Micro Focus

Conteúdo de segurança do software Fortify

Atualização 1 de 2021

sexta-feira, 26 de março de 2021

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 1.038 categorias de vulnerabilidade em 27 linguagens de programação e se estende por mais de um milhão de APIs individuais.

Saiba mais em: https://software.microfocus.com/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 2021.1.0), o Fortify WebInspect SecureBase (disponível via SmartUpdate) e o Fortify Premium Content.

Micro Focus Fortify Secure Coding Rulepacks [SCA]

Nesta versão, os Pacotes de regras de codificação segura do Fortify detectam 816 categorias únicas de vulnerabilidades em 27 linguagens de programação e abrangem mais de um milhão de APIs individuais. Em resumo, essa versão inclui o seguinte:

Suporte a Micro Focus Visual COBOL (Versão 6)[1]

Esta versão adiciona suporte para Micro Focus Visual COBOL versão 6. Em particular, a versão inclui suporte para Micro Focus COBOL Runtime System (RTS) com suporte estendido para a categoria de manipulação de caminho já com suporte em COBOL e as seguintes categorias adicionais:

- Command Injection
- Memory Leak
- Memory Leak: Reallocation
- Unreleased Resource
- Unreleased Resource: Synchronization

Android 11

Como parte de um esforço contínuo para oferecer suporte à versão mais recente do Android (API versão 30), os seguintes namespaces são abrangidos:

- android.accounts
- android.app
- android.database
- android.database.sqlite

Os usuários devem esperar melhor modelagem de aplicativos Android que geralmente melhoram os resultados, juntamente com descobertas de *SQL Injection* e *Access Control: Database*.

Atualizações do iOS

Como parte de um esforço contínuo para melhorar o suporte ao iOS, novas regras Swift foram adicionadas para as seguintes classes:

- Foundation.NSCache
- Foundation.URLFileProtection

Os usuários devem esperar resultados aprimorados relacionados a Data Protection e Privacy Violation, juntamente com melhorias gerais em outros tipos de pontos fracos e estruturas (consulte "Erratas Diversas - correções de bugs do iOS").

Atualizações do Suporte ao Angular (versão 11.2.3)

Esta versão inclui nosso suporte ao Angular para 11.2.3. Em particular, foram identificadas novas fontes de informações controladas pelo usuário do navegador, o que pode levar ao acionamento de muitas categorias que não ocorriam antes.

[1] Requer SCA 21.1 ou posterior.

Atualizações do Apache Commons

O Apache Commons fornece componentes Java reutilizáveis. Nesta versão, o SSR atualizou o suporte para os seguintes componentes:

- beanutils (1.9.4)
- collections4 (4.4)
- dbutils (1.7)
- fileupload (1.4)
- lang (3.11)
- math (3.6.1)
- io (2.8.0)
- text (1.9)

Essas atualizações melhoram a modelagem de aplicativos que usam esses componentes, identificam proteções contra categorias como Log Forging e JSON Injection e também identificam novos locais em que os seguintes tipos de pontos fracos podem ocorrer:

- Access Control: Database
- Denial of Service
- Insecure Randomness: User-Controlled Seed
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- SQL Injection
- System Information Leak (variantes)

Python (Versão 3.9)

Suporte atualizado para a versão mais recente do Python, melhorando a modelagem das APIs de linguagem principal.

Erratas diversas

Nesta versão, continuamos a investir 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:

Melhorias referentes a falsos positivos:

Continuamos a ouvir nossos clientes e nos esforçamos para melhorar as taxas de falsos positivos. Durante este lançamento, trabalhamos no seguinte para reduzir o número de falsos positivos:

- *Code Correctness: Erroneous Class Compare* em aplicativos Java e Kotlin
- *Dynamic Code Evaluation:* Problemas de *Code Injection* removidos em verificações do Python 3
- Problemas de *Key Management* foram abordados para remover falsos positivos em todas as linguagens
- *Cross-Site Scripting:* Problemas de *DOM* relacionados a jQuery agora estão corretamente categorizados como *Cross-Site Scripting: Self* quando provenientes de uma caixa de entrada.
- Problemas de *Password Management* removidos nos arquivos de configuração ao fazer a correspondência de conteúdo que não pode ser uma senha
- Melhorias em falsos positivos de *Password Management* ao comparar com dados de localização.
- Descobertas de *XML External Entity Injections* removidas em funções irrelevantes em aplicativos Java Spring.
- *ASP.NET MVC Bad Practices: Controller Not Restricted to POST* agora permite verbos adicionais como seguros (PATCH, DELETE, PUT).

Correções de bugs do iOS:
Devido a melhorias na análise, foram necessárias atualizações de regras. Isso pode fazer com que os usuários observem melhorias nos seguintes tipos de pontos fracos:

- Interceptação de Entrada: Extensões de Teclado Permitidas
- Privacy Violation: HTTP Get
- Privacy Violation: Cache de Teclado
- Privacy Violation: Cache de Tela
- Privacy Violation: Shoulder Surfing

Vários frameworks também tiveram pequenas atualizações que melhoram a precisão: Foundation, UIKit, WebKit, HealthKit, WatchKit, MessageUI, CoreLocation, CoreData.

Categorias removidas:
A seguinte categoria foi removida neste lançamento para aumentar a relevância dos resultados:

- Privilege Management: Rede Android

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

OGNL Expression Injection: Struts 2

Vulnerabilidades críticas de Expression Language injection OGNL identificadas por CVE-2019-0231 e CVE-2020-17530 afetam as versões do Struts 2.0 a 2.5.25. A exploração dessas vulnerabilidades pode levar à execução remota de código arbitrário no servidor. Esta versão inclui uma verificação para detectar essas vulnerabilidades em aplicativos Web que usam o Struts 2.

Detecção de WAF[2]

Esta versão inclui uma verificação "Detecção WAF" que sinaliza descobertas informativas quando um Firewall de aplicativo Web é detectado durante uma verificação. Essas descobertas indicam que a qualidade da verificação pode ser comprometida porque as solicitações de verificação são bloqueadas antes de chegar ao aplicativo.

Hacker Level Insights[2]

Hacker Level Insights fornecem aos desenvolvedores e profissionais de segurança um contexto relacionado à postura geral de segurança de seu aplicativo. Esta versão inclui uma verificação que sinaliza as bibliotecas que foram detectadas no aplicativo durante a verificação. Embora essas descobertas não necessariamente representem uma vulnerabilidade de segurança, é importante observar que os invasores geralmente realizam o reconhecimento desses tipos de alvos na tentativa de identificar pontos fracos ou padrões conhecidos.

[2] Requer WebInspect 21.1 ou posterior.

Atualizações da política

NIST SP 800-53 Rev. 5

Uma política personalizada para incluir verificações relevantes para o NIST SP 800-53 Rev. 5 foi adicionada à lista de políticas com suporte do WebInspect SecureBase.

CWE Top 25 2020

Uma política personalizada para incluir verificações relevantes para CWE Top 25 2020 foi adicionada à lista WebInspect SecureBase de políticas com suporte.

DISA STIG 5.1

Uma política personalizada para incluir verificações relevantes para DISA STIG 5.1 foi adicionada à lista WebInspect SecureBase de políticas com suporte.

Erratas diversas

Nesta versão, continuamos a investir 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:

Envenenamento do web cache
Esta versão inclui uma verificação atualizada para *Web Cache Poisoning: Unkeyed Headers*. Agora os usuários podem adicionar cabeçalhos personalizados que eles suspeitam que façam parte da chave do cache.

SpringBoot Actuators não seguros
Esta versão inclui uma verificação atualizada para detecção de Spring Boot Actuator sigiloso disponível para usuários sem privilégios, o que fornece resultados mais precisos.

Melhorias de XSS
Esta versão inclui verificações de ataque XSS aprimoradas para Vue 3 e Angular JS 1.5.9 e superior.

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.

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

26 de março de 2021