Anúncio da versão do Software Security Research

Conteúdo de Segurança de Software do Fortify

Atualização 2 de 2022

sexta-feira, 24 de junho de 2022

Sobre o CyberRes 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) e o Fortify WebInspect. Atualmente, o conteúdo de segurança de software do Fortify oferece suporte a 1.220 categorias de vulnerabilidade em 30 linguagens e se estende por mais de um milhão de APIs individuais.

CyberRes
A Micro Focus Line of Business

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 2022.2.0), o Fortify WebInspect SecureBase (disponível via SmartUpdate) e o Fortify Premium Content.

Fortify Secure Coding Rulepacks [SCA]

Nesta versão, os Pacotes de regras de codificação segura do Fortify detectam 1.000 categorias únicas de vulnerabilidades em 30 linguagens de programação e abrangem mais de um milhão de APIs individuais. Em resumo, essa versão inclui o seguinte:

Melhorias no .NET (versão com suporte: 6.0)

.NET é uma plataforma de programação geral que permite aos programadores escrever código em linguagens como C# e VB.NET usando um conjunto padronizado de APIs. Esta versão aumenta nossa cobertura para a versão mais recente do .NET para melhorar o fluxo de dados, além de expandir a cobertura da API para as seguintes categorias:

- Access Control: Database
- Path Manipulation
- Privacy Violation
- Server-Side Request Forgery
- SQL Injection
- System Information Leak: External
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Encryption: Insecure Mode of Operation

Melhorias no ASP.NET Core (versão com suporte: 6.0)

ASP.NET Core é a estrutura da Web principal usada com .NET. A estrutura inclui funcionalidade para criar vários tipos de aplicativos, incluindo aplicativos da Web MVC e APIs da Web. Essa versão aumenta nossa cobertura para a versão mais recente do ASP.NET Core, incluindo o mínimo de APIs, e expande nossas categorias com suporte para incluir:

- .NET Attribute Misuse: Authorization Bypass
- ASP.NET Bad Practices: Compression Over Encrypted WebSocket Connection
- ASP.NET Middleware Out of Order: Default Cookie Configuration
- ASP.NET Middleware Out of Order: Insecure Transport
- ASP.NET Middleware Out of Order: Insufficient Logging
- ASP.NET Misconfiguration: Insecure Transport
- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute

Weak Cryptographic Implementation

Psychic Signatures (CVE-2022-21449) é uma vulnerabilidade na implementação Java do Elliptical Curve Digital Signature Algorithm (ECDSA). Essa vulnerabilidade permite que um invasor force o aplicativo a aceitar uma assinatura digital composta por zeros como válida. As versões vulneráveis do Java incluem: 15, 16, 17 e 18. Se uma versão vulnerável do Java for usada, um invasor poderá falsificar alguns tipos de certificados SSL, tokens Web JSON assinados ou até mesmo mensagens de autenticação WebAuthn. Essa versão adiciona suporte para relatar *Weak Cryptographic Implementation* em Java.

Suporte a Jakarta EE (versão com suporte: 9.0.0)

O Jakarta EE fornece um conjunto de especificações abrangente, neutro e aberto ao fornecedor na forma de uma estrutura de código aberto usada para desenvolver aplicativos Java nativos da nuvem. Anteriormente era conhecido como Java EE (ou J2EE), que era uma das estruturas mais reconhecidas para Java do lado do servidor. Essa versão adiciona melhorias à cobertura de Java EE existente, abrangendo 52 categorias de vulnerabilidades.

Melhorias no secret scanning

O secret scanning é uma técnica para pesquisar e detectar segredos no código-fonte e nos arquivos de configuração. Às vezes, os arquivos de configuração que contêm senhas ou tokens de API podem vazar acidentalmente para os repositórios de código-fonte. Essa versão inclui suporte para formatos de hash de senha comuns. A cobertura inclui a identificação de formatos de hash de senha comuns e segredos em arquivos de configuração para produtos, incluindo o seguinte: OpenVPN, Windows Remote Desktop, netrc, IntelliJ IDEA, DBeaver, FileZilla, Heroku, and DigitalOcean doctl.
A cobertura aprimorada é fornecida para as seguintes categorias:

- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key
- Password Management: Hardcoded Password
- Password Management: Password in Configuration File
- Password Management: Weak Cryptography

Melhorias no Express JS (versão com suporte: 4.x)[1]

Express é uma estrutura para criar aplicativos da Web com Node.js. Ele fornece funcionalidade para roteamento, tratamento de erros, modelagem, gerenciamento de middleware e utilitários relacionados a HTTP. Nessa versão, melhoramos o suporte ao Express 4.x para as seguintes categorias:

- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute
- Insecure Transport
- Path Manipulation
- Privacy Violation

[1] Requer a versão 22.1.1 do SCA

- Process Control
- Setting Manipulation
- System Information Leak: External

Handlebars JavaScript (versão com suporte: 4.7.7)

Handlebars é uma biblioteca JavaScript projetada para criar modelos da Web reutilizáveis. Esses modelos são uma combinação de HTML, texto e expressões. As expressões são incorporadas diretamente no código HTML e servem como um espaço reservado para o conteúdo que deve ser inserido por código, tornando o documento facilmente reutilizável.
Nessa versão, adicionamos suporte para Handlebars 4.7.7, cobertura de fluxo de dados aprimorada e cobertura de API expandida para as seguintes categorias:

- Cross-Site Scripting: Handlebars Helper
- Handlebars Misconfiguration: Escaping Disabled
- Handlebars Misconfiguration: Prototypes Allowed
- Log Forging
- Log Forging (debug)
- Privacy Violation
- System Information Leak
- Template Injection

JavaScript Mustache (versão com suporte: 4.2.0)

Mustache é um sistema de modelo sem lógica de código aberto que fornece modelos e visualizações como base para a criação de modelos dinâmicos. Os modelos contêm o formato e o código da apresentação, enquanto as visualizações contêm os dados a serem incluídos nos modelos.
Nessa versão, adicionamos suporte ao Mustache 4.2.0 para identificar as vulnerabilidades de *Template Injection*.

GraphQL.js (versão com suporte: 16.5.0)

GraphQL.js é a implementação de referência JavaScript para GraphQL e é amplamente usado em aplicativos JavaScript. Essa versão adiciona suporte inicial ao servidor GraphQL para detectar as seguintes categorias de vulnerabilidade nas APIs do GraphQL:

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- GraphQL Bad Practices: Introspection Enabled
- GraphQL Bad Practices: GraphiQL Enabled
- Privacy Violation
- System Information Leak: External

Graphene-Python (versão com suporte: 3.0.0)

Python-Graphene é uma estrutura de servidor GraphQL popular para aplicativos Python. Essa versão aprimora nosso suporte ao servidor GraphQL a partir de 2022.1.0 para detectar as seguintes categorias de vulnerabilidade nas APIs do GraphQL:

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Privacy Violation
- System Information Leak: External

Infraestrutura como código da nuvem

Infraestrutura como código (IaC) é o processo de gerenciamento e provisionamento de recursos de computador por meio de código, em vez de vários processos manuais. Essa versão adiciona suporte expandido para IaC. As tecnologias com suporte incluem configurações do Ansible para implantação no Azure e configurações da AWS e do Terraform para implantação no Azure e GCP. Problemas comuns relacionados à configuração dos serviços mencionados agora são relatados ao desenvolvedor.

Configurações do Terraform:

Terraform é uma infraestrutura de código aberto como ferramenta de código para criar, alterar e controlar a versão da infraestrutura da nuvem. Ele usa sua própria linguagem declarativa conhecida como HashiCorp Configuration Language (HCL). A infraestrutura da nuvem é codificada em arquivos de configuração para descrever o estado desejado.

Os provedores do Terraform oferecem suporte à configuração e gerenciamento da infraestrutura do ***Microsoft Azure***. Nessa versão, relatamos as seguintes categorias para configurações do Terraform dos serviços do Microsoft Azure:

- Azure Terraform Misconfiguration: Insecure App Service Transport
- Azure Terraform Misconfiguration: Insecure CDN Endpoint Transport
- Azure Terraform Misconfiguration: Insecure Function App Transport
- Azure Terraform Misconfiguration: Insecure Logic App Transport
- Azure Terraform Misconfiguration: Insecure MariaDB Transport
- Azure Terraform Misconfiguration: Insecure MySQL Transport
- Azure Terraform Misconfiguration: Insecure Network Monitor Transport
- Azure Terraform Misconfiguration: Insecure PostgresSQL Transport
- Azure Terraform Misconfiguration: Insecure Redis Cache Transport
- Azure Terraform Misconfiguration: Insecure Spring Cloud Redis Transport
- Azure Terraform Misconfiguration: Insecure Spring Cloud Transport
- Azure Terraform Misconfiguration: Insecure Storage Account Transport

Os provedores do Terraform são compatíveis com a configuração e o gerenciamento da infraestrutura do ***Google Cloud Platform (GCP)***. Nessa versão, relatamos as seguintes categorias para configurações do Terraform do Google Cloud Platform:

- GCP Terraform Bad Practice: Overly Permissive Service Account
- GCP Terraform Misconfiguration: BigQuery Dataset Publicly Accessible

- GCP Terraform Misconfiguration: Cloud DNS DNSSEC Disabled
- GCP Terraform Misconfiguration: Cloud KMS CryptoKey Publicly Accessible
- GCP Terraform Misconfiguration: Cloud SQL Backup Disabled
- GCP Terraform Misconfiguration: Cloud Storage Bucket Publicly Accessible
- GCP Terraform Misconfiguration: Compute Engine Access Control
- GCP Terraform Misconfiguration: Compute Engine Default Service Account
- GCP Terraform Misconfiguration: Compute Engine Project-Wide SSH
- GCP Terraform Misconfiguration: Google Project Network Access Control
- GCP Terraform Misconfiguration: Insecure Cloud SQL Transport
- GCP Terraform Misconfiguration: Insecure Load Balancer Transport
- GCP Terraform Misconfiguration: Insufficient Cloud Storage Bucket Logging
- GCP Terraform Misconfiguration: Insufficient GKE Cluster Logging
- GCP Terraform Misconfiguration: Insufficient GKE Cluster Monitoring
- GCP Terraform Misconfiguration: Insufficient VPC Flow Logging
- GCP Terraform Misconfiguration: GKE Cluster Administrative Interface Access Control
- GCP Terraform Misconfiguration: GKE Cluster Certificate-Based Authentication
- GCP Terraform Misconfiguration: GKE Cluster Legacy Authorization
- GCP Terraform Misconfiguration: GKE Cluster HTTP Basic Authentication
- GCP Terraform Misconfiguration: GKE Container-Optimized OS Not In Use
- GCP Terraform Misconfiguration: GKE Node Auto-Upgrade Disabled
- GCP Terraform Misconfiguration: Weak Cryptographic Cloud DNS Signature
- GCP Terraform Misconfiguration: Weak GKE Cluster Network Management
- GCP Terraform Misconfiguration: Weak Key Management

Configurações do Ansible:
Ansible é uma ferramenta de automação de código aberto que fornece gerenciamento de configuração, implantação de aplicativos, provisionamento de nuvem e orquestração de nós para vários ambientes.

O Ansible inclui módulos que oferecem suporte à configuração e ao gerenciamento da ***Amazon Web Services (AWS)***. Nessa versão, relatamos as seguintes categorias para configurações do Ansible da AWS:

- AWS Ansible Misconfiguration: Amazon RDS Publicly Accessible
- AWS Ansible Misconfiguration: Insecure CloudFront Distribution Transport
- AWS Ansible Misconfiguration: Insufficient CloudTrail Logging

O Ansible também inclui módulos que dão suporte à configuração e gerenciamento de ***Serviços de Computação em Nuvem do Microsoft Azure***. Nessa versão, relatamos as seguintes categorias para configurações do Ansible do Microsoft Azure:

- Azure Ansible Misconfiguration: Overly Permissive Azure SQL Database Firewall

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:

Log4j (versão com suporte: 2.17)

O suporte para Log4j agora inclui a detecção de uma nova categoria, *Denial of Service: Stack Exhaustion*.

Oslo.config (versão com suporte: 8.8.0)

O suporte inicial para oslo.config para Python inclui a detecção de uma nova categoria, *Privacy Violation: Unobfuscated Logging*.

Correções de erros e melhorias de desempenho do Objective-C

Os clientes que verificaram seus projetos que incluem arquivos Objective-C usando os pacotes de regras 2022R1 podem ter encontrado os seguintes problemas:

- Durante a fase de verificação, mensagens de erro na forma de "[error] Unexpected exception during dataflow analysis..." podem aparecer na saída do SCA ou nos arquivos de log
- Tempo de verificação extraordinariamente longo na análise de fluxo de dados, o que pode resultar em perda de problemas de fluxo de dados

Um pacote de regras de hotfix do Objective-C foi fornecido aos clientes afetados para resolver esses problemas. A mesma correção está incluída nessa versão oficial do R2. Os clientes que estavam usando o pacote de regras do hotfix devem remover o pacote de regras do hotfix ao atualizar para os pacotes de regras da versão R2.

Melhorias em falsos positivos:

O trabalho continuou com o esforço para remover falsos positivos nessa versão. Além de outras melhorias, os clientes podem esperar uma maior remoção de falsos positivos nas seguintes áreas:

- *SQL Injection: iBatis Data Map*: falsos positivos são evitados quando caracteres literais '$' são encontrados
- *Password Management: Password in Configuration File*: falsos positivos são evitados quando o valor é um espaço reservado de variável
- *ASP.NET MVC Bad Practices: Model With Required Non-Nullable Property:* falsos positivos são evitados em aplicativos C# ASP.NET ao usar o atributo [BindRequired]
- *Often Misused: Authentication*: falsos positivos são evitados em aplicativos Java
- *XSS: Content Sniffing:* falsos positivos são evitados em aplicativos Java Spring
- *Privacy Violation:* falsos positivos são evitados em aplicativos .NET
- *SOQL Injection* and *SOSL Injection:* os problemas encontrados pelo analisador semântico agora serão relatados com Ordem de Prioridade Baixa da Fortify

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

OGNL Expression Injection: Double Evaluation

Uma vulnerabilidade crítica de OGNL Expression Injection identificada pelo CVE-2022-26134 afeta o Atlassian Confluence Server e o Data Center. Essa vulnerabilidade permite que um invasor não autenticado execute código arbitrário em aplicativos vulneráveis. As versões afetadas do Confluence Server e Data Center são 1.3.0 a 7.4.16, 7.13.0 a 7.13.6, 7.14.0 a 7.14.2, 7.15.0 a 7.15.1, 7.16.0 a 7.16.3, 7.17.0 a 7.17.3 e 7.18.0. Essa versão inclui uma verificação para detectar essa vulnerabilidade nos servidores Confluence e Data Center afetados.

Dynamic Code Evaluation: Code Injection

O Spring Framework da Pivotal foi considerado vulnerável a uma vulnerabilidade de execução remota de código (RCE) identificada pelo CVE-2022-22965. Um invasor remoto pode fornecer parâmetros de solicitação especialmente criados que podem levar à execução arbitrária de código. Essa versão inclui uma verificação para detectar essa vulnerabilidade em aplicativos Web com as versões afetadas do Spring Framework.

Insecure Deployment: OpenSSL

OpenSSL, uma biblioteca de criptografia popular amplamente usada para permitir conexões SSL/TLS, foi considerada vulnerável a uma vulnerabilidade de negação de serviço (DoS) identificada pelo CVE-2022-0778. É possível acionar um DoS de loop infinito no sistema afetado criando um certificado que tenha parâmetros de curva elíptica explícitos inválidos. Essa versão inclui uma verificação para detectar a vulnerabilidade CVE-2022-0778 nos servidores Web de destino. Como essa verificação tem o potencial de causar uma condição DoS no sistema afetado que resulta na indisponibilidade do serviço, essa verificação não está incluída na política padrão. Use a política Todas as Verificações, personalize uma política existente para incluir a verificação ou crie uma política personalizada para executar essa verificação.

Erratas diversas

Nessa versão, continuamos a investir recursos para reduzir 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 ao seguinte:

Password Management: Weak Password Policy

Essa versão inclui pequenas melhorias para a verificação da política de senha em que os campos de senha/nome de usuário são reconhecidos com maior precisão quando o tipo de entrada é uma caixa de texto.

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. Os clientes que procuram o site anterior com a última atualização com suporte, podem acessá-lo no Portal de suporte da 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, Pesquisa de Segurança de Software
CyberRes Fortify
hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
Gerente, Pesquisa de Segurança de Software
CyberRes Fortify
peter.blay@microfocus.com