Micro Focus

Conteúdo de Segurança de Software do Fortify

Atualização 4 de 2020

18 de dezembro de 2020

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 1.039 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 2020.4.0), 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 817 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 ao Dapper (Versão 2.0.78)

Suporte para o mapeamento objeto-relacional (ORM) do Dapper. O Dapper é usado para mapear a saída de consulta nativa para objetos C# fortemente tipados, estendendo a interface .NET IDdbConnection. O novo suporte trata o Dapper como uma fonte de dados controlados pelo usuário e também como um ativador para algumas categorias, tais como:

- Access Control: Database
- SQL Injection

Atualizações da biblioteca padrão Kotlin (versão 1.3)

Suporte estendido na biblioteca padrão Kotlin para incluir a cobertura dos seguintes pacotes:

- kotlin.concurrent
- kotlin.jvm
- kotlin.reflect
- kotlin.system

XML Pull (versão 1)

Suporte para implementação do pacote XML Pull no Android. O XML Pull é uma API de streaming simples usada para analisar e serializar arquivos XML nos quais o aplicativo controla a análise (pode ser interrompida e retomada). As categorias com suporte incluem:

- XML Entity Expansion Injection
- XML Injection

AIOPG (versão 1.0.0)[1]

Suporte à biblioteca aiopg do Python. O aiopg fornece uma maneira assíncrona de conexão com bancos de dados PostgreSQL. As categorias com suporte incluem:

- Access Control: Database
- Gerenciamento de senhas
- Gerenciamento de senhas: Empty Password
- Gerenciamento de senhas: Hardcoded Password
- Gerenciamento de senhas: Null Password
- Gerenciamento de senhas: Weak Cryptography
- SQL Injection

[1] A detecção completa de problemas relacionados a aiopg depende de uma melhoria futura para SCA relacionada com ‘async with’.

JavaScript Promises

- O suporte para JavaScript Promises foi aprimorado para análise de fluxo de dados.

Modelos do Azure Resource Management

Suporte inicial para os modelos do Azure Resource Management (ARM). Os modelos do ARM são usados para implementar infraestrutura como código para soluções Azure. Os modelos ARM são arquivos JSON que utilizam uma sintaxe declarativa para definir e configurar o projeto de um usuário. As categorias com suporte incluem:

- Configuração incorreta do Azure Resource Manager: HTTPS não exigida
- Configuração incorreta do Azure Resource Manager: Acesso público permitido

DISA STIG 5.1

Para dar suporte a nossos clientes governamentais na área de conformidade, foi adicionada uma correlação do Micro Focus Fortify Taxonomy com o Application Security and Development STIG, versão 5.1, da DISA (Defense Information Systems Agency).

NIST SP 800-53 Rev. 5

Para apoiar nossos clientes governamentais na área de conformidade, uma correlação do Micro Focus Fortify Taxonomy com os controles de segurança e privacidade na versão mais recente da Publicação Especial (SP) 800-53 Revisão 5 do National Institute of Standards and Technology (NIST) foi adicionada. Trinta controles de base estão cobertos, abrangendo as seguintes famílias de controle:

- Controle de Acesso (Access Control – AC)
- Auditoria e Responsabilização (Audit and Accountability – AU)
- Avaliação, Autorização e Monitoramento (Assessment, Authorization and Monitoring – CA)
- Gerenciamento de Configuração (Configuration Management – CM)
- Identificação e Autenticação (Identification and Authentication – IA)
- PII Processamento e Transparência (PII Processing and Transparency – PT)
- Proteção de Sistemas e Comunicações (System and Communications Protection – SC)
- Integridade de Sistemas e Informações (System and Information Integrity – SI)

2020 Common Weakness Enumeration (CWE™) Top 25

O Common Weakness Enumeration (CWE™) Top 25 foi introduzido em 2019 e substitui o SANS Top 25. Lançado em agosto, o 2020 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. 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 Micro Focus Fortify Taxonomy com o 2020 CWE Top 25.

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:

Suspensão de uso de SCA anteriores à versão 17.x

Como mencionado em nosso anúncio da versão 2020.3, aquele seria o último lançamento de Rulepacks compatíveis com SCA anteriores à versão 17.x. Neste lançamento, SCA anteriores à versão 17.x não vão mais carregar os Rulepacks mais recentes. Os clientes que usam SCA anteriores à versão 17.x devem fazer downgrade dos Rulepacks ou atualizar a versão SCA.

Em versões futuras, vamos oferecer suporte para as últimas quatro versões principais do SCA.

Obsolescência de mapeamentos

A equipe de Pesquisa de Segurança de Software continuou criando mapeamentos de categorias do Fortify para padrões externos e práticas recomendadas ao longo dos anos. Com isso, chegamos ao ponto em que as versões dos diferentes padrões suportados ficaram muito grandes, sendo que muitas versões antigas não são mais usadas.

Sendo assim, marcamos agora os seguintes padrões como “obsoletos”:

- Padrão de segurança de dados do setor de cartões de pagamento (PCI) 1.1
- Padrão de segurança de dados do setor de cartões de pagamento (PCI) 1.2
- Padrão de segurança de dados do setor de cartões de pagamento (PCI) 2.0
- Padrão de segurança de dados do setor de cartões de pagamento (PCI) 3.0
- Padrão de segurança de dados do setor de cartões de pagamento (PCI) 3.1
- Padrão de segurança de dados do setor de cartões de pagamento (PCI) 3.2
- Guia de implementação técnica de segurança (STIG) 4.1
- Guia de implementação técnica de segurança (STIG) 4.2
- Guia de implementação técnica de segurança (STIG) 4.3
- Guia de implementação técnica de segurança (STIG) 4.4
- Guia de implementação técnica de segurança (STIG) 4.5
- Guia de implementação técnica de segurança (STIG) 4.6
- Guia de implementação técnica de segurança (STIG) 4.7
- Guia de implementação técnica de segurança (STIG) 4.8

Essa mudança significa que os aplicativos Fortify e SCA, a partir da versão 20.2, não exibirão mais esses mapeamentos antigos por padrão.

Se houver necessidade de verificar a conformidade dessas versões antigas, você deve alterar os mapeamentos para definir o atributo *obsoleto* como “falso” ou remover o atributo inteiramente.

Melhorias nos 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:

- Removemos os falsos positivos de adulteração de verbo HTTP (Verb Tampering) quando a proteção está presente nos arquivos de configuração
- Removemos os falsos positivos de Mass Assignment ao usar o atributo JSONIGNORE no .NET
- Removemos o Insecure Storage: Falsos positivos de HTTP Response Cache Leak quando os caches são explicitamente desativados nos objetos URLSessionConfiguration
- Removemos a Swift Privacy Violation: Falsos positivos de HTTP GET de URLRequest
- Prática deficiente de registro em log: Uso das duplicatas de um fluxo de saída do sistema removido no Python
- Problemas de Unreleased Resource removidos ao usar variantes adicionais do Apache Commons closeQuietly

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

Assinatura de criptografia fraca: Chave secreta previsível

A integridade do payload do JSON Web Token geralmente é garantida por meio de assinaturas HMAC. No entanto, se o algoritmo HMAC usa um segredo fraco, um usuário mal-intencionado pode obter a chave secreta por força bruta e assinar novamente o JWT com qualquer payload. Esta versão inclui uma verificação para identificar se uma string de segredos comumente usados é usada para assinar o token JWT.

Gerenciamento de senhas: Política de senha fraca

Políticas de senha que garantam que os usuários criem senhas fortes são cruciais para implantar sites seguros. As senhas devem ser validadas para garantir que não sejam uma das senhas comumente usadas e uma string de senha deve atender às diretrizes definidas pelo NIST 800-53, NIST 800118 e OWASP. Esta versão inclui uma nova verificação para detectar se a senha configurada na macro de login corresponde a uma das senhas comumente usadas. A versão também inclui uma atualização para verificações da política de senha fraca para atender às diretrizes revisadas sobre a força da senha, conforme definido nos padrões NIST mencionados acima e nas diretrizes OWASP.

Gerenciamento de cache: Envenenamento do web cache

Os web caches armazenam uma cópia da página quando o usuário visita um site pela primeira vez. Na próxima vez que o usuário visitar a mesma página, uma cópia em cache será exibida para ele. No entanto, se esses web caches tiverem falhas de implementação ou de projeto, como aceitar solicitações GET com o corpo da solicitação (por exemplo, solicitações de fat GET ou entradas sem chave), elas ficam suscetíveis ao envenenamento do web cache. O envenenamento do web cache é uma técnica avançada usada por invasores para armazenar em cache respostas mal-intencionadas para solicitações legítimas de usuários. Esta versão inclui verificações para identificar se um site é vulnerável a envenenamento de web cache por meio de cabeçalhos sem chave e solicitações de fat GET.

Relatórios de conformidade

DISA STIG 5.1

Para apoiar nossos clientes governamentais na área de conformidade, este lançamento contém uma correlação das verificações do WebInspect com a versão mais recente da Segurança e Desenvolvimento de Aplicativos da Agência de Sistemas de Informação de Defesa (DISA STIG 5.1).

NIST SP 800-53 Rev. 5

Para apoiar nossos clientes governamentais na área de conformidade, este lançamento contém uma correlação das verificações do WebInspect com os controles na versão mais recente do National Institute of Standards and Technology (NIST), Publicação Especial (SP) 800-53, revisão 5.

2020 Common Weakness Enumeration (CWE™) Top 25

O Common Weakness Enumeration (CWE™) Top 25 foi introduzido em 2019 e substitui o SANS Top 25. Lançado em agosto, o 2020 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. Esta atualização do SecureBase inclui mapeamentos para as categorias CWE. Incluímos 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”.

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:

- A verificação de contrabando de solicitações HTTP foi reprojetada para reduzir falsos positivos, aumentar a eficiência e melhorar a precisão de seus resultados. A verificação

da ID 11621 não usa mais uma abordagem baseada no tempo para verificação de vulnerabilidade.

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 5.1, NIST SP 800-53 Rev. 5 e 2020 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 5.1 da DISA, o NIST SP 800-53 Rev. 5 e o 2020 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

18 de dezembro de 2020