Conteúdo de Segurança de Software do Fortify

Atualização 1 de 2024
29 de março de 2024

Sobre o OpenText Fortify Software Security Research

A equipe do Fortify Software Security Research traduz pesquisas de ponta em inteligência de segurança que potencializa o portfólio de produtos Fortify, incluindo o OpenText™ Fortify Static Code Analyzer (SCA) e o OpenText™ Fortify WebInspect. Atualmente, o Conteúdo de Segurança de Software da Fortify oferece suporte a 1.654 categorias de vulnerabilidade em 33 linguagens e se estende por mais de um milhão de APIs individuais.

O Fortify Software Security Research (SSR) tem o prazer de anunciar a disponibilidade imediata de atualizações para Fortify Secure Coding Rulepacks (idioma inglês, versão 2024.1.0), 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 1.429 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 Angular (versão compatível: 16.0.0)

Angular é uma estrutura gratuita de desenvolvimento de aplicativos da web baseada em typescript e de código aberto, especializada na criação de SPAs (Aplicativos de Página Única) e é usada principalmente no frontend para manipular dados de forma dinâmica e eficiente. O suporte para Angular foi expandido da versão 11.2.4 até Angular 16.0.0 (somente suporte inicial). Os resultados do Angular foram aprimorados para que os clientes possam esperar melhores resultados em categorias como *Cross-Site Request Forgery*, *Privacy Violation* e *System Information Leak*. A cobertura foi expandida para o documento DOM em JavaScript, bem como para os seguintes módulos:

- @angular/common/http
- @angular/core
- @angular/platform-browser

Suporte aprimorado para PHP (versão compatível: 8.2)

PHP é uma linguagem de script de uso geral amplamente usada, mais frequentemente usada para desenvolvimento da Web. A versão mais recente do SSR atualiza o suporte para PHP até a versão 8.2. Em particular, o lançamento inclui suporte inicial para as seguintes extensões básicas PHP adicionais:

- Sodium (versão compatível: 8.3.1)

  A extensão PHP Sodium é uma implementação da biblioteca Libsodium. O Sodium fornece recursos para criptografia, descriptografia, assinaturas, hash de senha e outras operações criptográficas. Os clientes podem encontrar problemas adicionais relacionados à criptografia e às assinaturas digitais, juntamente com alterações em problemas de Privacy Violation.

- Zip (versão compatível: 1.22.3)

  A extensão PHP Zip é uma implementação da biblioteca Libzip. Zip fornece capacidade de criação, modificação e leitura de arquivos zip, uma estrutura comum usada para realizar agrupamento e compactação de arquivos/dados. O suporte inicial da extensão inclui cobertura da classe ZipArchive específica para fluxo de dados básico do sistema de arquivos e expansão da cobertura PHP para as seguintes categorias:

  - Key Management: Empty PBE Password
  - Path Manipulation: Zip Entry Overwrite

Suporte aprimorado para Golang (versão compatível: 1.21)[1]

Go, também conhecido como Golang, é uma linguagem de programação compilada, digitada estaticamente e criada no Google. É conhecida por sua simplicidade, eficiência e forte suporte à simultaneidade, o que a torna ideal para a criação de serviços da Web escaláveis, pipelines de dados e sistemas distribuídos. Go combina os benefícios de desempenho das linguagens compiladas com a facilidade de programação observada nas linguagens interpretadas. Sua sintaxe concisa e sua poderosa biblioteca padrão permitem que os desenvolvedores escrevam códigos robustos rapidamente. A cobertura é ampliada para os seguintes pacotes:

- context
- crypto/ecdh
- html/template
- net
- reflect
- Runtime
- time

Infraestrutura como Código (IaC) da nuvem[2]

Suporte expandido para infraestrutura como código 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. Problemas comuns relacionados à configuração desses serviços mencionados agora são relatados ao desenvolvedor. A partir do Fortify Static Code Analyzer 24.2, os problemas de configuração do Azure ARM e do AWS CloudFormation são relatados usando novas técnicas. Isso resulta em um conjunto de problemas adicionados e removidos ao mesclar FPRs gerados com versões anteriores do Fortify Static Code Analyzer. Com o Fortify Static Code Analyzer 24.2 e versões posteriores, os Rulepacks 2024.1 são necessários para evitar problemas de IaC duplicados.

Configurações do Azure Resource Manager (ARM)

ARM é o serviço de implantação e gerenciamento do Azure. O ARM fornece uma camada de gerenciamento que permite criar, atualizar e excluir recursos na sua conta do Azure.

Configurações do Amazon Web Services (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. Com esses modelos, os usuários podem criar, excluir e modificar coleções de recursos, conhecidas como pilha, como uma única unidade. Nesta versão, relatamos as seguintes categorias adicionais de fraquezas para configurações do AWS CloudFormation:

- AWS CloudFormation Misconfiguration: Insecure SageMaker Transport
- AWS CloudFormation Misconfiguration: SageMaker Network Isolation Disabled
- AWS CloudFormation Misconfiguration: Weak SecretsManager Generated Password

[1] Para obter resultados ideais, atualize para o Fortify Static Code Analyzer 24.2 ou posterior.
[2] Requer o Fortify Static Code Analyzer 24.2 ou posterior.

Suporte aprimorado para Kotlin (versão compatível: 1.9.2)[3]

Kotlin é uma linguagem de uso geral, de tipagem estática, com interoperabilidade Java. Esta versão inclui suporte atualizado para novas APIs de biblioteca padrão introduzidas no Kotlin 1.7.2, 1.8 e 1.9 voltadas para namespaces do Kotlin: *jvm.optional*, *math*, *io.path*, *coroutines.cancellation* e *kotlinx.serialization.json*. Problemas adicionais podem ser detectados em categorias existentes, incluindo:

- Denial of Service: Regular Expression
- Path Manipulation
- Privacy Violation
- System Information Leak

Melhorias em JavaScript/TypeScript Node.js[4]

Nossas regras do Node.js foram atualizadas para se beneficiar da resolução de tipo durante o uso do Fortify Static Code Analyzer 24.2. As mudanças resultam na redução de falsos positivos, na melhoria de verdadeiros positivos e em descobertas mais precisas em aplicativos Node.js na maioria das categorias. Mais especificamente, os clientes podem esperar melhores resultados relacionados aos seguintes módulos Node.js:

- child_process
- dgram
- dns
- fs
- http
- https
- net
- querystring
- tls
- url
- util
- v8

O suporte parcial inicial para os seguintes pacotes NPM também está incluído:

- Bluebird
- child-process-promise

Suporte aprimorado para DISA STIG 5.3

Para oferecer suporte a nossos clientes federais na área de conformidade, a correlação do Fortify Taxonomy com o Defense Information Systems Agency (DISA) Application Security and Development STIG versão 5.3 foi atualizada para incluir os seguintes 45 IDs adicionais de STIG: APSC-DV-000010, APSC-DV-000210, APSC-DV-000230, APSC-DV-000240, APSC-DV-000330, APSC-DV-000380, APSC-DV-000390, APSC- DV-000400, APSC-DV-000410, APSC-DV-000430, APSC-DV-000450, APSC-DV-000580, APSC-DV- 000590, APSC-DV-000710, APSC-DV-001120, APSC-DV-001130, APSC-DV-001280, APSC-DV-001290, APSC-DV-001300, APSC-DV-001310, APSC-DV-001320, APSC-DV-001330,

[3] O suporte ao Kotlin 1.9 requer o Fortify Static Code Analyzer 24.2 ou posterior.

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

APSC-DV-001410, APSC-DV-001520, APSC-DV-001530, APSC-DV-001540, APSC-DV-001610, APSC-DV-001760, APSC-DV-001770, APSC-DV-001780, APSC-DV-001790, APSC-DV-001795, APSC-DV-001820, APSC-DV-001970, APSC-DV-002290, APSC-DV-002310, APSC-DV-002320, APSC-DV-002410, APSC-DV-002530, APSC-DV-002890, APSC-DV-002950, APSC-DV-002960, APSC-DV-003100, APSC-DV-003310 e APSC-DV-003320.

Erratas diversas

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

Redução de falsos positivos e outras melhorias notáveis na detecção

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

- *Access Control: Anonymous LDAP Bind* – falsos positivos removidos em aplicativos C/C++
- *Command Injection* – novos problemas detectados em aplicativos C/C++ que usam a variante do Windows das funções da biblioteca de tempo de execução C
- *Credential Management: Hardcoded API Credentials* – falsos positivos removidos em arquivos YAML
- *Dockerfile Misconfiguration: Dependency Confusion* – falsos positivos removidos em Dockerfiles que envolvem npm
- *Dynamic Code Evaluation: Code Injection* – novos problemas detectados em aplicativos ASP.NET que usam APIs do Azure Cosmos DB
- *GCP Terraform Misconfiguration: Insecure Supply Chain* – falsos positivos removidos nos arquivos de configuração do AWS Terraform
- *Insecure SSL: Server Identity Verification Disabled* – novos problemas detectados em aplicativos Python que usam a biblioteca "Requests"
- *Mass Assignment: Insecure Binder Configuration* – falsos positivos removidos em aplicativos ASP.NET MVC
- *Mass Assignment: Request Parameters Bound into Persisted Objects* – falsos positivos removidos de aplicativos Spring
- *Password Management: Hardcoded Password* – novos problemas detectados nas cadeias de conexão ODBC
- *Poor Style: Identifier Contains Dollar Symbol ($)* – falsos positivos removidos em aplicativos Java
- *Privacy Violation* – novos problemas detectados em aplicativos ASP.NET que usam Razor Pages
- *Privacy Violation* – novos problemas detectados em aplicativos Dart/Flutter
- *Privacy Violation* – novos problemas detectados em aplicativos JavaScript que usam o middleware "csurf" junto com a biblioteca ExpressJS
- *String Termination Error* – novos problemas detectados em aplicativos C/C++
- *System Information Leak: External* – novos problemas detectados em aplicativos ASP.NET que usam Razor Pages
- *System Information Leak: External* – novos problemas detectados em aplicativos C/C++
- *Weak Encryption: Inadequate RSA Padding* – falsos positivos removidos em aplicativos PHP que usam OpenSSL
- Vários falsos positivos de fluxo de dados removidos em aplicativos Python Django

- Vários novos problemas de fluxo de dados detectados em aplicativos Java Spring
- Vários problemas de fluxo de dados que aparecem no ponto de entrada main() nas varreduras de Java podem aparecer como novos e removidos. Isso também remove duplicatas e rastros incorretos encontrados em aplicativos Kotlin e Scala.

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 quatro seguintes categorias foram renomeadas:

Nome da categoria 2023 R4	Nome da categoria 2024 R1
Insecure Cross-Origin Opener Policy	HTML5: Insecure Cross-Origin Opener Policy
Insecure Transport: Client Identity Verification Disabled	Insecure SSL: Server Identity Verification Disabled
Kubernetes Terraform Misconfiguration: Improper Daemon Set Access Control	Kubernetes Terraform Misconfiguration: Improper DaemonSet Access Control
Kubernetes Terraform Misconfiguration: Improper Stateful Set Access Control	Kubernetes Terraform Misconfiguration: Improper StatefulSet Access Control

Suspensão da categoria "Header Checking Disabled"

A categoria foi removida para evitar confusão com outras categorias com nomes semelhantes. As regras anteriores nesta categoria agora são relatadas em:

- ASP.NET Misconfiguration: Header Checking Disabled
- ASP.NET Misconfiguration: Unsafe Header Parsing

Descontinuação de determinadas categorias de "Dead Code"

As seguintes categorias de "Dead Code" foram removidas dos pacotes de regras padrão:

- Dead Code: Empty Try Block
- Dead Code: Expression is Always false
- Dead Code: Expression is Always true
- Dead Code: Campo não utilizado
- Dead Code: Unused Method
- Dead Code: Unused Parameter

Para clientes que desejam continuar vendo essas vulnerabilidades detectadas, as regras podem ser baixadas do Portal de Suporte do Fortify em um Rulepack separado.

Renomeação e descontinuação do OWASP Mobile Top 10 2023
Após o lançamento do “OWASP Top 10 Mobile Risks – Initial Release 2023” em setembro de 2023, o projeto foi finalizado e renomeado para “OWASP Top 10 Mobile Risks – Final Release 2024” em janeiro de 2024. Como resultado, esta versão inclui um mapeamento adicional e renomeado para “OWASP Mobile Top 10 Risks 2024”. Os mapeamentos em si não apresentam alterações funcionais.

Na próxima versão do Fortify Software Security Content, o mapeamento OWASP Mobile Top 10 2023 será descontinuado e apenas o OWASP Mobile Top 10 2024 atualizado permanecerá.

Fortify SecureBase [Fortify WebInspect]

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

Suporte a vulnerabilidades

Insecure Deployment: Unpatched Application (CVE-2024-23897)

Jenkins é um servidor de automação baseado em Java usado para construir, testar e implantar software. Command Line Interface (CLI) do Jenkins é um recurso integrado do Jenkins que fornece uma maneira de interagir com o servidor Jenkins e é habilitado por padrão. Uma vulnerabilidade crítica de leitura de arquivos identificada por CVE-2024-23897 permite recursos arbitrários de leitura de arquivos no Jenkins. Essa vulnerabilidade está presente na biblioteca args4j que é usada para analisar argumentos e opções de comando fornecidos à CLI. O analisador de comandos possui um recurso que substitui o caractere de arroba (@) seguido por um caminho de arquivo em um argumento pelo conteúdo do arquivo especificado. As versões afetadas do Jenkins incluem 2.441 e anteriores e LTS 2.426.2 e anteriores. Esta versão inclui uma verificação para detectar CVE-2024-23897 em um servidor de destino.

Insecure Deployment: Unpatched Application (CVE-2023-22515)

Atlassian Confluence Data Center e Confluence Server são soluções autogerenciadas conhecidas por fornecer às organizações as práticas recomendadas de colaboração. Uma vulnerabilidade crítica de controle de acesso quebrado identificada por CVE-2023-22515 permite que atores mal-intencionados criem contas de administrador não autorizadas, concedendo-lhes acesso irrestrito à plataforma do Confluence. Mesmo quando os invasores não têm autenticação, eles podem aproveitar as vantagens de CVE-2023-22515 para estabelecer contas de administrador não autorizadas e obter acesso às instâncias do Confluence. Os invasores também podem manipular as configurações dos servidores do Confluence para sugerir que o processo de configuração não foi finalizado. As versões afetadas do Confluence Server e do Confluence Data Center são 8.0.0-8.0.4, 8.1.0-8.1.4, 8.2.0-8.2.3, 8.3.0-8.3.2, 8.4.0-8.4.2 e 8.5.0-8.5.1. Esta versão inclui uma verificação para detectar CVE-2023-22515 em um servidor de destino.

Insecure Deployment: Unpatched Application (CVE-2023-22518)

Uma vulnerabilidade crítica de autorização inadequada identificada por CVE-2023-22518 afeta o Atlassian Confluence Data Center e o Confluence Server. Essa vulnerabilidade permite que um invasor não autenticado redefina o Confluence e crie uma conta de administrador de instância do Confluence. Usando essa conta, um invasor pode executar todas as ações administrativas disponíveis para um administrador de instância do Confluence, causando perda total de confidencialidade, integridade e disponibilidade. As versões afetadas do Confluence Server e do Confluence Data Center são todas versões anteriores à 7.19.16 e versões 8.3.4, 8.4.4, 8.5.3 e 8.6.1. Esta versão inclui uma verificação para detectar CVE-2023-22518 em um servidor de destino.

OGNL Expression Injection: Double Evaluation (CVE-2023-22527)

Uma vulnerabilidade crítica de OGNL Expression Injection identificada pelo CVE-2023-22527 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 Data Center e do Confluence Server são 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x e 8.5.0-8.5.3. Esta versão inclui uma verificação para detectar essa vulnerabilidade nos servidores.

Relatórios de conformidade

DISA STIG 5.3 aprimorado

Para oferecer suporte a nossos clientes federais na área de conformidade, a correlação do Fortify Taxonomy com o Defense Information Systems Agency (DISA) Application Security and Development STIG, versão 5.3 foi atualizada para incluir os seguintes 8 IDs adicionais de STIG: APSC-DV-000210, APSC-DV-000230, APSC-DV-000240, APSC-DV-000450, APSC-DV-001280, APSC-DV-001300, APSC-DV-002530 e APSC-DV-003320.

Atualizações da política

DISA STIG 5.3 aprimorado

A política DISA STIG 5.3 foi atualizada para incluir verificações adicionais relevantes para DISA STIG 5.3.

Erratas diversas

Nesta 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:

Injeção de XPath

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

Fortify Premium Content

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

OWASP Mobile Top 10 2024

Para acompanhar as correlações de OWASP Mobile Top 10 Risks 2024 renomeadas, esta versão também contém um novo pacote de relatórios para o OpenText™ Fortify Software Security Center com suporte para OWASP Mobile Top 10 2024, 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