Conteúdo de segurança de software do Fortify

Atualização 3 de 2021
24 de setembro de 2021

Sobre o CyberRes Fortify Software Security Research

A equipe do Fortify Software Security Research transforma pesquisas de ponta nas tecnologias de segurança que estão por trás dos produtos Fortify — incluindo o Fortify Static Code Analyzer, o Fortify WebInspect e o Fortify Application Defender. Atualmente, o conteúdo de segurança de software do CyberRes Fortify oferece suporte a 1.051 categorias de vulnerabilidade em 27 linguagens de programação e se estende por mais de um milhão de APIs individuais.

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 2021.3.0), o Fortify WebInspect SecureBase (disponível por SmartUpdate) e o Fortify Premium Content.

CyberRes Fortify Secure Coding Rulepacks [Static Code Analyzer]

Nesta versão, o Fortify Secure Coding Rulepacks detecta 831 categorias únicas de vulnerabilidades em 27 linguagens de programação e se estende por mais de um milhão de APIs individuais. Em resumo, esta versão inclui o seguinte:

Atualizações para biblioteca padrão de Golang (versão: 1.16)

Suporte estendido para a biblioteca padrão de Go. Go é uma linguagem de código aberto estaticamente tipada, projetada pelo Google para facilitar a criação de softwares simples, confiáveis e eficientes. O Go é sintaticamente semelhante ao C, mas conta com mecanismos de segurança de memória, coleta de lixo e tipagem estrutural. Esta atualização abrange os namespaces da biblioteca padrão e oferece suporte para as novas categorias a seguir:

- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute
- Go Bad Practices: Leftover Debug Code
- Insecure Randomness: Hardcoded Seed
- Insecure Randomness: User-Controlled Seed
- Insecure Transport: Cipher Suite Downgrade
- Insecure Transport: Weak SSL Protocol
- Often Misused: Privilege Management
- Weak Cryptographic Signature

Atualizações para Android 11 (nível da API: 30)

A plataforma Android é um conjunto de tecnologias de código aberto, projetada para dispositivos móveis. Um dos principais componentes do Android é o Java API Framework, que disponibiliza os recursos do Android aos desenvolvedores. Esta versão amplia a detecção de vulnerabilidades em aplicativos nativos de Android programados em Java ou Kotlin que utilizam o Java API Framework. Os usuários podem esperar melhores resultados com as atualizações para modelagem de aplicativos e cobertura de APIs para Android. Esta versão também inclui as novas categorias de vulnerabilidades de gestão de privilégios a seguir, que ajudam a administrar permissões perigosas para Android:

- Privilege Management: Android Activity Recognition
- Privilege Management: Android Calendar
- Privilege Management: Android Call Log
- Privilege Management: Android Camera
- Privilege Management: Android Contacts
- Privilege Management: Android Microphone
- Privilege Management: Android Sensors

Atualizações para a biblioteca padrão de iOS (versão: iOS 14)

Esta versão atualiza nosso suporte para as APIs da biblioteca do iOS 14, tanto para Swift quanto para Objective-C. As atualizações focam-se nos seguintes frameworks:

- UIKit
- UserNotification
- SwiftUI
- MessageUI

Os usuários deverão ver melhorias nas categorias Insecure IPC, Link Injection, Path Manipulation, Privacy Violation, Shoulder Surfing e System Information Leak.

Atualizações para Micro Focus Visual COBOL (versão: 7.0)

Suporte ampliado para Micro Focus Visual COBOL versão 7, incluindo as duas categorias de vulnerabilidades a seguir:

- Integer Overflow
- Race Condition: File System Access

Suporte para SAPUI5/OpenUI5[1] (versão: 1.93)

SAPUI5 é um framework de JavaScript do lado do cliente, criado pela SAP, que compartilha um conjunto de bibliotecas de controle centrais com o framework de código aberto OpenUI5. Esta versão fornece suporte inicial de identificação de vulnerabilidades para as seguintes categorias:

- Cross-Site Scripting: DOM
- Cross-Site Scripting: SAPUI5 Control
- Cross-Site Scripting: Self
- Privacy Violation
- SAPUI5 Misconfiguration: Unsanitized Editor
- System Information Leak: External

Suporte para JSON[2]

JavaScript Object Notation (JSON) é um formato leve de troca de dados. Esta versão fornece suporte aprimorado para a identificação de vulnerabilidades em JSON para as seguintes categorias:

- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Password in Comment[3]

[1] Resultados potencialmente aprimorados ao usar o Static Code Analyzer v21.2.0 ou superior.
[2] Requer o Static Code Analyzer v21.1.0 e a flag: '-Dcom.fortify.sca.use.json-analyzer=true'.
[3] Requer Static Code Analyzer v21.2.0 ou superior. Não é necessário usar flags no Static Code Analyzer v21.2.0 e superiores.

Atualizações para a biblioteca padrão de Kotlin (versão: 1.4.30)

Kotlin é uma linguagem de programação de uso geral e estaticamente tipada, que conta com interoperabilidade com Java. Esta versão inclui suporte atualizado para novas APIs da biblioteca padrão introduzidas no Kotlin 1.4, relacionadas com a Java Virtual Machine (JVM).

ECMAScript 2021 (versão: ECMA-262)

Suporte para novas APIs introduzidas no ECMAScript 2021. ECMAScript é uma linguagem de programação de uso geral, definida pela especificação da linguagem de programação ECMAScript e conhecida por ser integrada em todos os navegadores web modernos. Entretanto ela é cada vez mais usada no desenvolvimento de servidores web, aplicativos móveis e outras formas de softwares convencionais. Os clientes podem esperar um fluxo de dados aprimorado ao fazer a verificação de aplicativos conforme o padrão ECMAScript mais recente.

2021 Common Weakness Enumeration (CWE™) Top 25

O Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) foi introduzido em 2019 em substituição ao SANS Top 25. Lançado em julho, o 2021 CWE Top 25 foi 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 relatadas com mais frequência no NVD, adicionamos uma correlação do CyberRes Fortify Taxonomy com o 2021 CWE Top 25.

Erratas diversas

Nesta versão, continuamos a investir recursos para garantir que possamos reduzir o número de problemas de falso-positivos e melhorar a capacidade dos clientes de auditar problemas. Os clientes também podem esperar alterações nos problemas relatados relacionadas com o que segue:

Suspensão de uso do Static Code Analyzer em versões anteriores à versão 18.x:

Conforme mencionado no lançamento da versão 2020.4, continuamos a oferecer suporte para as últimas quatro versões principais do Static Code Analyzer. Assim, esta será a última versão do Rulepacks compatível com o Static Code Analyzer em versões anteriores à versão 18.x. No próximo lançamento, o Static Code Analyzer em versões anteriores à versão 18.x não carregarão o Rulepacks mais recente. Será necessário fazer o downgrade do Rulepacks ou o upgrade do Static Code Analyzer.
Em versões futuras, continuaremos a oferecer suporte para as últimas quatro versões

principais do Static Code Analyzer.

Aprimoramentos para Java J2EE:

Suporte aprimorado para APIs do javax.servlet nas categorias *Privacy Violation* e *System Information*

Leak. ***Android Bound Services:***

Em atenção ao nosso suporte contínuo para Android, esta versão inclui cobertura para o Android Bound Services. Os clientes podem esperar novos problemas de fluxo de dados com origem nos parâmetros de métodos do Android Bound Services. Isto pode introduzir subtraços de fluxo de dados duplicados quando os métodos são chamados de dentro do serviço vinculado.

Hash de criptografia fraca no Node.js:

Identificação de usos de hashes de criptografia fraca em aplicativos Node.js.

O mapeamento do OWASP ASVS 4.0 agora oferece suporte para níveis

Em apoio aos clientes que queiram fazer consultas relacionadas com problemas que violem os níveis de verificação de segurança de aplicativos (L1, L2 e L3) do OWASP Application Security Verification Standard (ASVS), a última atualização de segurança adicionou esses níveis aos nomes de mapeamento. Agora, os clientes podem pesquisar dentro do agrupamento do *OWASP ASVS 4.0* as palavras-chave relacionadas de L1, L2 e L3, bem como projetar conjuntos e modelos de filtros relacionados para usar no AuditWorkbench e no Software Security Center (SSC).

Melhorias referentes a falso-positivos:

Remoção de outros falso-positivos nesta versão. Além de outras melhorias, os clientes podem esperar ver a remoção de certos falso-positivos nas seguintes áreas:

- Falso-positivos de *Cross-Site Scripting* em códigos jQuery
- *Privacy Violation: Shoulder Surfing* em aplicativos .NET usando o atributo JsonIgnore
- Mais consistência ao reduzir o Fortify Priority Order em problemas de *Path Manipulation* nos quais somente um número pode ser controlado
- Não mais identificamos senhas em Swift quando elas fazem parte de uma enumeração
- Problemas de *Missing XML Validation* em .NET
- *Missing Check against Null* em projetos Java

CyberRes 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

Insecure Deployment: HTTP Request Smuggling

O contrabando de HTTP2 por texto claro, ou h2c smuggling, é uma alternativa ao contrabando convencional de solicitações HTTP, a qual se aproveita de front-ends vulneráveis, como servidores proxy, para criar um túnel que leva aos sistemas back-end. Um invasor pode usar esse túnel para contrabandear solicitações adicionais para o servidor back-end sem ser detectado pelo servidor front-end. Assim, ele poderá contornar controles de autorização de front-end e acessar recursos restritos em sistemas back-end. Esta versão inclui uma verificação para detectar configurações que podem ser usadas em ataques de h2c smuggling.

Access Control: Missing Authorization Check

A introspecção do GraphQL permite enviar consultas ao servidor para obter informações sobre um esquema subjacente. Ela fornece detalhes sobre elementos como consultas, tipos e campos. Em geral, a introspecção do GraphQL está habilitada por padrão. Um invasor que não tenha a devida autorização pode aproveitar-se dessas informações para executar ataques como SQL Injection e ataques por lotes. Esta versão inclui uma verificação para detectar os endpoints do GraphQL com a introspecção habilitada.

NoSQL Injection: MongoDB

As vulnerabilidades de injeção de script NoSQL permitem que os invasores injetem consultas mal-intencionadas no banco de dados. O MongoDB é um banco de dados NoSQL, e sua documentação afirma que ele permite que os aplicativos executem operações de JavaScript. O ataque de NoSQL Injection é muito perigoso, porque um invasor não autenticado pode extrair dados ou executar códigos JavaScript. Isso pode levar à execução de códigos remotos, ao comprometimento da confidencialidade e da integridade dos dados do aplicativo e a ataques de Denial of Service (DoS). Esta versão inclui uma verificação para detectar a injeção de scripts NoSQL no MongoDB.

Dynamic Code Evaluation: Unsafe Deserialization

O CVE-2021-35464 identificou uma vulnerabilidade de desserialização insegura de pré-autorização em Java no servidor ForgeRock AM anterior à versão 7.0 e no servidor OpenAM anterior à versão 14.6.4. Essa vulnerabilidade permite que os invasores criem um objeto serializado mal-intencionado no parâmetro jato.pageSession e o enviem ao endpoint "/ccversion/Version" com uma única solicitação. A vulnerabilidade existe devido ao uso no aplicativo de uma biblioteca de Java insegura criada por terceiros. Esse problema normalmente permite que os invasores executem códigos arbitrários no servidor, abusem da lógica do aplicativo ou conduzam ataques de Denial of Service (DoS). Esta versão inclui uma verificação para detectar essa vulnerabilidade em servidores web.

Cross-Site Scripting: DOM[4]

O Cross-Site Scripting ocorre quando páginas web geradas automaticamente exibem entradas do usuário, como informações de acesso, que não são validadas corretamente. Isso permite que invasores insiram scripts mal-intencionados na página gerada e os executem na máquina de qualquer usuário que visualize o site. No caso do XSS baseado em Document Object Model (DOM), o conteúdo mal-intencionado é executado como parte de uma manipulação de DOM. Quando exploradas, as vulnerabilidades de DOM Cross-Site Scripting permitem manipular ou roubar cookies, criar solicitações que podem ser tomadas como legítimas, comprometer informações confidenciais ou executar códigos mal-intencionados em sistemas do usuário final. Esta versão contém uma nova verificação para detectar DOM XSS em fragmentos de URI no lado do cliente.

Web Server Misconfiguration: Insecure Mapping Directives

Por vezes, a fim de configurar o Nginx para executar PHP no servidor web, recomenda-se passar todos os URIs terminados em .php ao interpretador de PHP de back-end (como FastCGI). O Nginx com essa configuração insegura de PHP considerará as pastas no caminho do URL como o arquivo a ser executado, caso o caminho completo solicitado não leve a um arquivo existente. Essa configuração inadequada permite que um invasor execute códigos PHP arbitrários em qualquer tipo de arquivo, como arquivos de imagem, que possa ser carregado no servidor web e acessado. Esta versão inclui uma verificação para detectar essa vulnerabilidade em servidores web.

[4] Requer WI v21.2.0 ou superior.

Integer Overflow

O Nginx, da versão 0.5.6 à versão 1.13.2, é suscetível a uma vulnerabilidade de Integer Overflow, identificada pelo CVE-2017-7529. O problema encontra-se no módulo de filtro de intervalo do Nginx e permite que um invasor adquira informações potencialmente sensíveis ao enviar solicitações específicas. Esta versão inclui uma verificação para detectar a vulnerabilidade CVE-2017-7529 nos servidores web de destino.

Relatórios de conformidade

2021 Common Weakness Enumeration (CWE™) Top 25

O Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) foi introduzido em 2019 em substituição ao SANS Top 25. Lançado em julho, o 2021 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. Esta atualização do SecureBase inclui verificações que mapeiam diretamente para a categoria identificada pelo CWE Top 25 ou para um CWE-ID ligado a um CWE-ID no Top 25 por relacionamento “ChildOf”.

Atualizações da política

CWE Top 25 2021

Uma política personalizada para incluir verificações relevantes para CWE Top 25 2021 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 falso-positivos e melhorar a capacidade dos clientes de auditar problemas. Os clientes também podem esperar alterações nos problemas relatados relacionadas com o que segue:

LDAP Injection

Esta versão inclui melhorias para a verificação de LDAP Injection para reduzir falso-positivos e aumentar a precisão dos resultados.

CyberRes Fortify Premium Content

A equipe de pesquisa cria, estende e mantém uma variedade de recursos fora dos nossos principais produtos de inteligência de segurança.

2021 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 2021 CWE Top 25, que está disponível para download no Portal de Suporte ao Cliente Fortify em Premium Content.

CyberRes 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. O site anterior, que contém a última atualização com suporte, está disponível no Portal de Suporte do CyberRes Fortify.

Entre em contato com o suporte técnico do Fortify

CyberRes Fortify
http://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

SSR de Contato

Alexander M. Hoole
Gerente Sênior, Software Security Research
CyberRes Fortify hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
Gerente de Software Security Research
CyberRes Fortify
peter.blay@microfocus.com