Micro Focus

Conteúdo de segurança do software Fortify

Atualização 2 de 2020

sexta-feira, 26 de junho 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 1.022 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/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 2020.2.0), 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 810 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 para a biblioteca central Kotlin (versão 1.3)[1]

Suporte inicial para bibliotecas padrão Kotlin cobrindo os seguintes pacotes direcionados à JVM:

- Kotlin
- kotlin.collections
- kotlin.comparisons
- kotlin.io
- kotlin.properties
- kotlin.random
- kotlin.ranges
- kotlin.sequences
- kotlin.streams
- kotlin.text

A interoperabilidade limitada com Java implica que todas as categorias e bibliotecas compatíveis com Java são parcialmente compatíveis com Kotlin, bem como as seguintes compatíveis especificamente com as bibliotecas padrão Kotlin:

- Cross-Site Scripting: Comunicação entre componentes
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Negação de serviço: Regular Expression
- Negação de serviço: StringBuilder
- Formula Injection
- Insecure SSL: certificados totalmente confiáveis
- Falsificação de Log
- Path Manipulation
- Prática deficiente de registro em log: Uso de um fluxo de saída do sistema
- Privacy Violation
- Server-Side Request Forgery
- Vazamento de informações do sistema
- Vazamento de informações do sistema: External
- Vazamento de informações do sistema: interno
- Violação de Limite de Confiança
- Valor de retorno não verificado

[1] Exige liberação do patch SCA 20.1.2. Usar o SCA 20.1 resultará em vários erros relacionados a regras e funções lambda específicas, que não ocorrem com o lançamento do patch.

Melhorias em C# 8 e .NET Core

Suporte atualizado para as bibliotecas C# 8 e .NET Core, incluindo as versões 2.1, 2.2, 3.0 e 3.1. Com ele surge o suporte completo de regras para .NET Standard 2.1, assim como fluxo de dados aprimorado ao usar operações assíncronas de *foreach*, *range* e *using* de C# 8.

Melhorias na biblioteca central do Python[2]

Suporte atualizado para as bibliotecas centrais do Python, incluindo as versões 3.7 e 3.8. Além das categorias suportadas anteriormente, a seguinte nova categoria agora é suportada:

- Práticas incorretas de Python: Leftover Debug Code

Melhorias no suporte da biblioteca central Go (versão 1.13)

Suporte expandido para bibliotecas centrais Go para cobrir crypto/tls. Go é uma linguagem de software livre estaticamente tipada projetada pelo Google™ para 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. As categorias com suporte incluem:

- Insecure SSL: Server Identity Verification Disabled
- Path Manipulation
- Privacy Violation
- Server-Side Request Forgery
- Setting Manipulation
- Vazamento de informações do sistema: External

GORM (versão 1.9.12)

Suporte para a biblioteca GORM, que é um projeto de Mapeamento objeto-relacional (ORM) de código aberto para Golang escrito por Jinzhu. GORM é uma biblioteca ORM comum que pode apresentar riscos relacionados ao banco de dados para aplicativos corporativos. As categorias com suporte incluem:

- Access Control: Database
- Poluição de parâmetro da cadeia de conexão
- Dynamic Code Evaluation: Code Injection
- Transporte inseguro
- Falsificação de Log
- Gerenciamento de senhas: Empty Password
- Gerenciamento de senhas: Hardcoded Password
- Gerenciamento de senhas: Weak Cryptography
- Privacy Violation
- Setting Manipulation
- SQL Injection
- Vazamento de informações do sistema: interno
- Weak Cryptographic Hash

[2] Exige SCA 20.2 para resultados aprimorados quando os projetos incluem sintaxe recém-introduzida, como expressões de atribuição.

OWASP ASVS 4.0

Para apoiar nossos clientes que buscam estruturas para ajudar a executar seu programa appsec, esta versão oferece suporte à correlação entre nossas categorias de taxonomia Micro Focus Fortify Taxonomy e os requisitos do OWASP Application Security Verification Standard, versão 4.0. O ASVS fornece uma lista de requisitos, ou testes, que os clientes podem usar para ajudar na definição, criação, teste e verificação de aplicativos seguros.

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:

Mudanças no reino:
Em alguns lugares selecionados, o reino para categorias específicas foi alterado para obter consistência. Em versões mais antigas do SCA (versões inferiores a 6.30, ou seja, qualquer versão anterior a 17/04/2015), isso pode fazer com que alguns problemas sejam tratados como novos/removidos durante a fusão, em vez de permanecerem como “atualizados”. Esse problema não ocorrerá em qualquer versão do SCA 6.30 ou superior.
Em geral, isso também pode afetar a filtragem, caso os usuários estiverem filtrando por reino. As categorias afetadas incluem:

- Access Control: Manipulação do ACL. Alterado de “Validação e representação de entrada” para “Recursos de segurança”
- Access Control: Authorization Bypass. Alterado de “Validação e representação de entrada” para “Recursos de segurança”
- Vazamento de informações do sistema: Struts 2. Alterado de “Validação e representação de entrada” para “Encapsulamento”

Melhorias de 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 uma regra de origem JavaScript específica que estava causando falsos positivos em várias categorias.
- Regras Java “Recurso inédito: banco de dados” foram aprimoradas para contabilizar conexões fechando recursos subjacentes de acordo com a especificação JDBC 4.3.
- Foram removidos problemas de “Manipulação de caminho” de falso positivo em Java em torno de File.createTempFile().
- O relatório de problemas dos arquivos de definição do TypeScript foi desativado.
- Alguns falsos positivos do .NET “Server-Side Request Forgery” foram removidos do SendAsync.
- Falsos positivos do Java “Configuração incorreta do Spring Security: tipo de correspondência de solicitação incorreta” foram reduzidos.
- Problemas duplicados de “criptografia fraca” do .NET foram removidos.
- Falsos positivos da .NET “Práticas incorretas de ASP.NET: objeto não serializável armazenado na sessão” foram removidos dos tipos String.
- Os falsos positivos Golang removidos eram resultantes de contaminação não intencional de objetos net.http.Response.

- Foram identificados e removidos falsos positivos raros de “Correção do código: a classe não implementa iguais a” no Java.
- No JavaScript, muitos problemas de “gerenciamento de chaves” falsos positivos foram removidos e o progresso será continuado em versões posteriores.

Erros e avisos:
Com o SCA 19.2, para qualquer linguagem de programação suportada, o carregamento de regra durante uma varredura resultará no seguinte aviso produzido nos registros de criação e varredura quando combinado com o conjunto completo de pacotes de regras 2020.2.0:

```
[WARN  20599]
A linguagem de regras kotlin não possui mapeamento correspondente
em SCA
```

Este é um problema conhecido no SCA 19.2 que pode ser contornado removendo o seguinte arquivo do pacote de regras Kotlin:

<*FORTIFY_DIR*>\Fortify_SCA_and_Apps_19.2.0\Core\config\rules\core_kotlin.bin

A digitalização de Kotlin exige SCA 20.1.2.

Melhorias VulnCat
Melhoramos a classificação das categorias de filtro, bem como as subcategorias de filtro, para que as entradas sejam exibidas em uma ordem lógica.

Suporte de validação ESAPI
Ouvimos nossos clientes e muitos estão preocupados com as regras SCA que permitem que as APIs de ESAPI eliminem os problemas conforme eles são corrigidos, devido a questões de segurança na biblioteca.
Nesta versão, removemos a validação das bibliotecas ESAPI e agora o fluxo de dados continuará por meio das funções de codificação sem evitar o aparecimento de problemas de fluxo de dados.
Como sabemos que alguns clientes gostariam de continuar usando a biblioteca ESAPI especificamente para produtos legados, estamos disponibilizando um pacote de regras separado para incluir novamente essa validação.

Se desejar continuar usando ESAPI, você pode usar nosso pacote de regras de extensão ESAPI que pode ser encontrado no Portal de suporte em Conteúdo Premium, Fortify Exchange.

Observe que esta atualização também elimina todos os problemas sinalizados como “Obsoletos: preteridos por ESAPI”, que podem ser encontrados usando o pacote separado de regras mencionado acima.

Atualização de criptografia fraca
3DES, também conhecido oficialmente como algoritmo de criptografia de dados triplos (TDEA), agora será relatado sob criptografia fraca, seguindo as recomendações do National Institute of Standards and Technology (NIST) .

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

Web Server Misconfiguration: Divulgação de informações

Spring Boot inclui uma série de recursos adicionais, também conhecidos como atuadores, que permitem aos administradores monitorar e gerenciar seus aplicativos da Web. Esta versão inclui uma verificação para detectar Spring Boot Actuator confidencial disponível para usuários sem privilégios. Ao usar esses pontos de extremidade do atuador, um invasor pode reunir informações de auditoria, integridade e métricas ou até mesmo executar um ataque de execução remota de código em algumas configurações.

Cross-Site Scripting: Reflected

ResolveUrl da API ASP.NET é usado para resolver o caminho relativo à raiz do aplicativo em tempo de execução. A API não consegue validar o caminho relativo que inclui valores formatados de ID de estado sem cookies e permite que o invasor conduza um ataque de Cross-Site Scripting no aplicativo. Esta versão inclui uma verificação para detectar essa vulnerabilidade nos aplicativos .NET.

Segurança de cookies: Atributo SameSite ausente

O atributo SameSite em cookies fornece um mecanismo simples para proteger aplicativos contra ataques de Cross-Site Request Forgery. As versões recentes do navegador podem rejeitar cookies que não definem o atributo SameSite. Esta versão inclui uma verificação para detectar instâncias de cookies definidas que falham ao definir o atributo SameSite.

Segurança de cookies: Prefixo mal configurado

Cookies com nome prefixado com _Host- or_Secure- impõem restrições de nível de host e que o cookie seja enviado apenas em uma conexão HTTPS segura para protegê-los contra espionagem acidental e spoofing. Os cookies que não configuram adequadamente o caminho, o domínio e o atributo seguro podem ser rejeitados pelo navegador. Uma verificação para detectar o cookie prefixado mal configurado está incluída nesta versão.

Segurança de cookies: Atributo SameSite excessivamente permissivo

O valor estrito para o atributo SameSite em cookies impõe aos navegadores apenas anexar o cookie às solicitações que resultaram devido à navegação de nível superior para o domínio ou quando o mesmo host estiver fazendo a solicitação de várias tags HTML com link, como iframe, link e formulário, etc. Os IDs de sessão devem ser definidos com o valor Strict para o atributo SameSite para fornecer proteção máxima ao aplicativo contra ataques de Cross-Site Request Forgery. Esta versão inclui uma verificação para detectar a instância quando o atributo SameSite não está definido como Strict para cookies de sessão.

Relatório de conformidade

OWASP Application Security Verification Standard (ASVS)

A ASVS do OWASP fornece uma metodologia para testar aplicativos da Web para controles de segurança e também fornece diretrizes de desenvolvimento seguro. Esta versão contém uma correlação das verificações do WebInspect com a versão mais recente do OWASP ASVS 4.0.

Atualizações da política

Política do OWASP Application Security Verification Standard (ASVS)

Além da correlação das verificações do WebInspect com a versão mais recente do ASVS do OWASP, esta versão também inclui uma política para identificar vulnerabilidades que levam à correlação com o ASVS do OWASP.

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 no conteúdo de segurança para uso frequentemente indevido: o certificado SSL fraco agora reflete com mais precisão as informações sobre os motivos pelos quais um certificado é considerado fraco. Foi adicionada uma nova verificação com ID 11635.

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.

OWASP Application Security Verification Standard (ASVS):

O Application Security Verification Standard (ASVS) é uma lista de requisitos de segurança de aplicativos e testes a serem executados durante um ciclo de vida de desenvolvimento de software (SDLC) e de configuração para construir um software seguro. Prevemos que esse mapeamento continuará a evoluir à medida que colaboramos com parceiros do setor para melhorar a forma como os mapeamentos são projetados. Para acompanhar as novas correlações, esta versão também contém um novo pacote de relatórios para o Fortify SSC com suporte para OWASP ASVS 4.0, 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 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 junho de 2020