Conteúdo de Segurança de Software do Fortify

Atualização 2 de 2023
sexta-feira, 30 de junho 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 Fortify Static Code Analyzer (SCA) e o Fortify WebInspect. Atualmente, o Conteúdo de Segurança de Software da Fortify oferece suporte a 1.552 categorias de vulnerabilidade em 31 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 o Fortify Secure Coding Rulepacks (idioma inglês, versão 2023.2.0), o Fortify WebInspect SecureBase (disponível via SmartUpdate) e o Fortify Premium Content.

Fortify Secure Coding Rulepacks [Fortify Static Code Analyzer]

Nesta versão, os Fortify Secure Coding Rulepacks detectam 1.329 categorias únicas de vulnerabilidades em mais de 31 linguagens e abrangem mais de um milhão de APIs individuais. Em resumo, essa versão inclui o seguinte:

Suporte para Dart (versão compatível: 2.19.6)[1]

O kit de desenvolvimento de software (SDK) da Dart, desenvolvido pelo Google, fornece uma linguagem de programação fortemente tipada, baseada em classe e de coleta de lixo para a criação de aplicativos móveis, Web e de desktop. A Dart oferece versatilidade permitindo que os aplicativos sejam compilados em código de máquina específico da arquitetura, módulos portáteis ou JavaScript, dependendo do caso de uso pretendido. Com a Dart, os desenvolvedores podem criar aplicativos acompanhados de interfaces gráficas de usuário (GUIs), tornando-o uma opção flexível para criar uma ampla variedade de soluções de software. As categorias com suporte incluem:

- Access Control: Database
- Command Injection
- Denial of Service
- Denial of Service: Regular Expression
- Header Manipulation
- Insecure Transport
- Open Redirect
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Path Manipulation
- Privacy Violation
- Resource Injection
- Server-Side Request Forgery
- SQL Injection
- System Information Leak
- System Information Leak: Internal

Suporte inicial para Flutter (versão compatível: 3.7.11)[1]

O Flutter, um SDK de interface de usuário (UI) de código aberto criado pelo Google, aproveita o poder da linguagem de programação Dart. Ele fornece aos desenvolvedores um conjunto abrangente de ferramentas, bibliotecas e pacotes para facilitar a criação de aplicativos multiplataforma. Com o Flutter, os desenvolvedores podem criar aplicativos móveis, Web e de desktop por meio de uma única base de código, simplificando o processo de desenvolvimento e reduzindo tempo e esforço. Aproveitando os recursos do Flutter, os desenvolvedores podem criar aplicativos visualmente atraentes e de alto desempenho que são executados perfeitamente em várias plataformas. O suporte para Flutter inclui

[1] Requer o Fortify Static Code Analyzer 23.1.0. Para obter melhores resultados, use o Fortify Static Code Analyzer 23.1.1.

rastreamento de entrada fornecida pelo usuário, detecção de todas as categorias permitidas para a linguagem de programação Dart e as seguintes categorias especificamente para GUIs do Flutter:

- Privacy Violation: Shoulder Surfing
- System Information Leak: Internal

Android 13 (nível da API: 33)

A plataforma Android é uma pilha de software de código aberto projetada para dispositivos móveis. Um componente principal do Android é o Java API Framework, que expõe os recursos do Android para desenvolvedores de aplicativos. Essa versão expande a detecção de vulnerabilidade em aplicativos Android nativos escritos em Java ou Kotlin que utilizam o Java API Framework do Android. Cinco novas categorias de pontos fracos são introduzidas nesta versão para aplicativos Android:

- Privacy Violation: Android Insecure Indexing
- Privilege Management: Android Nearby Devices
- Privilege Management: Android Notifications
- Privilege Management: Android Read Aural Media
- Privilege Management: Android Read Visual Media

Atualizações adicionais do Android estão incluídas para oferecer suporte à detecção de categorias de fraqueza existentes nos seguintes namespaces:

- android.app
- android.content
- android.net
- android.os
- android.util
- java.nio
- java.security
- java.security.interfaces

Java SE JDK (versão compatível: 17)

O Java Platform, Standard Edition (SE) Java Development Kit (JDK) é um pacote de desenvolvimento de software que contém ferramentas e bibliotecas usadas para desenvolver aplicativos e componentes Java. Essa versão inclui suporte atualizado de categorias de fraqueza existentes nos seguintes namespaces para novas APIs introduzidas no Java SE JDK 15, 16 e 17:

- java.io
- java.lang
- java.lang.reflect
- java.net
- java.nio.channels
- java.util
- java.util.random
- java.util.stream

A cobertura de varredura aprimorada pode incluir problemas adicionais identificados nas seguintes categorias:

- Insecure Randomness
- Insecure Randomness: Hardcoded Seed
- Insecure Randomness: User-Controlled Seed
- Server-Side Request Forgery
- Setting Manipulation
- Unsafe Reflection

Atualizações da biblioteca padrão Kotlin (versão compatível: 1.7.21)

Kotlin é uma linguagem de uso geral, de tipagem estática, com interoperabilidade Java. Essa versão inclui suporte atualizado para novas APIs de biblioteca padrão introduzidas nas versões 1.6 e 1.7 da Kotlin voltadas para a Java Virtual Machine (JVM).

Atualização do Secret Scanning

O Secret Scanning é uma técnica para pesquisar automaticamente segredos no código-fonte e nos arquivos de configuração. Nesse contexto, "segredos" referem-se a senhas, tokens de API, chaves de criptografia e artefatos semelhantes destinados a serem mantidos em segredo. Essa versão inclui suporte atualizado para secret scanning nas seguintes categorias:

- Credential Management: Hardcoded API Credentials
- Key Management: Hardcoded Encryption Key
- Password Management: Hardcoded Password

Além disso, o secret scanning em scripts do PowerShell agora é compatível com as seguintes categorias:

- Password Management: Hardcoded Password
- Privacy Violation

Infraestrutura como código (IaC) da nuvem

Infraestrutura como código é o processo de gerenciamento e provisionamento de recursos de computador por meio de código, em vez de vários processos manuais. A cobertura expandida das tecnologias com suporte inclui configurações do Terraform para implantação na Amazon Web Services (AWS) e no Google Cloud Platform (GCP), bem como configurações para o AWS CloudFormation. Problemas comuns relacionados à configuração desses serviços mencionados agora são relatados ao desenvolvedor.

Configurações do AWS Terraform

Terraform é uma ferramenta de IaC de código aberto 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 ao gerenciamento da infraestrutura da AWS. Nessa versão, relatamos as seguintes categorias adicionais para configurações do Terraform:

- AWS Terraform Misconfiguration: Aurora Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: CloudWatch Missing Customer-Managed Encryption Key

- AWS Terraform Misconfiguration: Database Migration Service Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: DocumentDB Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: ElastiCache Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: Improper API Gateway Access Control
- AWS Terraform Misconfiguration: Improper EC2 Network Access Control
- AWS Terraform Misconfiguration: Improper ECR Access Control
- AWS Terraform Misconfiguration: Improper EKS Network Access Control
- AWS Terraform Misconfiguration: Improper ElastiCache Network Access Control
- AWS Terraform Misconfiguration: Improper Lambda Access Control
- AWS Terraform Misconfiguration: Improper MSK Network Access Control
- AWS Terraform Misconfiguration: Improper Neptune Access Control
- AWS Terraform Misconfiguration: Improper RDS Network Access Control
- AWS Terraform Misconfiguration: Improper S3 Access Control
- AWS Terraform Misconfiguration: Improper VPC Network Access Control
- AWS Terraform Misconfiguration: Insecure API Gateway Storage
- AWS Terraform Misconfiguration: Insecure API Gateway Transport
- AWS Terraform Misconfiguration: Insecure App Sync Storage
- AWS Terraform Misconfiguration: Insecure Athena Storage
- AWS Terraform Misconfiguration: Insecure CloudFront Transport
- AWS Terraform Misconfiguration: Insecure DynamoDB Storage
- AWS Terraform Misconfiguration: Insecure EC2 Storage
- AWS Terraform Misconfiguration: Insecure ECR Storage
- AWS Terraform Misconfiguration: Insecure ECS Transport
- AWS Terraform Misconfiguration: Insecure EKS Storage
- AWS Terraform Misconfiguration: Insecure ElastiCache Storage
- AWS Terraform Misconfiguration: Insecure Glue Storage
- AWS Terraform Misconfiguration: Insecure Kinesis Storage
- AWS Terraform Misconfiguration: Insecure MQ Storage
- AWS Terraform Misconfiguration: Insecure OpenSearch Service Storage
- AWS Terraform Misconfiguration: Insecure OpenSearch Service Transport
- AWS Terraform Misconfiguration: Insecure RDS Transport
- AWS Terraform Misconfiguration: Insecure S3 Storage
- AWS Terraform Misconfiguration: Insecure SageMaker Storage
- AWS Terraform Misconfiguration: Insufficient API Gateway Logging
- AWS Terraform Misconfiguration: Insufficient Aurora Backup
- AWS Terraform Misconfiguration: Insufficient CloudFront Logging
- AWS Terraform Misconfiguration: Insufficient CloudTrail Logging
- AWS Terraform Misconfiguration: Insufficient EC2 Logging
- AWS Terraform Misconfiguration: Insufficient ELB Logging
- AWS Terraform Misconfiguration: Insufficient ElastiCache Backup
- AWS Terraform Misconfiguration: Insufficient ElastiCache Logging
- AWS Terraform Misconfiguration: Insufficient Global Accelerator Logging
- AWS Terraform Misconfiguration: Insufficient GuardDuty Monitoring
- AWS Terraform Misconfiguration: Insufficient Lambda Logging
- AWS Terraform Misconfiguration: Insufficient OpenSearch Service Logging
- AWS Terraform Misconfiguration: Insufficient RDS Backup
- AWS Terraform Misconfiguration: Insufficient Redshift Logging
- AWS Terraform Misconfiguration: Insufficient S3 Backup
- AWS Terraform Misconfiguration: MemoryDB Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: MQ Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: Neptune Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: RDS Auto-Upgrade Disabled
- AWS Terraform Misconfiguration: Reduced CloudFront Availability

- AWS Terraform Misconfiguration: Reduced ELB Availability
- AWS Terraform Misconfiguration: Reduced StackSets Availability
- AWS Terraform Misconfiguration: Weak Cognito Authentication
- AWS Terraform Misconfiguration: Weak IAM Password Policy

Configurações do GCP 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 GCP. Nessa versão, relatamos as seguintes categorias de fraquezas para configurações do GCP Terraform:

- GCP Terraform Misconfiguration: Insufficient Cloud Load Balancing Logging
- GCP Terraform Misconfiguration: Insufficient Cloud NAT Logging
- GCP Terraform Misconfiguration: Insufficient Media CDN Logging
- GCP Terraform Misconfiguration: Insufficient Operations Suite Logging

Configurações do AWS CloudFormation

O CloudFormation é um serviço fornecido pela Amazon usado para automatizar o provisionamento e a configuração dos recursos da AWS. O CloudFormation permite que os usuários gerenciem recursos da AWS usando um modelo JSON ou YAML. Nessa versão, relatamos as seguintes categorias de fraquezas para configurações do AWS CloudFormation:

- AWS CloudFormation Misconfiguration: AmazonMQ Publicly Accessible
- AWS CloudFormation Misconfiguration: Backup Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: CloudTrail Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DataBrew Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DMS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DMS Publicly Accessible
- AWS CloudFormation Misconfiguration: DocDB Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DocDBElastic Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: DynamoDB Backup Disabled
- AWS CloudFormation Misconfiguration: EC2 Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: ECR Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: EFS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: ElastiCache Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: FinSpace Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: FSx Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: ImageBuilder Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Improper Athena Access Control
- AWS CloudFormation Misconfiguration: Improper CodeStar Access Control
- AWS CloudFormation Misconfiguration: Improper Cognito Access Control
- AWS CloudFormation Misconfiguration: Improper ECS Network Access Control
- AWS CloudFormation Misconfiguration: Improper EMR Access Control
- AWS CloudFormation Misconfiguration: Improper KMS Access Control
- AWS CloudFormation Misconfiguration: Improper Lambda Network Access Control
- AWS CloudFormation Misconfiguration: Improper Lightsail Access Control
- AWS CloudFormation Misconfiguration: Improper M2 Access Control

- AWS CloudFormation Misconfiguration: Improper QLDB Access Control
- AWS CloudFormation Misconfiguration: Improper RDS Access Control
- AWS CloudFormation Misconfiguration: Improper Redshift Access Control
- AWS CloudFormation Misconfiguration: Improper S3 Access Control
- AWS CloudFormation Misconfiguration: Improper SageMaker Access Control
- AWS CloudFormation Misconfiguration: Improper SageMaker Network Access Control
- AWS CloudFormation Misconfiguration: Improper Serverless Network Access Control
- AWS CloudFormation Misconfiguration: Improper Transfer Network Access Control
- AWS CloudFormation Misconfiguration: Insecure API Gateway Transport
- AWS CloudFormation Misconfiguration: Insecure CloudFront Transport
- AWS CloudFormation Misconfiguration: Insecure DAX Storage
- AWS CloudFormation Misconfiguration: Insecure ECR Supply Chain
- AWS CloudFormation Misconfiguration: Insecure EFS Storage
- AWS CloudFormation Misconfiguration: Insecure ELB Transport
- AWS CloudFormation Misconfiguration: Insecure Elasticsearch Storage
- AWS CloudFormation Misconfiguration: Insecure Elasticsearch Transport
- AWS CloudFormation Misconfiguration: Insecure WorkSpaces Storage
- AWS CloudFormation Misconfiguration: Insufficient API Gateway Logging
- AWS CloudFormation Misconfiguration: Insufficient AppSync Logging
- AWS CloudFormation Misconfiguration: Insufficient CloudFront Logging
- AWS CloudFormation Misconfiguration: Insufficient CloudFront Monitoring
- AWS CloudFormation Misconfiguration: Insufficient CloudTrail Monitoring
- AWS CloudFormation Misconfiguration: Insufficient Config Monitoring
- AWS CloudFormation Misconfiguration: Insufficient ECR Monitoring
- AWS CloudFormation Misconfiguration: Insufficient ELB Logging
- AWS CloudFormation Misconfiguration: Insufficient ElasticLoadBalancing Logging
- AWS CloudFormation Misconfiguration: Insufficient Elasticsearch Logging
- AWS CloudFormation Misconfiguration: Insufficient GuardDuty Monitoring
- AWS CloudFormation Misconfiguration: Insufficient Lambda Logging
- AWS CloudFormation Misconfiguration: Insufficient MQ Logging
- AWS CloudFormation Misconfiguration: Insufficient MSK Logging
- AWS CloudFormation Misconfiguration: Insufficient OpenSearch Service Logging
- AWS CloudFormation Misconfiguration: Insufficient RDS Monitoring
- AWS CloudFormation Misconfiguration: Insufficient Route 53 Logging
- AWS CloudFormation Misconfiguration: Insufficient Serverless Logging
- AWS CloudFormation Misconfiguration: Insufficient Stack Monitoring
- AWS CloudFormation Misconfiguration: Kinesis Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Lambda Denial of Service
- AWS CloudFormation Misconfiguration: Location Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Logs Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: M2 Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: MemoryDB Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Neptune Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Privileged Batch Container
- AWS CloudFormation Misconfiguration: RDS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: RDS Publicly Accessible
- AWS CloudFormation Misconfiguration: Redshift Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Reduced EC2 Availability
- AWS CloudFormation Misconfiguration: Reduced ElastiCache Availability

- AWS CloudFormation Misconfiguration: Reduced Stack Availability
- AWS CloudFormation Misconfiguration: Rekognition Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: S3 Backup Disabled
- AWS CloudFormation Misconfiguration: SQS Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: SageMaker Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Secrets Manager Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Serverless Denial of Service
- AWS CloudFormation Misconfiguration: Timestream Missing Customer-Managed Encryption Key
- AWS CloudFormation Misconfiguration: Weak API Gateway Authentication
- AWS CloudFormation Misconfiguration: Weak Certificate Manager Authentication
- AWS CloudFormation Misconfiguration: Weak IAM Authentication
- AWS CloudFormation Misconfiguration: Weak Lambda Authentication
- AWS CloudFormation Misconfiguration: Weak RDS Authentication

Atualização de expressões regulares personalizáveis de Gerenciamento de Senhas
As expressões regulares personalizáveis de Gerenciamento de Senhas para scripts do Salesforce Apex, da Dart e do PowerShell agora podem ser especificadas usando as seguintes propriedades:

- com.fortify.sca.rules.password_regex.apex
- com.fortify.sca.rules.password_regex.dart
- com.fortify.sca.rules.password_regex.powershell

Essas propriedades podem ser usadas para substituir as expressões regulares padrão usadas para identificar senhas ao verificar o código-fonte do Salesforce Apex, o código-fonte da Dart ou os scripts do PowerShell.

OWASP Mobile Application Security Verification Standard (MASVS) v2.0.0

O padrão OWASP MASVS v2.0.0 foi lançado em abril de 2023 como parte do projeto OWASP Mobile Application Security (MAS). Ele oferece uma linha de base para os requisitos de segurança de aplicativos móveis e destina-se a ser usado por arquitetos, desenvolvedores e testadores de software móvel. OWASP MASVS 2.0 destina-se a se concentrar na segurança do aplicativo móvel “cliente” em execução no dispositivo móvel. Como tal, deve ser usado em combinação com o OWASP ASVS para avaliar os riscos relacionados à segurança de aplicativos do lado do servidor relacionados a controles para terminais remotos. Para oferecer suporte a nossos clientes no desenvolvimento de aplicativos móveis seguros e na avaliação de aplicativos móveis para cobertura de controle de segurança e mitigação de riscos, uma correlação da Fortify Taxonomy com o OWASP MASVS v2.0.0 foi adicionada.

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:

Depreciação da categoria "Access Control"

A categoria *Access Control* para Salesforce Apex foi removida nesta versão. A falta de verificações de segurança em nível de campo agora é capturada indiretamente por meio de outras categorias, como *Access Control: Database* e *SOQL Injection*.

Remoção da categoria "Link Injection: Auto Dial"

A categoria *Link Injection: Auto Dial* foi removida por estar desatualizada. A categoria foi introduzida para abordar o CVE-2017-2484, em que a entrada não sanitizada do usuário em aplicativos iOS pode ser explorada por invasores para discar automaticamente números de telefone ou chamadas do Facetime. Essa exploração foi corrigida na atualização do iOS 10.3, portanto, não é mais relevante para os aplicativos iOS atuais.

Mapeamentos de padrões obsoletos

Os seguintes padrões e práticas recomendadas foram marcados como obsoletos, para que não apareçam por padrão:

- CWE Top 25 2019
- CWE Top 25 2020
- DISA STIG 4.9
- DISA STIG 4.10
- OWASP Top 10 2004
- OWASP Top 10 2007
- OWASP Top 10 2010
- SANS Top 25 2009
- SANS Top 25 2010
- WASC 24 + 2

Funções Dinâmicas do PHP[2]

O mais recente Fortify Static Code Analyzer inclui suporte ao PHP atualizado, permitindo o relatório de problemas de *Dynamic Code Evaluation: Code Injection* em relação a funções dinâmicas que são referenciadas por entrada externa não sanitizada.

Classe insegura Java

No Java JDK, há uma classe oculta para executar ações inerentemente inseguras que normalmente não estão disponíveis para desenvolvedores que requerem reflexão para instanciar. Agora, ao usar a classe `sun.misc.Unsafe` em projetos Java, os resultados da verificação relatarão qualquer uso como *Often Misused: sun.misc.Unsafe.*

[2] Requer SCA 23.1 e superior

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:

- *Access Control: Unenforced Sharing Rules* – falsos positivos removidos em disparadores do Salesforce, páginas do Visualforce e componentes
- *Command Injection* – falsos positivos removidos ao sinalizar em expressões regulares no JavaScript
- *Cookie Security: Cookie not Sent Over SSL* – falsos positivos removidos no Swift quando a correção recomendada é aplicada
- *Credential Management: Hardcoded API Credentials* – falsos positivos removidos ao identificar tokens de portador
- *Dead Code: Expression is Always false* – falsos positivos removidos quando aparecem em instruções de switch Java
- *Dockerfile Misconfiguration: Dependency Confusion* – falsos positivos removidos nos comandos "apt" e "apt-get" nos dockerfiles
- *Log Forging (debug)* – falsos positivos removidos em aplicativos Salesforce Apex ao imprimir valores de cabeçalho de solicitação HTTP
- *Race Condition: Signal Handling* – falsos positivos removidos em C/C++ ao invocar `sigaction()`
- *String Termination Error* – falsos positivos removidos ao disparar em tipos primitivos em C++
- *Unused Method* – falsos positivos removidos no código Java em que o método é chamado por um método serializável implementado
- Foram removidos falsos positivos do Dataflow em JavaScript que poderiam ter sido acionados em valores boolianos

Mudanças de categoria

Quando ocorrerem alterações no nome da categoria de vulnerabilidade, os resultados da análise ao mesclar verificações anteriores com novas verificações resultarão em categorias adicionadas/removidas.

Para melhorar a consistência, as seguintes categorias foram renomeadas:

- *Azure Terraform Misconfiguration: Improper CosmosDB CORS Policy* agora é relatada como *Azure Terraform Misconfiguration: Improper Cosmos DB CORS Policy*
- *Kubernetes Misconfiguration: Missing ServiceAccount Admission Controller* agora é relatada como *Kubernetes Misconfiguration: Missing Service Account Admission Controller*
- *NoSQL Injection: CosmosDB* agora é relatada como *NoSQL Injection: Cosmos DB*

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: Unpatched Application:

ZK Framework, uma biblioteca Java de código aberto usada para criar aplicativos corporativos móveis e da Web, contém uma vulnerabilidade de segurança identificada por CVE-2022-36537. Os invasores podem explorar essa vulnerabilidade para recuperar o conteúdo de um arquivo localizado no contexto da Web. A exploração bem-sucedida permite que um invasor obtenha informações confidenciais ou atinja um endpoint que, de outra forma, poderia ser inacessível. Essa versão inclui uma verificação para detectar essa vulnerabilidade em servidores de destino que usam as versões afetadas da ZK Framework.

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 ao seguinte:

Command Injection:

As verificações identificadas pelos ID 11722 e 11723 foram modificadas para usar cargas úteis compatíveis com o recurso Out-of-band Application Security Testing (OAST)[3]. Elas reduzem os falsos positivos e aumentam a precisão dos resultados da verificação do WebInspect.

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 MASVS v2.0.0

Para acompanhar as novas correlações, essa versão também contém um novo pacote de relatórios para o Fortify Software Security Center com suporte para OWASP MASVS v2.0.0, que está disponível para download no Portal de Suporte ao Cliente Fortify em Conteúdo Premium.

[3] Como a verificação 11723 envia um número significativo de solicitações, ela é excluída da 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.

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.
Uma nova versão fora da nuvem do site Fortify Taxonomy, consistente com o site ao vivo acima, agora está disponível para os clientes baixarem no Fortify Support Portal.

Entre em contato com o suporte técnico 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