# Micro Focus

## Conteúdo de segurança do software Fortify

### Atualização 4 de 2019

### 13 de dezembro de 2019

**Sobre o Micro Focus Fortify Software Security Research**

A equipe do Fortify Software Security Research converte pesquisa de ponta em inteligência de segurança que fortalece o portfólio de produtos Fortify, incluindo o Fortify Static Code Analyzer (SCA), o Fortify WebInspect e o Fortify Application Defender. Atualmente, o Conteúdo de segurança do software Micro Focus Fortify oferece suporte a 1.018 categorias de vulnerabilidade em 26 linguagens de programação e se estende por mais de um milhão de APIs individuais.

Saiba mais em: https://software.microfocus.com/en-us/software/security-research

O Fortify Software Security Research (SSR) tem a satisfação de anunciar a disponibilidade imediata de atualizações para o Fortify Secure Coding Rulepacks (versão em inglês 2019.4.0), Fortify WebInspect SecureBase (disponível via SmartUpdate) e Fortify Premium Content.

## Micro Focus Fortify Secure Coding Rulepacks [SCA]

Nesta versão, os Pacotes de regras de codificação segura do Fortify detectam 807 categorias únicas de vulnerabilidades em 26 linguagens de programação e abrangem mais de um milhão de APIs individuais. Em resumo, essa versão inclui o seguinte:

### Suporte inicial para Go[1]

Suporte inicial para Go. O Go é uma linguagem de software livre estaticamente tipada projetada pelo Google™ que visa facilitar a criação de software simples, confiável e eficiente. O Go é sintaticamente semelhante ao C, mas com mecanismos de segurança de memória, coleta de lixo e tipagem estrutural. Esta atualização abrange 10 namespaces da biblioteca padrão principal e suporte para as 34 seguintes categorias:

- Access Control: Banco de dados
- Command Injection
- Poluição de parâmetro da cadeia de conexão
- Segurança de cookies: cookie não enviado sobre SSL
- Segurança de cookies: HTTPOnly não definido
- Segurança de cookies: domínio excessivamente amplo
- Segurança de cookies: caminho excessivamente amplo
- Script entre sites: persistente
- Script entre sites: validação inadequada
- Script entre sites: refletido
- File Permission Manipulation
- Header Manipulation
- Header Manipulation: cookies
- HTML5: detecção de MIME
- Transporte inseguro
- Gerenciamento de chaves: chave de criptografia vazia
- Gerenciamento de chaves: chave de criptografia inserida em código fixo
- Gerenciamento de chaves: chave de criptografia nula
- Open Redirect
- Gerenciamento de senhas
- Gerenciamento de senhas: senha vazia
- Gerenciamento de senhas: Hardcoded Password
- Gerenciamento de senhas: senha nula
- Gerenciamento de senhas: criptografia fraca
- Path Manipulation
- Path Manipulation: Zip Entry Overwrite
- Privacy Violation
- Server-Side Request Forgery
- Setting Manipulation
- SQL Injection
- Vazamento de informações do sistema: externo
- Vazamento de informações do sistema: interno

[1] Requer o SCA v19.2.0 ou posterior.

- Criptografia fraca
- Criptografia fraca: tamanho de chave insuficiente

## Spring Security

O Spring Security é uma estrutura de autenticação e controle de acesso que também fornece camadas adicionais de segurança, como cabeçalhos de segurança, que oferecem proteção adicional contra ataques como fixação de sessão, clickjacking e solicitação intersite forjada. É o padrão de fato para proteger aplicativos baseados em Spring. Esta atualização inclui suporte, até a versão 5.2.1, para as 21 seguintes categorias:

- Segurança de cookies: cookie não enviado sobre SSL
- Segurança de cookies: domínio excessivamente amplo
- Cross-Site Request Forgery
- Header Manipulation
- HTML5: Proteção contra script entre sites
- HTML5: detecção de MIME
- HTML5: política de segurança de conteúdo ausente
- HTML5: política de segurança de conteúdo excessivamente permissiva
- HTML5: Política de CORS excessivamente permissiva
- HTML5: política de referência excessivamente permissiva
- Transporte inseguro: HSTS não inclui subdomínios
- Transporte inseguro: HSTS não definido
- Transporte inseguro: tempo de expiração de HSTS insuficiente
- Gerenciamento de senhas
- Gerenciamento de senhas: senha vazia
- Gerenciamento de senhas: Hardcoded Password
- Gerenciamento de senhas: senha nula
- Gerenciamento de senhas: criptografia fraca
- Privacy Violation
- Fixação de sessão
- Vazamento de informações do sistema

Além disso, são introduzidos os sete seguintes novos tipos de pontos fracos:

- HTML5: Proteção contra enquadramento ausente
- HTML5: Política de segurança de conteúdo não imposta
- Configuração incorreta do Spring: Permissão padrão
- Configuração incorreta do Spring: Cabeçalhos de Segurança desabilitados
- Configuração incorreta do Spring: Tipo de correspondência de solicitação incorreto
- Configuração incorreta do Spring: Ausência de verificação de fallback
- Configuração incorreta do Spring: Política de firewall excessivamente permissiva

## Spring Boot

O Spring Boot cria aplicativos do Spring autônomos e configura automaticamente as bibliotecas do Spring e de terceiros sempre que possível. Ele também fornece recursos prontos para produção, como métricas, verificações de integridade e configuração externa. Além das categorias com suporte anteriormente, esta atualização inclui suporte, até a versão 2.2.1, para as nove seguintes categorias adicionais:

- Segurança de cookies: HTTPOnly não definido no cookie de sessão
- Segurança de cookies: domínio de cookie de sessão excessivamente amplo
- Segurança de cookies: caminho de cookie de sessão excessivamente amplo
- Segurança de cookies: cookie de sessão persistente
- Segurança de cookies: cookie de sessão não enviado sobre SSL

- Gerenciamento de senhas: senha vazia em arquivo de configuração
- Transporte inseguro
- Transporte inseguro: verificação de identidade do servidor desabilitada
- Vazamento de informações do sistema: externo

Além disso, enquanto os Pacotes de regras anteriores davam suporte apenas a arquivos de configuração de Propriedades e ao sistema de compilação Maven, esta versão também inclui suporte para arquivos de configuração YAML e Gradle.

## Java 12[2]

Suporte para novas APIs no Java 12. Essas regras exigem o SCA versão 19.1 ou posterior, quando é usada a nova sintaxe do Java 12, como a nova instrução Switch.

## Biblioteca XML JSTL

A JSST (Standard Tag Library) do JSP (JavaServer Pages) é uma biblioteca que fornece uma maneira centrada em JSP de manipular e criar documentos XML. Agora o suporte inclui cobertura para as seguintes categorias do JSTL v1.1:

- Injeção de XSLT
- Injeção de entidade externa XML
- Privacy Violation
- Vazamento de informações do sistema: externo

## Melhorias no OpenXML SDK .NET

O suporte atualizado para o OpenXML SDK v2.9.0 inclui suporte para três categorias adicionais:

- Access Control: banco de dados
- Poluição de parâmetro da cadeia de conexão
- SQL Injection

## Suporte ao React-Router

O React Router é uma coleção de componentes de navegação compostos de forma declarativa com seu aplicativo. Se você deseja ter URLs que possam ser marcadas como favoritas para seu aplicativo Web ou uma maneira composta de navegar no React, o React Router funciona onde quer que o React esteja renderizando. As categorias com suporte no React-Router 5.1.2 incluem:

- Open Redirect
- Privacy Violation
- Vazamento de informações do sistema: externo

## 2019 CWE Top 25

O CWE (Common Weakness Enumeration) Top 25 mudou fundamentalmente a maneira como é determinado, em comparação com a época em que era conhecido como o SANS Top 25. Lançado em setembro, o novo Top 25 é determinado usando uma fórmula heurística que normaliza a frequência e a gravidade das vulnerabilidades relatadas ao NVD (National Vulnerability Database) nos últimos dois anos. Para dar suporte a nossos clientes que desejam priorizar suas auditorias em torno das vulnerabilidades críticas mais comumente relatadas no

[2] Requer o SCA v19.2.0 ou posterior.

NVD, foi adicionada uma correlação da Micro Focus Fortify Taxonomy à versão 2019 do CWE Top 25.

### DISA STIG 4.10

Para dar suporte a nossos clientes federais na área de conformidade, foi adicionada uma correlação do Micro Focus Fortify Taxonomy ao Application Security e ao Development STIG, versão 4.10, da DISA (Defense Information Systems Agency).

### Erratas diversas

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

- Consistência insegura de desserialização: Anteriormente, algumas regras sinalizavam apenas quando as informações vinham de um navegador. Isso foi corrigido para sinalizar em outros cenários possíveis.
- Referências de descrição verificadas: alguns dos materiais referenciados estavam desatualizados ou apontavam para links inválidos. Agora, essas instâncias foram corrigidas, e as referências apropriadas estão em seu lugar.

## Micro Focus 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

#### Práticas incorretas de SSO: Reprodução de token de autenticação

Os tokens de autenticação trocados durante um processo de logon único são suscetíveis a ataques de reprodução e podem permitir que um invasor represente um usuário válido para obter acesso não autorizado ao serviço. Esta versão inclui uma verificação que executa o ataque de reprodução para a estrutura de identidade do Windows e provedores de serviços usando o protocolo SAML.

#### Gerenciamento de cache: cabeçalhos

O cabeçalho de resposta HTTP Vary contém uma lista de cabeçalhos HTTP usados para decidir a resposta em cache correta para atender a uma solicitação recebida. A ausência de ‘Origin’ no cabeçalho Vary pode deixar o aplicativo aberto a ataques por envenenamento de cache no lado do cliente e do servidor, especialmente quando é feita uma solicitação entre origens. Esta versão inclui uma verificação para detectar quando há um cabeçalho 'Origin' ausente no valor do cabeçalho Vary.

### HTML5: Abuso de funcionalidade do CORS

Permitir solicitações do CORS de origens nulas, 'Origin: null' pode comprometer a segurança do sistema e deixar o aplicativo vulnerável ao roubo de dados. Esta versão inclui uma verificação para detectar a presença do valor 'null' no cabeçalho CORS Access-Control-Allow-Origin em uma resposta do servidor.

### Insecure Deployment: Contrabando de solicitação HTTP[3]

As vulnerabilidades de Contrabando de solicitação de HTTP surgem devido à discrepância na análise de cabeçalhos HTTP não compatíveis por servidores front-end e back-end. Fornecendo uma solicitação interpretada como sendo de diferentes comprimentos por servidores diferentes, um invasor pode envenenar o soquete TCP/TLS de back-end e anexar dados arbitrários à próxima solicitação ou contrabandear solicitações adicionais para o servidor de back-end sem que o servidor front-end esteja ciente disso. Esta versão inclui uma verificação para detectar essa vulnerabilidade.

### Header Manipulation[4]

A verificação de Header Manipulation existente foi aprimorada nesta versão para incluir ataques de retorno de carro ('CR') e avanço de linha ('LF'), além do ataque de CRLF existente.

## Relatório de conformidade

### DISA STIG 4.10

Para dar suporte a nossos clientes federais na área de conformidade, esta versão contém uma correlação das verificações do WebInspect com a versão mais recente do STIG de Segurança e Desenvolvimento de Aplicativos, versão 4.10, da Defense Information Systems Agency.

## Atualizações da política

### DISA STIG 4.10

Uma política personalizada para incluir verificações relevantes para o STIG 4.10 da DISA foi adicionada à lista existente de políticas com suporte no WebInspect SecureBase.

# Micro Focus Fortify Premium Content

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

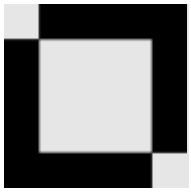
[3]Insecure Deployment: A verificação de Contrabando de solicitação HTTP requer o WebInspect v19.2.0 ou posterior.
[4] O aprimoramento de Header Manipulation requer o WebInspect v19.2.0 ou posterior.

## STIG 4.10 da DISA e 2019 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 o STIG 4.10 da DISA e o 2019 CWE Top 25, que está disponível para download no Portal de suporte ao cliente do Fortify, em Conteúdo premium.

## Micro Focus Fortify Taxonomy: Software Security Errors

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 do Micro Focus Fortify.



**Entre em contato com o suporte técnico do Fortify**
Micro Focus Fortify
https://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

**SSR de Contato**
Alexander M. Hoole
Gerente de Software Security Research
Micro Focus Fortify
hoole@microfocus.com
+1 (650) 258-5916



13 de dezembro de 2019