-in de solicitação em lote. Se o APISIX usar uma chave de Administrador padrão, com a API Admin habilitada e nenhuma porta de administração personalizada atribuída, um invasor poderá invocar a API Admin por meio do plug-in de solicitações em lote, resultando em RCE. Essa versão inclui uma verificação para detectar essa vulnerabilidade no servidor de destino que executa as versões afetadas do Apache APISIX.

Dynamic Code Evaluation: JNDI Reference Injection[3]

Java Naming and Directory Interface (JNDI) é uma API Java que permite que os clientes descubram e pesquisem dados e objetos por nome. Esses objetos podem ser armazenados e recuperados por meio de diferentes serviços de nomenclatura ou diretório, como Remote Method Invocation (RMI), Common Object Request Broker Architecture (CORBA), Lightweight Directory Access Protocol (LDAP) ou Serviço de Nomes de Domínio (DNS). Se os invasores obtiverem o controle do argumento para uma operação de pesquisa JNDI, eles poderão apontar a pesquisa para um serviço de Nomenclatura ou Diretório sob seu controle e retornar uma referência JNDI que usa uma fábrica remota para instanciação de objeto. Esse ataque pode permitir a execução de código remoto arbitrário no servidor de destino que executa a operação de pesquisa. Essa versão inclui uma verificação para detectar essa vulnerabilidade nos servidores web de destino.

Dynamic Code Evaluation: Unsafe Deserialization[3]

Uma vulnerabilidade de desserialização Java insegura de pré-autorização em componentes do ADF Faces do Oracle Fusion Middleware versões 12.2.1.3.0 e 12.2.1.4.0 foi identificada pelo CVE-2022-21445. Ela afeta todos os aplicativos que dependem dos componentes do ADF Faces, incluindo Business Intelligence, Enterprise Manager, Identity Management, SOA Suite, WebCenter Portal, Application Testing Suite e Transportation Management. Esse problema permite que invasores executem código arbitrário no servidor, abusem da lógica do aplicativo ou montem ataques de negação de serviço (DoS). Essa versão inclui uma verificação para detectar essa vulnerabilidade nos servidores web de destino.

Relatórios de conformidade

2022 CWE Top 25

O Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) foi introduzido em 2019 e substitui o SANS Top 25. Lançado em junho, o 2022 CWE Top 25 é determinado usando uma fórmula heurística que normaliza a frequência e a gravidade das vulnerabilidades relatadas ao National Vulnerability Database (NVD) nos últimos dois anos.

---

[3] Requer os recursos OAST disponíveis no patch WebInspect 21.2.0.117 ou posterior.

O SecureBase inclui verificações que mapeiam diretamente para a categoria identificada pelo CWE Top 25, ou um CWE-ID relacionado a um CWE-ID no Top 25 via relacionamento “ChildOf”.

Atualizações de política

2022 CWE Top 25

Uma política personalizada para incluir verificações relevantes para 2022 CWE Top 25 foi adicionada à lista WebInspect SecureBase de políticas com suporte.

Erratas diversas

Nesta versão, foram investidos recursos para reduzir ainda mais o número de problemas de falsos positivos e melhorar a capacidade dos clientes de auditar problemas. Os clientes também podem esperar alterações nas descobertas relatadas relacionadas ao seguinte:

Dynamic Code Evaluation: Unsafe Deserialization[4]

A verificação identificada pelo ID 11504 foi modificada para usar cargas úteis compatíveis com o recurso OAST. A melhoria dessa verificação reduz os falsos positivos e aumenta a eficiência e a precisão dos seus resultados.

Fortify Premium Content

A equipe de pesquisa cria, estende e mantém uma variedade de recursos fora dos nossos principais produtos de inteligência de segurança.

2022 CWE Top 25

Para acompanhar as novas correlações, esta versão também contém um novo pacote de relatórios para o Fortify Software Security Center com suporte para 2022 CWE Top 25, que está disponível para download no Portal de Suporte ao Cliente Fortify em Conteúdo Premium.

Fortify Taxonomy: Erros de segurança de software

O site do Fortify Taxonomy, que contém descrições para suporte de categoria recém-adicionadas, está disponível em https://vulncat.fortify.com. Os clientes que procuram o site anterior com a última atualização com suporte, podem acessá-lo no Portal de suporte da Fortify.

[4] Requer os recursos OAST disponíveis no patch WebInspect 21.2.0.117 ou posterior.

Entre em contato com o suporte técnico do Fortify

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

SSR de Contato

Alexander M. Hoole
Gerente Sênior, Software Security Research
CyberRes Fortify
hoole@microfocus.com
+1 (650) 258-5916

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