Micro Focus

Conteúdo de segurança do software Fortify

Atualização 2 de 2019

28 de junho 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 1.005 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 a satisfação de anunciar a disponibilidade imediata de atualizações para o Fortify Secure Coding Rulepacks (versão em inglês 2019.2.0), Fortify WebInspect SecureBase (disponível via SmartUpdate), Fortify Application Defender e Fortify Premium Content.

Micro Focus Fortify Secure Coding Rulepacks [SCA]

Nesta versão, os Pacotes de regras de codificação segura do Fortify detectam 799 categorias únicas de vulnerabilidades em 25 linguagens de programação e abrangem mais de um milhão de APIs individuais. Em resumo, essa versão inclui o seguinte:

Atualizações de .NET

Suporte para inclusões de API introduzidas no .NET Framework versões 4.7.1 e 4.7.2. As atualizações incluem suporte a regras para o .NET Standard 2.0 e o .NET Core 2.0, que abrangem as mesmas categorias que o .NET Framework. As regras para as versões atualizadas do .NET Framework incluem suporte aprimorado para as seguintes categorias:

- Header Manipulation: Cookies
- Insecure SSL: Server Identity Verification Disabled
- Insecure Transport: Weak SSL Protocol
- Weak Cryptographic Hash
- Weak Cryptographic Signature: Insufficient Key Size
- Weak Encryption

Realm Database

O Realm Database, um banco de dados leve de software livre projetado especificamente para aplicativos móveis, agora tem suporte no iOS (Swift e Objective-C) e no Android (Java). As categorias com suporte incluem o seguinte:

- Access Control: Database
- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key
- Path Manipulation

Além disso, há suporte para duas novas categorias:

- Insecure Storage: Missing Database Encryption
- NoSQL Injection: Realm

Python urllib3

Agora há suporte para a biblioteca Python urllib3, um cliente HTTP comumente usado e poderoso. A cobertura da categoria inclui o seguinte:

- Header Manipulation
- Insecure SSL: Server Identity Verification Disabled
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Server-Side Request Forgery

Atualizações do Java SE 10 e 11

A cobertura para Java SE foi estendida para as versões 10 e 11, incluindo suporte para a nova API do cliente HTTP.

Cross-Site Scripting: SOP Bypass

Suporte em JavaScript e TypeScript para a nova categoria "Cross-Site Scripting: SOP Bypass". Essa nova categoria abrange a situação específica em que uma falha permite que um invasor ignore a Same-Origin Policy (SOP) para ativar um ataque Cross-Site Scripting.

PCI SSF 1.0

Para apoiar os nossos clientes de comércio eletrônico e serviços financeiros na área de conformidade, esta versão oferece suporte à correlação entre nossas categorias do Micro Focus Fortify Taxonomy e os objetivos de controle especificados nos novos "Requisitos e procedimentos de avaliação de software seguro", definidos no Payment Card Industry (PCI) Secure Software Standard (SSS) como parte do novo Software Security Framework (SSF), versão 1.0. O novo padrão está definido para substituir o Data Security Standard (DSS) do PCI por novos envios de DSS do Payment Application (PA) que terminem em meados de 2020 e alterações no PA-DSS existente que expirem em 2022.

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 ver alterações nos problemas relatados relacionados ao seguinte:

Log Forging

Redução de falsos positivos, em todos os idiomas, devido ao reconhecimento mais preciso de APIs que removem novas linhas para evitar problemas de Log Forging e Log Forging (depuração).

Unreleased Resource: Database

Em Java, os algoritmos não identificaram corretamente que um ResultSet é fechado automaticamente se a instrução que o criou foi fechada primeiro. Os falsos positivos relacionados agora são eliminados.

Unsafe JNI and Unsafe JSNI

Os clientes que atualizaram para o SCA v19.1.x podem ter assistido a um surgimento de novos problemas "Unsafe JNI" e "Unsafe JSNI" em aplicativos Java. Isso foi devido a uma melhoria no mecanismo. Isso significava que muitas APIs estavam sendo sinalizadas que os clientes não têm controle sobre a correção. Isso agora foi corrigido para que o SCA sinalize apenas as APIs em que o usuário tem controle sobre a origem. Com essa redução nos problemas, os clientes também podem notar uma redução nos problemas de "Access Control: SecurityManager Bypass".

Dynamic Code Evaluation and Other Sinks on Lambdas

Em aplicativos JavaScript, poderiam ser gerados resultados confusos de um problema resultante de uma chamada lambda. Um exemplo comum disso foi com setTimeout(). Esses problemas irrelevantes agora são removidos e, embora haja alguns casos em que eles ainda possam ocorrer, estamos trabalhando ativamente para reduzir a frequência. Essa redução só pode ser observada ao se usar o SCA v18.20 ou posterior.

Cross-Site Scripting: Content Sniffing support

Antes, a SCA relatou problemas de Cross-Site Scripting em situações em que o tipo de conteúdo da resposta impedia que um navegador processasse o conteúdo HTML/JS (por exemplo, application/json). A razão para isso é que os usuários do aplicativo Web podem estar usando navegadores mais antigos que poderiam permitir um ataque de detecção de conteúdo. Com esta versão, modificamos esses problemas para serem relatados como “Cross-Site Scripting: Content Sniffing”. Isso permite que os auditores e desenvolvedores os reconheçam rapidamente e os distingam dos casos mais graves de Cross-Site Scripting. O Spring framework e o JAX-RS no Java Rulepacks oferecem suporte a essa nova categoria.

Lowering of Fortify Priority Order Based On Taint

Antes, o SCA relatava uma SQL Injection originada de um parâmetro de solicitação HTTP com a mesma gravidade que se fosse originada de uma variável do Ambiente do Sistema. Entendemos que a probabilidade de um invasor controlar variáveis do sistema é muito baixa ou, pelo menos, menor do que controlar um parâmetro de solicitação. Já estávamos reduzindo o valor do Fortify Priority Order de um problema com base nisso em determinados cenários. No entanto, a partir desta versão, o SCA aplicará de forma mais consistente a origem de contaminação como um novo fator ao calcular o valor do Fortify Priority Order de um problema.

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

Atualização do WebSocket[1]

Esta versão inclui aprimoramentos para detectar vulnerabilidades de vazamento de informações e desserialização não segura (para .NET) no tráfego do WebSocket. Especificamente, as seguintes categorias foram aprimoradas para oferecer suporte a WebSocket:

- Dynamic Code Evaluation: Unsafe Deserialization
- Poor Error Handling: Unhandled Exception
- Privacy Violation

[1] A atualização do WebSocket requer o WebInspect 19.1.0 ou posterior.

- Privacy Violation: Credit Card Number
- Privacy Violation: National ID Disclosure
- Privacy Violation: Social Security Number
- System Information Leak: Internal IP

Atualização da configuração de cabeçalhos de resposta segura

O servidor pode usar um conjunto de cabeçalhos de resposta HTTP para fornecer uma configuração do navegador que aumenta a segurança do aplicativo. Esses cabeçalhos são considerados como mecanismo de defesa em profundidade e, quando configurados, podem impedir adequadamente as vulnerabilidades. Esta versão inclui suporte aprimorado para os seguintes cabeçalhos e categorias relevantes:

- Cache-Control
  - Cache Management: Insecure Policy
- Content-Security-Policy
  - HTML5: Missing Content Security Policy
  - HTML5: Deprecated Content Security Policy
  - HTML5: Misconfigured Content Security Policy
- X-Content-Type-Options
  - Web Server Misconfiguration: Insecure Content-Type
- X-XSS-Protection
  - HTML5: Cross-Site Scripting Protection

Web Server Misconfiguration: Deprecated SSL/TLS Certificate

Todos os certificados SSL/TLS emitidos antes de 1º de dezembro de 2017 pela autoridade de certificação da Symantec (incluindo marcas de propriedade da Symantec como Thawte, VeriSign, Equifax, GeoTrust e RapidSSL) não são confiáveis e não são mais aceitos pelos principais navegadores, incluindo Chrome, Internet Explorer, Firefox e Safari. Esta versão inclui uma verificação para sinalizar o uso de certificados Symantec obsoletos.

Insecure Deployment: Unpatched Application

Uma vulnerabilidade crítica de execução remota de código no sistema de gerenciamento de conteúdo (CMS) do Drupal, identificado pelo CVE-2019-6340, permite que invasores remotos executem código arbitrário no servidor. Esta versão inclui uma verificação para detectar essa vulnerabilidade em aplicativos que implantam o Drupal CMS.

Relatório de conformidade

PCI SSF 1.0

Para apoiar nossos clientes na área de conformidade, esta versão inclui um novo modelo de conformidade que correlaciona o Micro Focus Fortify Taxonomy aos objetivos de controle especificados nos novos "Requisitos e procedimentos de avaliação de software seguro", definidos no Payment Card Industry (PCI) Secure Software Standard (SSS) como parte do novo Software Security Framework (SSF), versão 1.0. O novo padrão está definido para substituir o Data Security Standard (DSS) do PCI por

novos envios de DSS do Payment Application (PA) que terminem em meados de 2020 e alterações no PA-DSS existente que expirem em 2022.

Atualizações da política

PCI SSF 1.0

Foi adicionada uma política personalizada para incluir verificações relevantes ao PCI SSF 1.0 à lista existente de políticas com suporte no WebInspect SecureBase.

Erratas diversas

Cache Management: Insecure Policy

Foram feitos aprimoramentos para verificar a ID 11306 para excluir a sinalização de respostas HTML de tipos de conteúdo específicos que foram auditados com mais frequência como descobertas de falso positivo na verificação manual.

Expression Language Injection: Spring

Foi aprimorada a precisão do algoritmo de detecção de vulnerabilidade na verificação da ID 11579 do 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.

PCI SSF 1.0

Para acompanhar as novas correlações, esta versão também contém um novo pacote de relatórios para o Fortify SSC com suporte para PCI SSF 1.0, que está disponível para download no site Fortify Customer Portal em Premium Content.

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.

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

© Copyright 2019 Micro Focus ou uma de suas afiliadas. The information contained herein is subject to change without notice. The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

28 de junho de 2019