Conteúdo de Segurança de Software do Fortify

Atualização 3 de 2023
sexta-feira, 29 de setembro 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 1.627 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 2023.3.0), 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 1.403 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 Android 13 (versão compatível: 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. as seguintes três categorias de pontos fracos são introduzidas nesta versão para aplicativos Android:

- Intent Manipulation: Implicit Internal Intent
- Intent Manipulation: Implicit Pending Intent
- Intent Manipulation: Mutable Pending Intent

Suporte inicial para Android Jetpack (AndroidX)

O Android Jetpack é um conjunto de bibliotecas, ferramentas e orientações que ajuda os desenvolvedores a criar aplicativos Android com maior facilidade. O Jetpack abrange os pacotes androidx.* e é desagregado das APIs da plataforma, o que ajuda a facilitar a compatibilidade com versões anteriores e permite atualizações mais frequentes. Nesta versão, fornecemos cobertura inicial para este pacote de software.

A cobertura inicial do Android Jetpack oferece suporte à detecção de pontos fracos nas seguintes bibliotecas:

- androidx.appsearch (version supported: 1.1.0-alpha03)
- androidx.compose.foundation (version supported: 1.5.1)
- androidx.compose.material (version supported: 1.5.1)
- androidx.compose.material3 (version supported: 1.1.2)
- androidx.compose.ui (version supported: 1.5.1)
- androidx.core (version supported: 1.12.0)
- androidx.credentials (version supported: 1.2.0-beta04)
- androidx.datastore (version supported: 1.0.0)
- androidx.security.crypto (version supported: 1.0.0)
- androidx.sqlite (version supported: 2.3.1)

Exemplos de melhorias na cobertura de categoria incluem o seguinte:

- 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 ao MySQL Connector/Python (versão compatível: 8.1.0)

O MySQL Connector/Python é uma biblioteca de software que facilita a interação entre aplicativos Python e bancos de dados MySQL. Ele serve como uma ponte ou um conector entre a linguagem de programação Python e o sistema de gerenciamento de banco de dados MySQL, permitindo que os desenvolvedores conectem, consultem e manipulem facilmente dados em bancos de dados MySQL usando o código Python.

A cobertura de categorias aprimorada inclui:

- Access Control: Database
- Denial of Service
- Insecure Transport: Client Identity Verification Disabled
- Insecure Transport: Database
- Insecure Transport: Weak SSL Protocol
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Weak Cryptography
- Path Manipulation
- Server-Side Request Forgery
- SQL Injection

Suporte aprimorado para Django (versão compatível: 3.2)

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. Nesta versão, atualizamos nossa cobertura existente do Django para oferecer suporte até a versão 3.2.

A cobertura aprimorada inclui os seguintes namespaces: *Django.contrib.auth.models, Django.db.models* e *Django.http.response*. Além disso, a melhor cobertura das categorias de pontos fracos inclui o seguinte:

- Cookie Security: Overly Permissive SameSite Attribute
- Header Manipulation
- Password Management
- Password Management: Empty Password

- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Privacy Violation
- System Information Leak
- System Information Leak: External

Suporte inicial para Bicep (versão compatível: 0.21.1)[1]

O Microsoft Bicep é uma linguagem específica de domínio (DSL) de código aberto para soluções de infraestrutura como código (IaC) desenvolvida pela Microsoft para simplificar e otimizar a implantação de recursos do Azure. Ele serve como uma camada de abstração sobre os modelos do Azure Resource Manager (ARM), oferecendo uma maneira mais intuitiva e legível de definir e gerenciar a infraestrutura do Azure. Com o Bicep, os usuários podem escrever código conciso e legível para descrever os recursos, as configurações e as dependências do Azure.

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

- Azure ARM Misconfiguration: Automation Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Batch Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Cognitive Services Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Databricks Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Event Hubs Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Hardcoded Secret
- Azure ARM Misconfiguration: HTTPS Not Required
- Azure ARM Misconfiguration: Improper AKS Network Access Control
- Azure ARM Misconfiguration: Improper App Service Access Control
- Azure ARM Misconfiguration: Improper Blob Storage Access Control
- Azure ARM Misconfiguration: Improper Compute VM Access Control
- Azure ARM Misconfiguration: Improper Container Registry Network Access Control
- Azure ARM Misconfiguration: Improper CORS Policy
- Azure ARM Misconfiguration: Improper Custom Role Access Control Policy
- Azure ARM Misconfiguration: Improper DocumentDB Network Access Control
- Azure ARM Misconfiguration: Improper KeyVault Access Control Policy
- Azure ARM Misconfiguration: Improper Security Group Network Access Control
- Azure ARM Misconfiguration: Improper SQL Server Network Access Control
- Azure ARM Misconfiguration: Improper Storage Network Access Control
- Azure ARM Misconfiguration: Insecure Active Directory Domain Service Transport
- Azure ARM Misconfiguration: Insecure App Service Transport
- Azure ARM Misconfiguration: Insecure CDN Transport
- Azure ARM Misconfiguration: Insecure Database for MySQL Storage
- Azure ARM Misconfiguration: Insecure Database for PostgreSQL Storage
- Azure ARM Misconfiguration: Insecure DataBricks Storage
- Azure ARM Misconfiguration: Insecure EventHub Storage
- Azure ARM Misconfiguration: Insecure EventHub Transport
- Azure ARM Misconfiguration: Insecure IoT Hub Transport
- Azure ARM Misconfiguration: Insecure MySQL Server Transport
- Azure ARM Misconfiguration: Insecure PostgreSQL Server Transport

[1] Requer o Fortify Static Code Analyzer 23.2.0 e posterior. O conteúdo de segurança inicial do Bicep é distribuído com o Fortify Static Code Analyzer 23.2.x.

- Azure ARM Misconfiguration: Insecure Recovery Services Backup Storage
- Azure ARM Misconfiguration: Insecure Recovery Services Vaults Storage
- Azure ARM Misconfiguration: Insecure Redis Enterprise Transport
- Azure ARM Misconfiguration: Insecure Redis Transport
- Azure ARM Misconfiguration: Insecure Service Bus Storage
- Azure ARM Misconfiguration: Insecure Service Bus Transport
- Azure ARM Misconfiguration: Insecure Storage Account Storage
- Azure ARM Misconfiguration: Insecure Storage Account Transport
- Azure ARM Misconfiguration: Insufficient AKS Monitoring
- Azure ARM Misconfiguration: Insufficient Application Insights Logging
- Azure ARM Misconfiguration: Insufficient Application Insights Monitoring
- Azure ARM Misconfiguration: Insufficient Microsoft Defender Monitoring
- Azure ARM Misconfiguration: Insufficient SQL Server Logging
- Azure ARM Misconfiguration: Insufficient SQL Server Monitoring
- Azure ARM Misconfiguration: IoT Hub Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: NetApp Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Public Access Allowed
- Azure ARM Misconfiguration: Service Bus Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Storage Account Missing Customer-Managed Encryption Key
- Azure ARM Misconfiguration: Weak App Service Authentication
- Azure ARM Misconfiguration: Weak SignalR Authentication
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Privacy Violation
- Privacy Violation: Missing Secure Decorator

Suporte inicial para Solidity (versão compatível: 0.8.x)[2]

O Solidity é uma linguagem de programação orientada a objetos usada para desenvolver contratos inteligentes em vários ambientes de blockchain descentralizados, principalmente no blockchain Ethereum. Os contratos inteligentes gravados no Solidity são executados principalmente em uma máquina virtual Ethereum (EVM), mas também podem ser executados em outras máquinas virtuais compatíveis.

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

- Authorization Bypass: tx.origin
- Code Correctness: Failing Assertion
- Code Correctness: Reentrancy
- Code Correctness: Typographical Error
- Dead Code
- Denial of Service: External Call
- Dynamic Code Evaluation: Delegatecall
- Integer Overflow
- Obsolete
- Often Misused: Block Values
- Poor Style: Confusing Naming

[2] Requer o Fortify Static Code Analyzer 23.2.0 e posterior. O conteúdo de segurança inicial do Solidty é distribuído com o Fortify Static Code Analyzer 23.2.x.

- Poor Style: Variable Never Used
- Solidity Bad Practices: Default Function Visibility
- Solidity Bad Practices: Ether Balance Check
- Solidity Bad Practices: Hardcoded Gas Amount
- Solidity Bad Practices: Lack of Explicit Variable Visibility
- Solidity Bad Practices: Missing Constructor
- Solidity Misconfiguration: Compiler With Known Vulnerabilities
- Solidity Misconfiguration: Floating Pragma
- Unchecked Return Value
- Uninitialized Variable

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 ampliada das tecnologias compatíveis inclui configurações do Terraform para implantação no Microsoft Azure, bem como configurações para o AWS Ansible. Problemas comuns relacionados à configuração desses serviços mencionados agora são relatados ao desenvolvedor.

Configurações do Microsoft Azure 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 do Microsoft Azure. A cobertura aprimorada de categorias de pontos fracos inclui o seguinte para as configurações do Terraform:

- Azure Terraform Misconfiguration: App Service Auto Upgrade Disabled
- Azure Terraform Misconfiguration: Improper AKS Access Control
- Azure Terraform Misconfiguration: Improper AKS Network Access Control
- Azure Terraform Misconfiguration: Improper App Service Access Control
- Azure Terraform Misconfiguration: Improper Cognitive Search Network Access Control
- Azure Terraform Misconfiguration: Improper Container Registry Access Control
- Azure Terraform Misconfiguration: Improper Functions Access Control
- Azure Terraform Misconfiguration: Improper MariaDB Network Access Control
- Azure Terraform Misconfiguration: Improper MySQL Network Access Control
- Azure Terraform Misconfiguration: Improper SQL Database Network Access Control
- Azure Terraform Misconfiguration: Improper Storage Account Access Control
- Azure Terraform Misconfiguration: Improper Virtual Network Access Control
- Azure Terraform Misconfiguration: Insecure Disk Storage
- Azure Terraform Misconfiguration: Insecure PostgreSQL Storage
- Azure Terraform Misconfiguration: Insufficient AKS Monitoring
- Azure Terraform Misconfiguration: Insufficient Application Gateway Monitoring
- Azure Terraform Misconfiguration: Insufficient Defender for Cloud Monitoring
- Azure Terraform Misconfiguration: Insufficient Front Door Monitoring
- Azure Terraform Misconfiguration: Insufficient MariaDB Backup
- Azure Terraform Misconfiguration: Insufficient Monitor Logging
- Azure Terraform Misconfiguration: Insufficient Network Watcher Logging
- Azure Terraform Misconfiguration: Insufficient PostgreSQL Monitoring
- Azure Terraform Misconfiguration: Insufficient SQL Database Monitoring
- Azure Terraform Misconfiguration: Redis Cache Auto Upgrade Disabled

- Azure Terraform Misconfiguration: Reduced Virtual Network Availability
- Azure Terraform Misconfiguration: Weak App Service Authentication
- Azure Terraform Misconfiguration: Weak Functions Authentication
- Azure Terraform Misconfiguration: Weak Linux Virtual Machines Authentication
- Azure Terraform Misconfiguration: Weak Service Fabric Authentication

Configurações do Ansible da Amazon Web Services (AWS)
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). A cobertura aprimorada de categorias de pontos fracos inclui o seguinte para as configurações do AWS Ansible:

- AWS Ansible Misconfiguration: EFS Missing Customer-Managed Encryption Key
- AWS Ansible Misconfiguration: Improper API Gateway Network Access Control
- AWS Ansible Misconfiguration: Improper ECR Access Control
- AWS Ansible Misconfiguration: Improper ECS Network Access Control
- AWS Ansible Misconfiguration: Improper S3 Access Control
- AWS Ansible Misconfiguration: Improper Stack Access Control
- AWS Ansible Misconfiguration: Insecure API Gateway Transport
- AWS Ansible Misconfiguration: Insecure CloudFront Transport
- AWS Ansible Misconfiguration: Insecure CloudTrail Storage
- AWS Ansible Misconfiguration: Insecure CodeBuild Storage
- AWS Ansible Misconfiguration: Insecure RDS Transport
- AWS Ansible Misconfiguration: Insufficient API Gateway Logging
- AWS Ansible Misconfiguration: Insufficient CloudFront Logging
- AWS Ansible Misconfiguration: Insufficient Lambda Logging
- AWS Ansible Misconfiguration: Insufficient RDS Backup
- AWS Ansible Misconfiguration: Insufficient S3 Backup
- AWS Ansible Misconfiguration: Insufficient S3 Logging
- AWS Ansible Misconfiguration: Insufficient S3 Monitoring
- AWS Ansible Misconfiguration: Insufficient Stack Monitoring
- AWS Ansible Misconfiguration: Privileged Batch Container
- AWS Ansible Misconfiguration: RDS Auto-Upgrade Disabled
- AWS Ansible Misconfiguration: RDS Missing Customer-Managed Encryption Key
- AWS Ansible Misconfiguration: Reduced CloudFront Availability
- AWS Ansible Misconfiguration: Reduced EC2 Availability
- AWS Ansible Misconfiguration: Reduced ELB Availability
- AWS Ansible Misconfiguration: Weak IAM Password Policy

2023 Common Weakness Enumeration (CWE™) Top 25
The Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) foi introduzido em 2019 e substitui o SANS Top 25. Lançado em junho de 2023, o 2023 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. Para oferecer suporte a nossos clientes que desejam priorizar suas auditorias em torno das vulnerabilidades críticas mais comumente relatadas no NVD, foi adicionada uma correlação do Fortify Taxonomy com o 2023 CWE Top 25.

OWASP API Security Top 10 2023

O Open Worldwide Application Security Project (OWASP) API Security Top 10 2023 fornece uma lista dos principais riscos de segurança que afetam as APIs em 2023. Seu objetivo é aumentar a conscientização sobre os pontos fracos da segurança de APIs e educar os envolvidos no desenvolvimento e na manutenção de APIs, como desenvolvedores, designers, arquitetos, gerentes e/ou organizações em geral que precisam proteger Web APIs.

O OWASP API Security Top 10 se concentra nos pontos fracos que afetam as Web APIs e não se destina a ser usado apenas por si só, mas sim em combinação com outros padrões e práticas recomendadas para capturar completamente todos os riscos relevantes. Por exemplo: ele deve ser usado em conjunto com o OWASP Top 10 para identificar problemas relacionados à validação de entrada, como injeções. Para dar suporte aos nossos clientes que desejam reduzir o risco dos Aplicativos Web, foi adicionada a correlação do Fortify Taxonomy com o recém-lançado OWASP API Security Top 10 2023.

Center for Internet Security (CIS) Benchmarks

Os Center for Internet Security (CIS) benchmarks são uma coleção de recomendações de configuração segura desenvolvidas pela comunidade que são mapeadas para o CIS Critical Security Controls. O objetivo dessas recomendações é permitir a segurança da infraestrutura de nuvem e demonstrar a conformidade com os padrões do setor. Os CIS benchmarks são atualizados continuamente para se adaptarem ao estado de evolução da segurança cibernética das mais de 25 famílias de produtos de fornecedores cobertas. As famílias de produtos compatíveis incluem as seguintes:

- Amazon Elastic Kubernetes Service (EKS) Benchmark v1.3.0
- Amazon Web Services Foundations Benchmark v2.0.0
- Azure Kubernetes Service (AKS) Benchmark v1.3.0
- Google Cloud Computing Platform Benchmark v2.0.0
- Google Kubernetes Engine (GKE) Benchmark v1.4.0
- Kubernetes Benchmark v1.7.1
- Microsoft Azure Foundations Benchmark v2.0.0

Smart Contract Weakness Classification (SWC)[3]

A Smart Contract Weakness Classification (SWC) é uma estrutura sistemática que categoriza e explica as vulnerabilidades em contratos inteligentes. Ela fornece uma maneira padronizada de entender e abordar os pontos fracos desses códigos autoexecutáveis executados em blockchains como o Ethereum. Notavelmente, o conteúdo do registro de SWC não foi atualizado de forma abrangente desde 2020, resultando em incompletude conhecida, erros e omissões importantes. Para dar suporte aos nossos clientes que desejam reduzir riscos em contratos inteligentes, foi adicionada a correlação do Fortify Taxonomy com a versão atual do SWC.

[3] Requer verificação do Fortify Static Code Analyzer 23.2.0 e posterior.

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

Conforme observado na versão 2022.4, continuamos a oferecer suporte às últimas quatro versões principais do Fortify Static Code Analyzer. Portanto, essa será a última versão do Rulepacks que oferece suporte a versões do Fortify Static Code Analyzer anteriores à 20.x. No próximo lançamento, as versões do Fortify Static Code Analyzer anteriores à 20.x não vão mais carregar o Rulepacks mais recente. Será necessário fazer o downgrade do Rulepacks ou o upgrade da versão do Fortify Static Code Analyzer. Nas versões futuras, vamos continuar a oferecer suporte para as últimas quatro versões principais do Fortify Static Code Analyzer.

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:

- *ASP.NET MVC Bad Practices: Optional Submodel With Required Property* — remoção de falsos positivos relacionados a campos virtuais em aplicativos ASP.NET
- *Code Correctness: Double-Checked Locking* — remoção de falsos positivos em aplicativos Java
- *Cross-Site Request Forgery* — remoção de falsos positivos para formulários HTML usando `AntiForgery.GetHtml()` ou `Html.AntiForgeryToken()` em aplicativos .NET
- *Cross-Site Scripting: Persistent* — remoção de falsos positivos relacionados à tag `cycle` em aplicativos Django
- *Double Free* — remoção de falsos positivos em aplicativos C/C++ que usam `throw_error()` da biblioteca boost
- *HTML5: Missing Content Security Policy* — remoção de falsos positivos em aplicativos Java
- *JSON Injection* — remoção de falsos positivos em aplicativos PHP
- *Mass Assignment: Insecure Binder Configuration* — remoção de falsos positivos relacionados a tipos Enum em aplicativos .NET
- *Often Misused: File System* — remoção de falsos positivos relacionados a `GetFullPathNameW()` e chamadas de função semelhantes em aplicativos C++
- *Path Manipulation* — remoção de falsos positivos em aplicativos Java usando o Amazon AWS SDK
- *Type Mismatch: Signed to Unsigned* — remoção de falsos positivos relacionados a valores boolianos em aplicativos C/C++
- *Unreleased Resource* — remoção de falsos positivos ao usar `CreateFileW()` em aplicativos C++

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 aprimorar a consistência, as 14 seguintes categorias foram renomeadas:

Categorias removidas	Categoria adicionada
AWS CloudFormation Misconfiguration: Insecure Elasticache Storage	AWS CloudFormation Misconfiguration: Insecure ElastiCache Storage
AWS CloudFormation Misconfiguration: Insecure Elasticache Transport	AWS CloudFormation Misconfiguration: Insecure ElastiCache Transport
AWS Terraform Misconfiguration: Elasticache Missing Customer-Managed Encryption Key	AWS Terraform Misconfiguration: ElastiCache Missing Customer-Managed Encryption Key
Azure Terraform Bad Practices: AKS Cluster Missing Host-Based Encryption	Azure Terraform Misconfiguration: AKS Cluster Missing Host-Based Encryption
Azure Terraform Bad Practices: Azure MySQL Server Missing Infrastructure Encryption	Azure Terraform Misconfiguration: MySQL Missing Infrastructure Encryption
Azure Terraform Bad Practices: Azure PostgreSQL Server Missing Infrastructure Encryption	Azure Terraform Misconfiguration: PostgreSQL Missing Infrastructure Encryption
Azure Terraform Bad Practices: Missing Azure Storage Infrastructure Encryption	Azure Terraform Misconfiguration: Storage Account Missing Infrastructure Encryption
Azure Terraform Bad Practices: Missing SQL Database Backup Encryption	Azure Terraform Misconfiguration: SQL Server Backup Missing Encryption
Azure Terraform Bad Practices: Scale Set Missing Host-Based Encryption	Azure Terraform Misconfiguration: Scale Set Missing Host-Based Encryption
Azure Terraform Bad Practices: VM Missing Host-Based Encryption	Azure Terraform Misconfiguration: VM Missing Host-Based Encryption
GCP Terraform Bad Practices: Overly Permissive Service Account	GCP Terraform Misconfiguration: Improper Compute Engine Access Control
GCP Terraform Misconfiguration: Weak Key Management	GCP Terraform Misconfiguration: Compute Engine Missing Customer-Managed Encryption Key
Kubernetes Bad Practices: Improper Admission Controller Access Control	Kubernetes Misconfiguration: Improper Admission Controller Access Control
Kubernetes Misconfiguration: Missing Service Account Admission Controller	Kubernetes Misconfiguration: Missing ServiceAccount Admission Controller

Alterações da Ordem de Prioridade do Fortify

Para melhorar a consistência entre as categorias de vulnerabilidade relacionadas à falta de chaves de criptografia gerenciadas pelo cliente, a Ordem de Prioridade do Fortify das 20 seguintes categorias foi alterada para "baixa":

- *Azure ARM Misconfiguration: Automation Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Batch Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Cognitive Services Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Databricks Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Event Hubs Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: IoT Hub Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: NetApp Missing Customer-Managed Encryption Key*
- *Azure ARM Misconfiguration: Service Bus Missing Customer-Managed Encryption Key*

- *Azure ARM Misconfiguration: Storage Account Missing Customer-Managed Encryption Key*
- *Azure Terraform Misconfiguration: AKS Cluster Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Azure Disk Snapshot Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Container Registry Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Cosmos DB Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Managed Disk Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Shared Image Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: SQL Database Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Storage Account Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: Storage Encryption Scope Missing Customer-Managed Key*
- *Azure Terraform Misconfiguration: VM Storage Missing Customer-Managed Key*
- *GCP Terraform Misconfiguration: Compute Engine Missing Customer-Managed Encryption Key*

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

Insecure Deployment: Unpatched Application

Uma vulnerabilidade de Execução Remota de Código (RCE) de pré-autorização nas versões 5.6.0 a 5.6.8 do vBulletin foi identificada pelo CVE-2023-25135. O vBulletin, um software popular para a criação de comunidades e fóruns on-line dinâmicos, higieniza incorretamente a entrada fornecida pelo usuário para desserialização não autenticada. Esse problema permite que invasores executem código arbitrário no servidor, abusem da lógica do aplicativo ou montem ataques de negação de serviço (DoS). Essa versão inclui uma verificação para detectar essa vulnerabilidade nos servidores de destino.

Poluição do protótipo: Lado do servidor

A poluição do protótipo do lado do servidor ocorre quando um invasor pode manipular o protótipo de um objeto. Isso é possível em linguagens baseadas em protótipos, como o JavaScript, que permite a alteração de propriedades e métodos em tempo de execução. A gravidade da exploração depende de onde o objeto poluído é usado no aplicativo. Os ataques incluem Negação de Serviço, alteração da configuração do aplicativo e, em alguns casos, Execução Remota de Código. Esta versão inclui uma verificação para detectar a poluição de protótipos em aplicativos da Web.

Relatórios de conformidade

2023 Common Weakness Enumeration (CWE™) Top 25

The Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) foi introduzido em 2019 e substitui o SANS Top 25. Lançado em junho, o 2023 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. O SecureBase inclui verificações que mapeiam diretamente para a categoria identificada pelo CWE Top 25, ou um CWE-ID relacionado a um CWE-ID no Top 25 via relacionamento “ChildOf”.

OWASP API Security Top 10 2023

O Open Worldwide Application Security Project (OWASP) API Security Top 10 2023 fornece uma lista dos principais riscos de segurança que afetam as APIs em 2023. Seu objetivo é aumentar a conscientização sobre os pontos fracos da segurança da API e educar os envolvidos no desenvolvimento e na manutenção da API, como desenvolvedores, designers, arquitetos, gerentes e organizações em geral que precisam proteger as Web APIs. O OWASP API Security Top 10 concentra-se nos pontos fracos que afetam as Web APIs e não se destina a ser usado isoladamente. Em vez disso, ele deve ser usado em conjunto com outros padrões e práticas recomendadas para capturar completamente todos os riscos relevantes. Por exemplo: Use o OWASP API Security Top 10 2023 em combinação com o OWASP Top 10 para identificar problemas relacionados à validação de entrada, como injeções. Esta atualização do SecureBase inclui um novo modelo de relatório de conformidade que fornece correlação entre as categorias do OWASP API Security Top 10 2023 e as verificações do WebInspect.

Atualizações da política

2023 CWE Top 25

Uma política personalizada para incluir verificações relevantes para 2023 CWE Top 25 foi adicionada à lista WebInspect SecureBase de políticas com suporte.

OWASP API Security Top 10 2023

Uma política personalizada para incluir verificações relevantes para OWASP API Security Top 10 2023 foi adicionada à lista WebInspect SecureBase de políticas com suporte. Essa política contém um subconjunto das verificações disponíveis do WebInspect que permite aos clientes executar varreduras específicas de conformidade do WebInspect.

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:

LDAP Injection

Esta versão inclui melhorias na verificação de Injeção de LDAP para reduzir falsos positivos e aumentar a precisão dos resultados.

Discrepância de Nome de Host do Certificado SSL

O conteúdo do relatório de verificação de Discrepância de Nome de Host do Certificado SSL agora inclui informações mais detalhadas que devem ajudar os clientes a aplicar uma correção adequada para esse problema de segurança.

Cobertura Agressiva por Entradas de Verificação

Para algumas verificações do WebInspect, é possível ativar a Cobertura Agressiva que orienta o WebInspect a enviar uma lista mais longa de ataques que visam uma gama mais ampla de endpoints. Esta versão inclui melhorias nessas verificações, que permitem que os clientes configurem a Cobertura Agressiva alterando as Entradas de Verificação em vez de adicionar verificações separadas à política de varredura. As verificações que têm recursos de Cobertura Agressiva incluem o seguinte: *Log4Shell*, *JNDI Reference Injection*, *Server-Side Request Forgery*, *OS Command Injection* e *Server-Side Prototype Pollution*. As verificações com Cobertura Agressiva ativada proporcionam uma varredura mais precisa, mas é importante considerar que o número de solicitações e o tempo de varredura podem aumentar drasticamente. Portanto, o Fortify recomenda enfaticamente que você execute verificações com a Cobertura Agressiva ativada em uma política separada sem outras verificações.

Web Server Misconfiguration: Arquivo desprotegido

Esta versão inclui uma pequena correção de bug para melhorar a detecção de arquivos de configuração relacionados a Java.

Fortify Premium Content

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

2023 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 2023 CWE Top 25, que está disponível para download no Portal de Suporte ao Cliente Fortify em Conteúdo Premium.

OWASP API Security Top 10 2023

Para acompanhar as novas correlações, esta versão também contém um novo pacote de relatórios para o Fortify Software Security Center com suporte para OWASP API Security Top 10, 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 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