Conteúdo de Segurança de Software do Fortify

Atualização 2 de 2024
sexta-feira, 28 de junho de 2024

Sobre o OpenText Fortify Software Security Research

A equipe do Fortify Software Security Research traduz pesquisas de ponta em inteligência de segurança que potencializa o portfólio de produtos Fortify, incluindo o OpenText™ Fortify Static Code Analyzer e o OpenText™ Fortify WebInspect. Atualmente, o Conteúdo de Segurança de Software da Fortify oferece suporte a 1.660 categorias de vulnerabilidade em 33 linguagens e se estende por mais de um milhão de APIs individuais.

O Fortify Software Security Research (SSR) tem o prazer de anunciar a disponibilidade imediata de atualizações para Fortify Secure Coding Rulepacks (idioma inglês, versão 2024.2.0), Fortify WebInspect SecureBase (disponível via SmartUpdate) e Fortify Premium Content.

Fortify Secure Coding Rulepacks [Fortify Static Code Analyzer]

Nesta versão, os Fortify Secure Coding Rulepacks detectam 1.435 categorias únicas de vulnerabilidades em mais de 33 linguagens e abrangem mais de um milhão de APIs individuais. Em resumo, essa versão inclui o seguinte:

Suporte aprimorado para Node.js (versão compatível: 21.x)[1]

Node.js é um ambiente de execução JavaScript para várias plataformas que permite aos desenvolvedores criar servidores, aplicativos da Web, ferramentas de linha de comando e muito mais. Esta versão contém atualizações significativas em nosso suporte ao Node.js para os seguintes módulos no Node.js 21.x:

- async_hooks
- buffer
- child_process
- crypto
- dgram
- dns
- fs
- http
- https
- net
- os
- path
- process
- punycode
- querystring
- stream
- string_decoder
- timers
- tls
- url
- util
- v8
- vm
- worker_threads
- zlib

Essas atualizações melhoram a detecção de problemas para as seguintes categorias de pontos fracos:

- Command Injection
- Dynamic Code Evaluation: Code Injection
- Header Manipulation

[1] Requer o Fortify Static Code Analyzer 24.2 ou posterior.

- Insecure Transport: Weak SSL Cipher
- Insecure Transport: Weak SSL Protocol
- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- System Information Leak
- System Information Leak: External

Além disso, as seguintes categorias de pontos fracos foram introduzidas nesta versão para aplicativos Node.js:

- DNS Spoofing
- Dynamic Code Evaluation: Script Injection
- Insecure Transport: Insufficient Diffie Hellman Strength
- Key Management: Empty HMAC Key
- Key Management: Empty PBE Password
- Key Management: Hardcoded HMAC Key
- Key Management: Hardcoded PBE Password
- Weak Cryptographic Hash
- Weak Cryptographic Hash: Empty PBE Salt
- Weak Cryptographic Hash: Hardcoded PBE Salt
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Cryptographic Hash: Predictable Salt
- Weak Cryptographic Hash: User-Controlled PBE Salt
- Weak Encryption
- Weak Encryption: Insecure Initialization Vector
- Weak Encryption: Insecure Mode of Operation
- Weak Encryption: Stream Cipher

Suporte aprimorado para Java (versão compatível: 21)

Java 21 é a versão mais recente com suporte de longo prazo (LTS) para a plataforma Java. Inclui melhorias nas APIs existentes, como também um número significativo de novos recursos, e os mais significativos são: Função Estrangeira e Memória, Coleções Sequenciadas, Encapsulamento de Chave, Threads Virtuais, Simultaneidade Estruturada, Variáveis Sem Nome e Valores com Escopo. Alguns desses recursos ainda estão em estado de visualização, mas são considerados maduros o suficiente para incluir cobertura. As categorias atualizadas incluem o seguinte:

- Process Control
- Unreleased Resource
- Weak Encryption
- Weak Cryptographic Hash

Além disso, há suporte para as seguintes novas categorias:

- Restricted Method
- Weak Cryptographic Signature: XML Signature Secure Validation Disabled

Suporte aprimorado para MyBatis (versão compatível: 3.5.x)

MyBatis é um mapeador SQL usado para acoplar objetos em um banco de dados relacional a objetos em um aplicativo orientado a objetos. Essa estrutura combina procedimentos armazenados e instruções SQL usando descritores XML ou anotações de código para facilitar o processo de desenvolvimento e a comunicação do banco de dados. O suporte para MyBatis foi atualizado para a versão 3.5.16. As melhorias incluem suporte atualizado para as seguintes categorias de pontos fracos:

- Dynamic Code Evaluation: Unsafe Deserialization
- SQL Injection
- System Information Leak
- Unreleased Resource: Database
- Unsafe Reflection

Suporte inicial para o MyBatis-Plus (versão compatível: 3.5.x)

O MyBatis-Plus se baseia na estrutura MyBatis existente para simplificar o desenvolvimento, fornecendo recursos úteis, eficientes e prontos para uso, além daqueles encontrados na estrutura original. Há suporte inicial para o MyBatis - Plus 3.5.x. O suporte inicial da categoria é fornecido para *SQL Injection*.

Detecção de riscos originados de modelos de inteligência artificial (IA) e aprendizado de máquina (ML)

Com o uso de IA generativa e modelos de linguagem grandes (LLMs) mudando rapidamente o panorama de soluções do setor de software, novos riscos estão surgindo. Esta versão melhora a cobertura para projetos que consomem APIs OpenAI (Python e JavaScript), TensorFlow (Python) ou Anthropic Claude (Python e JavaScript). O suporte detecta os pontos fracos resultantes da confiança implícita nas respostas das APIs de modelos de IA/ML, além dos seguintes recursos:

Suporte aprimorado para OpenAI (versão compatível: 1.14.x [Python], 4.33.x [JavaScript])

As bibliotecas OpenAI para Python, TypeScript e JavaScript fornecem ferramentas abrangentes para integração de recursos avançados de IA em vários aplicativos. Essas bibliotecas oferecem suporte a uma variedade de funcionalidades, incluindo processamento de linguagem natural, geração de texto e IA de conversação. Com APIs intuitivas e fáceis de usar, os desenvolvedores podem incorporar perfeitamente os modelos de IA de última geração da OpenAI em seus projetos, aprimorando a interatividade e a inteligência em ambientes Python, TypeScript e JavaScript. O suporte aprimorado expande a cobertura para *Cross-Site Scripting: AI* e adiciona duas novas categorias de pontos fracos:

- Cross-Site Scripting: DOM AI
- Prompt Injection

TensorFlow (versão compatível: 2.16.x)

TensorFlow, uma estrutura líder de aprendizado de máquina de código aberto do Google, oferece um conjunto poderoso de ferramentas para criar e implantar modelos de aprendizado de máquina. Com bibliotecas integradas e modelos pré-treinados, simplifica a construção de aplicativos de aprendizado profundo. O TensorFlow é escalonável para um conjunto diversificado de projetos, desde protótipos de pesquisa até sistemas de produção em larga escala. A cobertura inclui suporte para as seguintes categorias:

- Path Manipulation
- Privacy Violation
- System Information Leak: Internal

Além disso, o suporte adiciona a nova categoria de pontos fracos:

- Dynamic Code Evaluation: Unsafe TensorFlow Deserialization

Anthropic Claude SDK (versão compatível: 0.21.3 [Python], 0.20.5 [JavaScript])

As bibliotecas Anthropic Claude para Python e JavaScript fornecem ferramentas abrangentes para integrar o Claude, um sofisticado modelo de linguagem de IA, a aplicativos. A cobertura inicial inclui suporte para *Cross-Site Scripting: AI* e adiciona duas novas categorias de pontos fracos:

- Cross-Site Scripting: DOM AI
- Prompt Injection

Suporte aprimorado para Django (versão compatível: 5.0.x)

O Django é uma estrutura da Web escrita em Python que foi projetada para facilitar o desenvolvimento seguro e rápido da Web. A velocidade e a segurança do desenvolvimento são alcançadas pelo alto nível de abstração da estrutura, em que as construções e a geração de código são usadas para reduzir drasticamente o código padrão. Nessa versão, atualizamos nossa cobertura existente do Django para oferecer suporte até a versão 5.0.x.

Essas atualizações melhoram a detecção de problemas para as seguintes categorias de pontos fracos:

- Access Control: Database
- Cookie Security: CSRF Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set on CSRF Cookie
- Cookie Security: HTTPOnly not Set on Session Cookie
- Cookie Security: Session Cookie not Sent Over SSL
- Cross-Frame Scripting
- Cross-Site Request Forgery
- HTML5: Cross-Site Scripting Protection
- HTML5: MIME Sniffing
- HTML5: Misconfigured Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- Insecure Transport
- Insecure Transport: HSTS Does Not Include Subdomains
- Insecure Transport: HSTS not Set
- Insecure Transport: Insufficient HSTS Expiration Time
- Privacy Violation: BREACH
- SQL Injection

Suporte inicial para Paramiko (versão compatível: 3.4.x)

Paramiko é uma biblioteca Python para conexão com máquinas via SSH. Paramiko fornece um conjunto de funcionalidades para abstrair os métodos criptográficos do desenvolvedor. Isso fornece funções de alto nível semelhantes à programação de soquete e concede aos desenvolvedores acesso aos métodos de nível inferior para configuração de microgerenciamento de uma conexão SSH. O suporte inicial abrange as seguintes categorias de pontos fracos:

- Command Injection
- Insecure Transport: Cipher Suite Downgrade
- Insecure Transport: Weak SSL Cipher
- Password Management: Hardcoded Password
- SSH Misconfiguration: Missing Authentication

Suporte aprimorado para PHP (versão compatível: 8.3)

PHP é uma linguagem de script de uso geral amplamente usada, mais frequentemente usada para desenvolvimento da Web. Esta versão atualiza o suporte para PHP até a versão 8.3. Em particular, o lançamento inclui suporte aprimorado para as seguintes extensões:

- DOM (versão compatível: 8.3)

  A extensão DOM do PHP permite operações em documentos XML e HTML em PHP usando um modelo de objeto de documento. O suporte expandido para essa biblioteca inclui suporte aprimorado de fluxo de dados para operações DOM, bem como cobertura adicional para a identificação dos pontos fracos de *Setting Manipulation*.

- JSON (versão compatível: 8.3)

  A extensão JSON do PHP permite o uso de um analisador JSON escrito e licenciado sob a licença PHP. O suporte inicial dessa extensão inclui suporte de fluxo de dados para as funções da extensão.

- OpenSSL (versão compatível: 8.3)

  A extensão OpenSSL do PHP implementa recursos da biblioteca OpenSSL para uma variedade de operações criptográficas. O suporte expandido para essa biblioteca inclui suporte aprimorado de fluxo de dados para pares de chaves criptográficas.

- Simdjson (versão compatível: 8.3)

  A extensão Simdjson do PHP implementa as ligações específicas do PHP do projeto simdjson para fornecer decodificação JSON rápida. O suporte inicial inclui a seguinte nova categoria para PHP:

  - JSON Path Manipulation

Suporte aprimorado para iOS (versão compatível: 17)[2]

Os SDKs do iOS e iPadOS da Apple fornecem uma coleção de estruturas que permitem aos desenvolvedores criar aplicativos móveis para os dispositivos iPhone e iPad da Apple. Esta versão contém atualizações incrementais para nosso suporte do SDK do iOS para Swift e Objective-C. Regras novas e atualizadas ampliam nossa cobertura para APIs das seguintes estruturas no iOS 17:

- CryptoKit

[2] As APIs do iOS 17 requerem Xcode 15 ou superior, que por sua vez requer o Fortify Static Code Analyzer 23.2 ou posterior. No entanto, pode haver avisos do compilador ao usar o Source Code Analyzer 23.2 para criar aplicativos que usam APIs do iOS 17. Recomenda-se o Fortify Static Code Analyzer 24.2 ou posterior para garantir compilações e verificações válidas.

- Foundation
- Network
- os
- System
- SwiftUI
- UIKit

Essas atualizações melhoram a detecção de problemas para as seguintes categorias de pontos fracos:

- Insecure Transport
- Path Manipulation
- Privacy Violation
- Privacy Violation: Health Information
- System Information Leak: External
- System Information Leak: Internal
- Unreleased Resource: Synchronization
- Unsafe Reflection
- Weak Cryptographic Hash
- Weak Cryptographic Hash: User-Controlled Salt
- Weak Encryption: User-Controlled Key Size

Suporte aprimorado para MISRA C 2012

MISRA é uma organização de padrões que cria e mantém vários padrões para desenvolvimento de aplicativos usados em ambientes críticos de segurança que necessitam de alta integridade ou alta confiabilidade em software. Esta versão inclui suporte para duas novas categorias que mapeiam fortemente duas regras de orientação obrigatórias no padrão MISRA C 2012:

- Undefined Behavior: File Pointer Dereference
- Undefined Behavior: File Pointer Use After Close

Atualização das propriedades de expressão regular de senha

As propriedades de expressão regular de senha, introduzidas no Fortify Static Code Analyzer versão 23.1, são propriedades personalizáveis com expressões regulares que determinam como as regras do Fortify correspondem aos identificadores de senha em vários idiomas. Nesta versão, expandimos o valor padrão da propriedade com.fortify.sca.rules.password_regex.global para reconhecer identificadores de senha que envolvem a palavra "secreto". Além disso, adicionamos novas regras para utilizar as propriedades de expressão regular de senha na análise de cadeias JSON geradas dinamicamente. Como resultado, os clientes podem esperar uma detecção aprimorada nas seguintes categorias em todos os idiomas:

- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Privacy Violation

Suporte aprimorado para Golang (versão compatível: até 1.21)

Go, também conhecido como Golang, é uma linguagem de programação compilada, digitada estaticamente e criada no Google. É conhecida por sua simplicidade, eficiência e forte suporte à simultaneidade, o que a torna ideal para a criação de serviços da Web escaláveis, pipelines de dados e sistemas distribuídos. Esta versão inclui detecção para os pontos fracos de *Unreleased Resource* e introduz nova detecção de *SQL Injection* para projetos que usam GORM v2.

Melhorias na API do WordPress (versão compatível: até 6.5) (contagem de APIs: 2)

A Interface de Programação de Aplicativo (API) do WordPress pode ser separada em várias seções/tópicos de API, cada uma abrangendo as funções envolvidas e o uso de um determinado conjunto de funcionalidades. Juntos, eles formam o que pode ser chamado de API do WordPress, que é a interface de plug-in/tema/complemento criada por todo o projeto do WordPress. Esta versão adiciona suporte inicial para a identificação de problemas nas seguintes APIs:

- REST API
- Shortcode API

Erratas diversas

Nesta versão, continuamos a investir recursos para garantir que possamos reduzir o número de problemas de falsos positivos, refatorar para consistência e melhorar a capacidade dos clientes de auditar problemas. Os clientes também podem esperar alterações nos problemas relatados relacionadas ao seguinte:

Redução de falsos positivos e outras melhorias notáveis na detecção

O trabalho continuou com o esforço para remover falsos positivos nessa versão. Os clientes podem esperar mais remoção de falsos positivos e outras melhorias notáveis relacionadas às seguintes áreas:

- *ASP.NET MVC Bad Practices: Optional Submodel With Required Property* – falsos positivos reduzidos em aplicativos ASP.NET
- *Insecure Transport: Mail Transmission* – falsos positivos reduzidos em aplicativos Java
- *Password Management: Hardcoded Password* – falsos positivos reduzidos em arquivos JSON/YAML
- *Unreleased Resource: Streams* – falsos positivos reduzidos em aplicativos Java
- *Password Management: Hardcoded Password* – novos problemas detectados em aplicativos Python relacionados a tipos de dicionário
- *Password Management: Hardcoded Password* – novos problemas detectados em aplicativos ASP.NET relacionados a cadeias interpoladas
- Muitos falsos positivos removidos provenientes das propriedades integradas do sistema JDK

Alterações no nome da categoria

Quando ocorrem alterações no nome da categoria de ponto fraco, a mesclagem dos resultados da análise de verificações anteriores com novas verificações pode resultar em categorias adicionadas/removidas.

Para aprimorar a consistência, as três seguintes categorias foram renomeadas:

Nome da categoria 2024 R1	Nome da categoria 2024 R2
Access Control: gRPC Authentication Bypass	Access Control: gRPC Fail Open
AWS CloudFormation Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key	AWS CloudFormation Misconfiguration: SecretsManager Missing Customer-Managed Encryption Key
AWS Terraform Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key	AWS Terraform Misconfiguration: SecretsManager Missing Customer-Managed Encryption Key

DISA Control Correlation Identifier (CCI) Versão 2

O Defense Information Systems Agency (DISA) CCI é um documento que preenche a lacuna entre as orientações de segurança cibernética de alto e baixo nível, fornecendo um conjunto de identificadores padrão emparelhados com declarações singulares e acionáveis. O DISA Application Security and Development STIG está intimamente mapeado para o DISA CCI, em que um único controle STIG pode ser aplicado a um ou mais CCIs. Esta versão traz os CCIs mapeados em paridade com as atualizações recentes dos mapeamentos do STIG em relação ao Fortify Taxonomy durante as versões anteriores.

Revisões 4 e 5 da Publicação Especial do NIST 800-53

A Publicação Especial 800-53 do Instituto Nacional de Padrões e Tecnologia (NIST) é um documento que fornece um catálogo de controles de segurança e privacidade para sistemas de informação que podem ser aproveitados pelo campo da segurança cibernética em geral para fornecer orientação sobre como proteger os sistemas. A Publicação Especial 800-53 do NIST está intimamente mapeada para o DISA CCI, em que um único CCI pode ser aplicado a um ou mais controles do NIST 800-53. Esta versão traz os controles mapeados do NIST 800-53 em paridade com as atualizações recentes dos mapeamentos do DISA CCI em relação ao Fortify Taxonomy.

OWASP Mobile Top 10 2023

Como anunciado anteriormente, nesta versão do Fortify Software Security Content, o mapeamento OWASP Mobile Top 10 2023 será descontinuado e apenas o OWASP Mobile Top 10 2024 atualizado permanecerá.

Alinhando lançamentos de conteúdo de segurança de software com controle de versão OpenText

A próxima versão conterá uma alteração no controle de versão do conteúdo de segurança. Este será o último lançamento da atualização de conteúdo de segurança do OpenText Fortify que segue a convenção de nomenclatura de "Atualização 2 de 2024". Para se alinhar aos padrões de versão do OpenText, os lançamentos são programados um por trimestre a cada ano e são numerados de acordo com o ano e o trimestre — portanto, o próximo lançamento do OpenText™ Fortify™ Software Security Content será 24.4, indicando um lançamento no primeiro mês do 4º trimestre de 2024.

Fortify SecureBase [Fortify WebInspect]

O Fortify SecureBase combina verificações de milhares de vulnerabilidades com políticas que orientam os clientes nas atualizações a seguir, disponíveis imediatamente usando o SmartUpdate.

Suporte a vulnerabilidades

Denial of Service: GraphQL

A linguagem de consulta GraphQL para APIs fornece um tempo de execução para consultar dados existentes. O esquema GraphQL é um modelo que consiste em objetos de dados, seus campos e tipos e seus relacionamentos com outros objetos de dados. As referências entre diferentes objetos de dados podem criar um ciclo. Um invasor pode desencadear o uso excessivo de CPU e memória criando uma consulta maliciosa cíclica, dispendiosa e aninhada que causa uma negação de serviço (DoS). Esta versão inclui uma verificação para detectar referências circulares no esquema GraphQL.

Access Control: Authorization Bypass (CVE-2024-27198)

A CVE-2024-27198 foi identificada como uma vulnerabilidade crítica no software JetBrains e representa uma ameaça significativa à segurança. Essa vulnerabilidade destaca os riscos associados a mecanismos de autenticação insuficientes, que podem permitir que invasores não autenticados obtenham controle administrativo sobre os sistemas afetados. A versão mais recente inclui uma verificação para detectar essa vulnerabilidade nos servidores de destino.

Directory Traversal (CVE-2024-27199)

As versões do servidor JetBrains TeamCity On-Premises anteriores à 2023.11.4 são vulneráveis a uma falha de passagem de caminho, identificada como CVE-2024-27199. Os invasores podem usar essa falha para contornar os controles de autenticação e ameaçar significativamente a integridade e a confidencialidade do sistema. A versão mais recente inclui uma verificação para detectar essa vulnerabilidade nos servidores de destino.

Dynamic Code Evaluation: Unsafe Deserialization (CVE-2023-26360)

As versões do Adobe ColdFusion Atualização 15 de 2018 e anteriores, bem como a Atualização 5 de 2021 e anteriores, são afetadas por uma vulnerabilidade de avaliação dinâmica de código, identificada pela CVE -2023-26360. Essa vulnerabilidade pode resultar na execução arbitrária de código no contexto do usuário atual. A exploração desse problema não requer interação do usuário. Essa versão inclui uma verificação para detectar essa vulnerabilidade nos servidores de destino.

Insecure Deployment: Unpatched Application (CVE-2024-32962)

CVE-2024-32962 é uma vulnerabilidade crítica associada a xml-crypto, uma assinatura digital de XML e biblioteca de criptografia para Node.js. Esta vulnerabilidade foi introduzida na versão 4.0.0 e foi corrigida na versão 6.0.0. A vulnerabilidade surge porque, nas versões afetadas, a configuração padrão não verifica a autorização do assinante. Um invasor pode explorar isso modificando um documento XML e substituindo a assinatura existente por uma gerada com uma chave privada maliciosa, anexando o certificado correspondente ao elemento <KeyInfo/>. Esta versão inclui uma verificação para detectar essa vulnerabilidade em servidores de destino que usam as versões afetadas da xml-crypto.

Erratas diversas

Nessa versão, investimos recursos para reduzir ainda mais o número de problemas de falsos positivos e melhorar a capacidade dos clientes de auditar problemas. Os clientes também podem esperar alterações nas descobertas relatadas relacionadas às seguintes áreas:

Insecure Deployment: OpenSSL

Esta versão inclui melhorias na verificação de OpenSSL ChangeCipherSpec Man-in-the-Middle (MitM) para reduzir falsos positivos e aumentar a precisão dos resultados.

Fortify Premium Content

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

Fortify Taxonomy: Erros de segurança de software

O site do Fortify Taxonomy, que contém descrições para suporte de categoria recém-adicionadas, está disponível em https://vulncat.fortify.com.

Entre em contato com o suporte ao cliente

OpenText Fortify
https://softwaresupport.softwaregrp.com/
+1 (800) 509-1800

SSR de Contato

Alexander M. Hoole
Gerente Sênior, Software Security Research
OpenText Fortify
hoole@opentext.com
+1 (650) 427-9973

Peter Blay
Gerente de Software Security Research
OpenText Fortify
pblay@opentext.com
+1 (669) 309-1634