Micro Focus

de segurança de software do Micro Focus Fortify

Atualização 4 de 2018

14 de dezembro de 18

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 de software do Micro Focus Fortify oferece suporte a 992 categorias de vulnerabilidade em 25 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 o prazer de anunciar a disponibilidade imediata de atualizações para os Pacotes de regras de codificação segura do Fortify (idioma: inglês, versão 2018.4.0), do Fortify WebInspect SecureBase (disponível via SmartUpdate), do Fortify Application Defender e do Fortify Premium Content.

Micro Focus Fortify Secure Coding Rulepacks [SCA]

Nesta versão, os Pacotes de regras de codificação segura do Fortify detectam 789 categorias únicas de vulnerabilidades em 25 linguagens de programação e abrangem mais de um milhão de APIs individuais. Em resumo, a versão inclui o seguinte:

Melhorias no SQLite e no iOS

Suporte expandido para APIs SQLite nas linguagens Swift, Objective-C, C e C++. A cobertura abrange 16 categorias de vulnerabilidades existentes, incluindo SQL Injection, Access Control: Database e problemas relacionados ao gerenciamento de senhas e chaves. Deficiências de codificação relacionadas à interação com qualquer tipo de banco de dados podem resultar em vazamento de informações confidenciais, modificações não intencionais ou até mesmo perda de dados. Dessa forma, foram feitas melhorias adicionais no iOS relacionadas à privacidade, o que inclui a cobertura da categoria Privacy Violation: Heap Inspection para Swift.

Akka HTTP

Suporte para os módulos Scala Akka HTTP, um kit de ferramentas compatível com Reactive Streams baseado no Akka Streams, que implementa uma pilha HTTP completa nos lados do servidor e do cliente. A cobertura de categorias de vulnerabilidade abrange 22 tipos de deficiências existentes.

Melhorias no JAX-RS

Suporte revisado para a versão mais recente do JAX-RS e sua implementação Jersey de referência. Além de oferecer suporte a novos recursos adicionados na versão 2.1, este pacote de regras também inclui suporte para APIs no lado do cliente. As categorias de vulnerabilidades afetadas incluem Privacy Violation, Server-Side Request Forgery e System Information Leak. Além disso, uma nova categoria de deficiência foi adicionada a uma subcategoria especializada de Cross-Site Scripting causada quando respostas são enviadas usando tipos de conteúdo seguros para XSS. Nesse caso, indicaremos um problema de "Cross-Site Scripting: Content Sniffing", uma vez que navegadores específicos podem realizar "sniffing de conteúdo" e executar scripts na resposta.

Python six

Suporte para a biblioteca "six" do Python. O six é uma biblioteca de compatibilidade do Python que tem como objetivo oferecer suporte a bases de código compatíveis com o Python 2 e o Python 3 sem modificação. As categorias de vulnerabilidade com suporte incluem:

- Command Injection
- Dynamic Code Evaluation: Unsafe Pickle Deserialization
- Privacy Violation
- Server-Side Request Forgery
- System Information Leak: External
- Unsafe Reflection

DISA STIG 4.8

Para dar suporte aos nossos clientes federais na área de conformidade, foi adicionada uma correlação do Micro Focus Fortify Taxonomy ao Application Security e ao Development STIG, versão 4.8, da Defense Information Systems Agency (DISA).

PCI DSS 3.2.1

Para oferecer suporte aos nossos clientes de serviços financeiros e comércio eletrônico na área de conformidade, esta versão oferece suporte à correlação entre as categorias do Security Fortify Taxonomy e os requisitos especificados na versão mais recente do Payment Card Industry Data Security Standard, versão 3.2.1.

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

LDAP Injection

LDAP Injection é um ataque usado para explorar aplicativos baseados na Web que constroem instruções LDAP com base na entrada fornecida pelo usuário. Quando um aplicativo não consegue limpar corretamente a entrada fornecida pelo usuário, é possível modificar as instruções LDAP por meio de técnicas semelhantes às da SQL Injection. Ataques de LDAP Injection podem resultar no acesso não autorizado a dados confidenciais. Esta versão inclui uma verificação para identificar vulnerabilidades de LDAP Injection em aplicativos Web.

Open Redirect

Uma vulnerabilidade Open Redirect pode permitir que um invasor explore facilmente a confiança do usuário em sites conhecidos. De acordo com o comunicado ao fornecedor SA-CORE-2018-006, o Drupal 7 e 8 são vulneráveis a essa deficiência.

Drupal Destination Parameter Anonymous Open Redirect

No Drupal 8, a limpeza inadequada do valor do parâmetro "destination" pode ser explorada para acionar um redirecionamento aberto a uma URL mal-intencionada controlada pelo invasor. Esta versão inclui uma verificação para detectar essa vulnerabilidade.

Drupal Path Alias Open Redirect

No Drupal 7 e no Drupal 8, uma vulnerabilidade no Path Module permite que um invasor crie, edite e administre aliases de caminho que podem acionar um redirecionamento aberto a uma URL mal-intencionada controlada pelo invasor.

Access Control: Authorization Bypass

O JSON Web Token (JWT) é um padrão para criar um meio seguro para a URL de transferência de dados entre duas partes. As informações dentro do token são assinadas digitalmente usando o algoritmo HMAC ou RSA. No entanto, o padrão também permite o uso de "none" como o algoritmo de hash no JWT. Os servidores que

aceitam o código do JWT com "none" consideram todos os JWTs válidos, sem executar uma verificação na integridade dos dados. Isso pode ser explorado por usuários mal-intencionados para enviar dados arbitrários ao servidor. Isso pode resultar no acesso não autorizado e no comprometimento dos dados do sistema e do usuário. Esta versão inclui uma verificação para detectar a vulnerabilidade de bypass de autorização do algoritmo "none" do JWT.

Privacy Violation

JSON Web Tokens (JWTs) são usados para transferir dados entre duas partes. Dados confidenciais podem ser expostos a usuários não autorizados caso não sejam adequadamente criptografados. Esta versão inclui atualizações de verificações existentes que detectam a violação de privacidade relacionada à divulgação de números de cartão de crédito, à divulgação de números de previdência social e à detecção do armazenamento de informações confidenciais no repositório HTML5 no lado do cliente.

Dynamic Code Evaluation: Code Injection

O Spring Framework by Pivotal foi considerado vulnerável à vulnerabilidade de execução remota de código, conforme identificado pela CVE-2018-1270. A vulnerabilidade permite que um invasor envie mensagens mal-intencionadas para endpoints STOMP expostos sobre WebSocket, podendo resultar em execução remota de código. Esta versão contém uma verificação para detectar essa vulnerabilidade no Spring Framework. A verificação pode ser acessada por meio da política de WebSocket.

WebSocket Discovered

Esta versão inclui uma verificação informativa para indicar a presença de WebSockets no aplicativo verificado. Além disso, a verificação aciona um lembrete para nossos clientes considerarem verificar o aplicativo com a nova política de WebSocket que contém todas as verificações relevantes para as vulnerabilidades de WebSocket.

Relatório de conformidade

DISA STIG 4.8

Para dar suporte aos nossos clientes federais na área de conformidade, esta versão contém uma correlação das verificações do WebInspect com a versão mais recente do Application Security e do Development STIG, versão 4.8, da Defense Information Systems Agency.

PCI DSS 3.2.1

Esta versão inclui suporte para a versão mais recente do modelo de conformidade do Payment Card Industry Data Security Standard (DSS), versão 3.2.1.

Atualizações da política

DISA STIG 4.8

Uma política personalizada para incluir verificações relevantes ao DISA STIG 4.8 foi adicionada à lista existente de políticas com suporte no WebInspect SecureBase.

WebSocket

A nova política WebSocket realiza uma avaliação de segurança do aplicativo para vulnerabilidades relacionadas ao WebSocket.

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.

DISA STIG 4.8[1]

Para acompanhar as novas correlações, esta versão também contém um novo pacote de relatórios para o Fortify SSC com suporte para o STIG 4.8 da DISA, que está disponível para download no Portal de suporte ao cliente do Fortify, em Conteúdo premium.

PCI DSS 3.2.1[1]

Para acompanhar as novas correlações, esta versão também contém um novo pacote de relatórios para o Fortify SSC com suporte para o PCI DSS 3.2.1, que está disponível para download no Portal do 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 compatível podem acessá-lo no Portal de suporte do Micro Focus Fortify.

[1]O suporte para relatórios DISA STIG 4.8 e PCI DSS 3.2.1 requer o Fortify SSC versão 18.20 ou superior.

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

14 de dezembro de 2018