Conteúdo de Segurança de Software do Fortify

Atualização 4 de 2023
sexta-feira, 15 de dezembro de 2023

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 (SCA) e o OpenText™ Fortify WebInspect. Atualmente, o Conteúdo de Segurança de Software da Fortify oferece suporte a 1.657 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 2023.4.0), 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 1.432 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 Python (versão compatível: 3.12)

Python é uma poderosa linguagem de programação de uso geral, com tipagem dinâmica e estruturas de dados de alto nível eficientes. Ele oferece suporte a vários paradigmas de programação, incluindo programação estruturada, orientada a objetos e funcional. Essa versão aumenta nossa cobertura para a versão mais recente do Python, expandindo nosso suporte para alterações na API da biblioteca padrão do Python. Atualização da cobertura das regras existentes para os seguintes módulos:

- os
- pathlib
- tomllib

Suporte aprimorado para Django (versão compatível: 4.2)

O Django é uma estrutura da Web escrita em Python, 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 dar suporte às versões: 4.0, 4.1 e 4.2.

A cobertura aprimorada inclui os seguintes namespaces: *asyncio, django.core.cache.backends.base.BaseCache, django.db.models.Model* e *django.middleware.security.SecurityMiddleware*. Além disso, melhoramos a cobertura das categorias de pontos fracos, que inclui o seguinte:

- Header Manipulation
- Insecure Cross-Origin Opener Policy
- Resource Injection
- Setting Manipulation

PyCryptodome e PyCrypto (versão compatível: 3.19.0)

O PyCryptodome é um pacote Python autônomo que fornece uma coleção abrangente de algoritmos e protocolos criptográficos. Ele funciona como uma versão ampliada e com manutenção mais ativa da biblioteca PyCrypto. O PyCryptodome foi projetado para oferecer uma ampla gama de funcionalidades criptográficas, tornando-o uma opção versátil para desenvolvedores que precisam implementar comunicação segura, proteção de dados e operações criptográficas em seus aplicativos Python.

A cobertura inicial das categorias de pontos fracos inclui o seguinte:

- Key Management: Empty Encryption Key
- Key Management: Empty PBE Password
- Key Management: Hardcoded Encryption Key
- Key Management: Hardcoded HMAC Key
- Key Management: Hardcoded PBE Password
- Key Management: Unencrypted Private Key
- Password Management: Hardcoded Password
- Password Management: Lack of Key Derivation Function
- Password Management: Password in Comment
- Weak Cryptographic Hash
- Weak Cryptographic Hash: Hardcoded PBE Salt
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Cryptographic Hash: Predictable Salt
- Weak Cryptographic Signature: Insufficient Key Size
- Weak Encryption
- Weak Encryption: Insecure Initialization Vector
- Weak Encryption: Insecure Mode of Operation
- Weak Encryption: Insufficient Key Size
- Weak Encryption: Stream Cipher
- Weak Encryption: User-Controlled Key Size

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

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. O suporte inicial do Fortify abrange projetos Python que consomem a API OpenAI, o SageMaker da Amazon Web Services (AWS) ou o LangChain. O suporte detecta os pontos fracos resultantes da confiança implícita nas respostas das APIs de modelos de IA/ML, além dos seguintes recursos exclusivos:

Suporte inicial para a API Python OpenAI (versão compatível: 1.3.8)

A biblioteca OpenAI Python permite que os desenvolvedores acessem convenientemente a API REST da OpenAI para interagir com os modelos da OpenAI, como o GPT-4 e o DALL-E. A API OpenAI permite que um aplicativo envie prompts para os modelos da OpenAI e receba as respostas geradas, além de ajustar os modelos existentes. O módulo Python da OpenAI oferece suporte à capacidade de enviar e receber solicitações assíncronas e síncronas com a tecnologia *httpx*. O suporte inclui a identificação de resultados potencialmente perigosos do modelo, bem como a seguinte categoria nova:

- Cross-Site Scripting: AI

Suporte inicial para Python AWS SageMaker (Boto3) (versão compatível: 1.33.9)

O AWS SageMaker é uma oferta do grande abrangência de serviços do Amazon AWS. O AWS SageMaker oferece um amplo conjunto de ferramentas para dar suporte a uma grande variedade de projetos de ML, desde o treinamento de modelos personalizados até a configuração de pipelines de desenvolvimento completos com suporte de MLOps. O SDK para Python (Boto3) da Amazon permite

a comunicação com uma ampla variedade de ofertas do AWS, incluindo o AWS SageMaker. O suporte inclui a identificação de resultados potencialmente perigosos do modelo, bem como a seguinte categoria nova:

- Cross-Site Scripting: AI

Suporte inicial para Python LangChain (versão compatível: 0.0.338)[1]

O LangChain é uma estrutura popular de orquestração de código aberto para o desenvolvimento de aplicativos que usam modelos de linguagem grandes (LLMs). O LangChain oferece ferramentas e APIs que facilitam a criação de aplicativos orientados por LLM, como chatbots e agentes virtuais. Elas estão disponíveis como bibliotecas baseadas em Python e JavaScript. O suporte inclui identificação de resultados potencialmente perigosos do modelo, detecção de *Manipulação de caminho,* bem como a seguinte categoria nova:

- Cross-Site Scripting: AI

.NET 8 (versão compatível: 8.0.0)

Como sucessor do .NET 7, o .NET 8 é uma estrutura de desenvolvimento multiplataforma, gratuita e de código aberto que permite aos programadores escrever aplicativos em diferentes linguagens, como C# e VB, com um conjunto padronizado de APIs. Essa versão aumenta nossa cobertura para a versão mais recente do .NET a fim de melhorar a detecção de pontos fracos em APIs novas e existentes.

A cobertura ampliada abrange os seguintes namespaces:

- System.Collections.Frozen
- System.Net.Http.Json
- System
- System.Security
- System.Text
- System.Text.Unicode
- System.Net.Http

Criptografia simplificada Java (Jasypt) (versão compatível: 1.9.3)

O Java Simplified Encryption (Jasypt) é uma pequena biblioteca Java usada para executar criptografia baseada em senha, bem como criar resumos de senha para armazenamento. Ele tem integração com estruturas Java populares, como Spring, Wicket e Hibernate.

A cobertura inicial das categorias de pontos fracos inclui o seguinte:

- Insecure Randomness
- Key Management: Empty PBE Password
- Key Management: Hardcoded PBE Password
- Key Management: Null PBE Password
- Password Management: Lack of Key Derivation Function
- Privacy Violation: Heap Inspection

[1] O LangChain ainda é muito novo. A consideração cuidadosa da segurança deve ser avaliada antes do uso na produção.

- Setting Manipulation
- 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: User-Controlled PBE Salt
- Weak Encryption
- Weak Encryption: Insecure Mode of Operation

ECMAScript 2023

O ECMAScript 2023, também conhecido como ES2023 ou ES14, é a versão mais recente do padrão ECMAScript para a linguagem JavaScript. Os principais recursos do ES2023 incluem novas funções de matriz que permitem alterá-las por cópia e pesquisar começando do final. O suporte para ES2023 estende a cobertura de todas as categorias de pontos fracos JavaScript relevantes para a versão mais recente do padrão ECMAScript.

Poluição do protótipo

A Poluição de protótipo é uma vulnerabilidade em aplicativos JavaScript que permite que usuários mal-intencionados ignorem ou afetem a lógica de negócios, além de executar potencialmente seu próprio código.

Essa atualização do Rulepack detecta se um invasor pode poluir o protótipo de um objeto nos seguintes pacotes NPM:

- assign-deep
- deap
- deep-extend
- defaults-deep
- dot-prop
- hoek
- lodash
- merge
- merge-deep
- merge-objects
- merge-options
- merge-recursive
- mixin-deep
- object-path
- pathval

Configurações do Kubernetes

O Kubernetes é uma solução de gerenciamento de contêineres de código aberto para automatizar a implantação, o dimensionamento e o gerenciamento de aplicativos em contêineres. Ele fornece abstrações de infraestrutura centradas em contêineres que removem as dependências da infraestrutura subjacente, permitindo implementações portáteis e simplificando o gerenciamento de sistemas distribuídos complexos. A cobertura melhorada das categorias de pontos fracos inclui o seguinte:

- Kubernetes Misconfiguration: Improper API Server Network Access Control
- Kubernetes Misconfiguration: Improper CronJob Access Control
- Kubernetes Misconfiguration: Improper DaemonSet Access Control
- Kubernetes Misconfiguration: Improper Deployment Access Control
- Kubernetes Misconfiguration: Improper Job Access Control
- Kubernetes Misconfiguration: Improper Pod Access Control
- Kubernetes Misconfiguration: Improper RBAC Access Control
- Kubernetes Misconfiguration: Improper ReplicaSet Access Control
- Kubernetes Misconfiguration: Improper Replication Controller Access Control
- Kubernetes Misconfiguration: Improper StatefulSet Access Control
- Kubernetes Misconfiguration: Insecure Secret Transport
- Kubernetes Misconfiguration: Insufficient Kubelet Logging
- Kubernetes Misconfiguration: Scheduler System Information Leak
- Kubernetes Misconfiguration: Uncontrolled Kubelet Resource Consumption
- Kubernetes Terraform Misconfiguration: Improper Daemon Set Access Control
- Kubernetes Terraform Misconfiguration: Improper Deployment Access Control
- Kubernetes Terraform Misconfiguration: Improper Job Access Control
- Kubernetes Terraform Misconfiguration: Improper Pod Access Control
- Kubernetes Terraform Misconfiguration: Improper Pod Network Access Control
- Kubernetes Terraform Misconfiguration: Improper RBAC Access Control
- Kubernetes Terraform Misconfiguration: Improper Replication Controller Access Control
- Kubernetes Terraform Misconfiguration: Improper Stateful Set Access Control
- Kubernetes Terraform Misconfiguration: Insecure Secret Transport

DISA STIG 5.3

Para oferecer suporte a nossos clientes federais na área de conformidade, foi adicionada a correlação do Fortify Taxonomy com o Defense Information Systems Agency (DISA) Application Security and Development STIG, versão 5.3.

OWASP Mobile Top 10 Risks 2023

O Open Worldwide Application Security Project (OWASP) Mobile Top 10 Risks 2023 visa aumentar a conscientização sobre os riscos de segurança móvel e educar os envolvidos no desenvolvimento e manutenção de aplicativos móveis. Para dar suporte a nossos clientes que desejam reduzir o risco de aplicativos da Web, foi adicionada a correlação do Fortify Taxonomy com a versão inicial do OWASP Mobile Top 10 2023.

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:

Descontinuação das versões do Fortify Static Code Analyzer anteriores à 20.x

Como mencionado em nosso anúncio da versão 2023.3, aquele foi o último lançamento de Rulepacks compatíveis com Static Code Analyzer anteriores à versão 20.x. Para esta versão,

as versões do Static Code Analyzer anteriores à 20.x não carregarão os Rulepacks. Será necessário fazer o downgrade do Rulepacks ou o upgrade da versão do Static Code Analyzer. Nas versões futuras, vamos continuar a oferecer suporte para as últimas quatro versões principais do Static Code Analyzer.

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 Misconfiguration: Persistent Authentication* – falsos positivos removidos em aplicativos ASP.NET que usam serviços de autenticação de formulários
- *Credential Management: Hardcoded API Credentials* – falsos positivos removidos da verificação secreta relacionada a tokens HTTP Bearer
- *Credential Management: Hardcoded API Credentials* – novos problemas detectados para chaves de API Avature
- *Cross-Site Request Forgery* – novos problemas detectados em aplicativos NodeJS que usam a estrutura JavaScript "Express.js"
- *Cross-Site Scripting* – novos problemas detectados em aplicativos Go que usam o pacote "html/template"
- *Cross-Site Scripting: Reflected* – falsos positivos removidos em aplicativos ASP.NET que usam a classe "ListControl"
- *Denial of Service: Format String* – mapeamentos incorretos para as categorias do OWASP Top 10
- *Insecure Transport* – falsos positivos removidos em aplicativos ASP.NET relacionados a métodos de controlador que lidam com dados de usuários privados
- *Insecure Transport: Mail Transmission* – falsos positivos removidos de aplicativos Python que usam a classe "smtplib.SMTP"
- *Key Management: Hardcoded Encryption Key* – falsos positivos removidos em aplicativos Java que usam a classe "RSAKeyGenParameterSpec"
- *Link Injection: Missing Validation* – falsos positivos removidos em aplicativos Swift e Objective-C que usam o protocolo `WKNavigationDelegate`[2]
- *Mass Assignment: Insecure Binder Configuration* – falsos positivos removidos de aplicativos Java que usam APIs Jakarta EE
- *Password Management: Password in Configuration File* – falsos positivos removidos dos arquivos de configuração
- *Path Manipulation* – novos problemas detectados em aplicativos PHP com uploads de arquivos
- *SQL Injection* – novos problemas detectados em aplicativos NodeJS que usam o banco de dados marsdb
- *SQL Injection: MyBatis Mapper* – novos problemas detectados nos arquivos XML do mapeador MyBatis
- *String Termination Error* – falsos positivos removidos em aplicativos C/C++ que usam "printf()" e suas variantes
- *System Information Leak: Incomplete Servlet Error Handling* – falsos positivos removidos em aplicativos Java
- *Weak Encryption: Insecure Initialization Vector* – falsos positivos removidos em aplicativos Python que usam a biblioteca "Pycryptodome"
- *Unreleased Resource: Streams* – falsos negativos identificados em aplicativos Java que usam APIs "java.nio.file"
- Vários falsos positivos de fluxo de dados em aplicativos do Visualforce relacionados a informações do perfil de usuário

[2] Requer o Fortify Source Code Analyzer 23.1 ou posterior

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 duas seguintes categorias foram renomeadas:

Categorias removidas	Categoria adicionada
Azure ARM Misconfiguration: Insecure DataBricks Storage	Azure ARM Misconfiguration: Insecure Databricks Storage
Azure ARM Misconfiguration: Insecure Redis Enterprise Transport	Azure ARM Misconfiguration: Insecure Redis Transport

Fortify SecureBase [Fortify WebInspect]

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

Suporte a vulnerabilidades

Access Control: Interface administrativa

Essa versão inclui uma verificação para detectar a configuração não segura do Spring Cloud Gateway quando o endpoint do atuador do gateway está ativado, exposto e não protegido. Nesse caso, os invasores podem criar novas rotas e obter acesso a ativos internos ou confidenciais em nome do aplicativo. Isso pode levar ao roubo de chaves de metadados da nuvem, à exposição de aplicativos internos ou a ataques de negação de serviço (DoS).

Expression Language Injection: Spring

As versões 3.1.0, 3.0.0 a 3.0.6 e versões anteriores à 3.0.0 do Spring Cloud Gateway contêm uma vulnerabilidade de segurança identificada pelo CVE-2022-22947. Essa vulnerabilidade permite um ataque de injeção de código quando o endpoint do atuador do gateway está ativado, exposto e não seguro. Essa versão inclui uma verificação para detectar se essa vulnerabilidade existe no servidor de destino que usa as versões afetadas do Spring Cloud Gateway.

Insecure Deployment: Unpatched Application

As versões 2023.05.3 e anteriores do servidor TeamCity On-Premises estão sujeitas a um desvio de autenticação, o que permite que um invasor não autenticado obtenha execução remota de código (RCE) no servidor. Essa vulnerabilidade foi identificada pelo CVE-2023-42793. Essa versão inclui uma verificação para detectar essa vulnerabilidade nos servidores de destino.

Descoberta de informações: API não documentada

A documentação não documentada ou limitada dos endpoints da API pode fornecer aos invasores uma superfície de ataque que não foi suficientemente testada quanto a vulnerabilidades de segurança. Um invasor pode realizar um reconhecimento para descobrir endpoints obsoletos, sem patches e sem manutenção para obter acesso a informações confidenciais ou funcionalidades perigosas. Esta versão inclui uma verificação que visa descobrir endpoints de API com versão que são acessíveis, mas não estão definidos no documento de especificação da API.

Relatórios de conformidade

DISA STIG 5.3

Para atender às necessidades de conformidade de nossos clientes federais, esta versão contém uma correlação das verificações do WebInspect com a versão mais recente do Defense Information Systems Agency Application Security and Development (DISA) STIG, versão 5.3.

Atualizações da política

DISA STIG 5.3

Uma política personalizada para incluir verificações relevantes para DISA STIG 5.3 foi adicionada à lista WebInspect SecureBase de políticas com suporte.

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 Transport: Fluxo de renegociação do SSLv3/TLS

O TLS 1.3 não oferece suporte à renegociação. Essa versão inclui melhorias na verificação de Renegotiation Stream Injection para reduzir falsos positivos e aumentar a precisão dos resultados.

HTML5: Cross-Site Scripting Protection

O cabeçalho X-XSS-Protection está obsoleto em todos os navegadores modernos. Nessa versão, descontinuamos as verificações de cabeçalho X-XSS-Protection ausentes ou mal configuradas.

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 5.3 e OWASP Mobile Top 10 2023

Para acompanhar as novas correlações, essa versão também contém um novo pacote de relatórios para o OpenText™ Fortify Software Security Center com suporte para DISA STIG 5.3 e OWASP Mobile Top 10 2023, que está disponível para download no Portal de Suporte ao Cliente Fortify em Conteúdo Premium.

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 do Fortify

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