Anúncio da versão do Software Security Research

Conteúdo de Segurança de Software Fortify

Atualização 4 de 2021

17 de dezembro de 2021

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), o Fortify WebInspect e o Fortify Application Defender. Atualmente, o conteúdo de segurança de software do CyberRes Fortify oferece suporte a 1.137 categorias de vulnerabilidade em 29 linguagens de programação e se estende por mais de um milhão de APIs individuais.
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 2021.4.0), o Fortify WebInspect SecureBase (disponível por SmartUpdate) e o Fortify Premium Content.

CyberRes Fortify Secure Coding Rulepacks [SCA]

Nesta versão, o Fortify Secure Coding Rulepacks detecta 917 categorias únicas de vulnerabilidades em 29 linguagens de programação e se estende por mais de um milhão de APIs individuais. Em resumo, esta versão inclui o seguinte:

Atualizações do .NET Core e ASP.NET (versão suportada: .NET Core 3.1)

Melhorado o suporte para namespaces do .NET Core e ASP.NET Core, incluindo o seguinte:

- Microsoft.AspNetCore.Http
- Microsoft.AspNetCore.Mvc
- Microsoft.Extensions.Logging
- System
- System.IO
- System.Net
- System.Threading

O suporte melhorar a abrangência das seguintes categorias:

- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Log Forging
- Log Forging (debug)
- Privacy Violation
- System Information Leak

Azure

A Azure é a plataforma pública de computação em nuvem da Microsoft que oferece uma variedade de serviços em nuvem, incluindo computação, contêineres, internet das coisas, IA e aprendizado de máquina.

Nesta versão, oferecemos suporte inicial para diversos serviços fundamentais da Azure: Funções, identidade e CosmosDB. Além disso, agora, as seguintes tecnologias específicas da Azure são suportadas:

Azure Functions (Versões Suportadas: Java 1.3.1, C# 3.x)

Functions são soluções de computação sem servidor da Microsoft Azure. O Azure Functions oferece uma infraestrutura permanentemente atualizada para executar sua aplicação, desenvolver APIs web, responder a alterações no banco de dados e gerenciar filas de mensagem. Esta atualização inclui suporte inicial para os seguintes tipos de acionadores para C# e Java:

- Blob Trigger
- CosmosDB Trigger
- Event Trigger
- Http Trigger (as class library)
- Http Trigger (as C# isolated process)
- Queue Trigger
- ServiceBus Trigger

O suporte ao Azure Functions inclui as seguintes categorias:

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set
- Cookie Security: Overly Broad Path
- Cookie Security: Overly Broad Domain
- Cookie Security: Persistent Cookie
- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Denial Of Service
- Header Manipulation
- Header Manipulation: Cookies
- HTML5: Overly Permissive CORS Policy
- Privacy Violation
- Resource Injection
- Setting Manipulation
- System Information Leak: External

Azure Identity (Versões Suportadas: C# 1.5.0, Java 1.4.1)

O Azure Identity é um serviço de gerenciamento de identidade e acesso baseado em nuvem da Microsoft. Ele oferece autenticação e autorização a recursos dentro de uma organização. Essa atualização inclui suporte inicial para os seguintes namespaces:

C#

- Azure.Identity (version 1.5.0)

Java

- com.azure.identity (version 1.4.1)

O suporte do Azure Identity inclui as seguintes categorias:

- Password Management
- Password Management: Empty/Hardcoded/Null Password
- Password Management: Weak Cryptography
- Resource Injection

Azure CosmosDB (Versão Suportada: 3.x)

O Azure Cosmos DB é um serviço de banco de dados multimodelo, distribuído globalmente. Como o Azure Cosmos DB é possível armazenar e acessar documento, key-value, wide-column e bases de dados gráficas usando APIs e modelos de programação. Essa atualização inclui suporte inicial para os seguintes namespaces para C#:

- Microsoft.Azure.Cosmos
- Microsoft.Azure.Cosmos.Scripts
- Microsoft.Azure.Cosmos.Table

O suporte do Azure Cosmos DB inclui as seguintes categorias:

- Denial of Service
- HTML5: Overly Permissive CORS Policy
- Insecure Transport
- NoSQL Injection: CosmosDB
- Resource Injection
- Setting Manipulation
- SQL Injection

AWS

O Amazon Web Services (AWS) é uma plataforma pública de computação em nuvem que oferece uma variedade de serviços em nuvem, incluindo computação, armazenamento, rede, banco de dados, internet das coisas e aprendizado de máquina.

Nesta versão, oferecemos suporte inicial para diversos serviços fundamentais da AWS: IAM, DynamoDB, e RDS. Esta versão também inclui suporte inicial Lambda para C# e suporte atualizado para Java. Além disso, agora, as seguintes tecnologias específicas da AWS são suportadas:

Atualizações AWS Lambda (Versões Suportadas: .NET AWS SDK 3.7.x, Java AWS SDK v2 2.17.x) [1]

O Lambda é um serviço de computação oferecido pela Amazon como parte da Amazon Web Services (AWS), que executa códigos sem o provisionar ou gerenciar servidores. O serviço Lambda executa código em resposta a eventos e gerencia automaticamente recursos computacionais exigidos pelo código. Esta atualização inclui suporte inicial para C# e suporte adicionar para Java. Esta atualização inclui suporte para os seguintes namespaces para C# e Java:

C#

- Amazon.Lambda
- Amazon.Lambda.APIGatewayEvents
- Amazon.Lambda.Core

Java

- com.amazonaws.services.lambda.runtime
- com.amazonaws.services.lambda.runtime.events

[1] Para uma análise melhorada, inclua modelos AWS SAM ou CloudFormation YAML/JSON na tradução.

Essa atualização inclui suporte adicional para os seguintes tipos de evento:

- API Gateway Events (C#, Java)
- DynamoDB (Java)
- S3 Events (Java)
- Scheduled Events (Java)

O suporte do AWS Lambda inclui as seguintes categorias:

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Header Manipulation
- Header Manipulation: Cookies
- Log Forging
- Privacy Violation
- System Information Leak: External
- System Information Leak: Internal

AWS IAM (Versões Suportadas: .NET AWS SDK 3.7.x, Java AWS SDK v2 2.17.x)

O AWS Identity and Access Management (IAM) é um serviço da web que controla o acesso aos recursos AWS. O IAM pode ser usado para controlar o uso autenticado e autorizado dos recursos AWS. Esta atualização inclui suporte para C# e Java. Esta atualização inclui suporte para os seguintes namespaces para C# e Java:

C#

- Amazon.IdentityManagement.Model

Java

- com.amazonaws.services.identitymanagement.model
- software.amazon.awssdk.services.iam.model

Além de identificar informações confidencias, o suporte do AWS IAM inclui as seguintes categorias:

- Password Management
- Password Management: Empty/Hardcoded/Null Password
- Password Management: Weak Cryptography

AWS DynamoDB (Versões Suportadas: .NET AWS SDK 3.7.x, Java AWS SDK v2 2.17.x)

O AWS DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que suporta estruturas de dado key-value e document. O DynamoDB pode ser usado para armazenar e recuperar dados e atender quantidades arbitrárias de solicitar tráfego. Esta atualização inclui suporte inicial para C# e suporte adicional para Java. O suporte inclui os seguintes namespaces:

C#

- Amazon.DynamoDBv2.Model
- Amazon.DynamoDBv2.DataModel
- Amazon.DynamoDBv2.DocumentModel

Java

- com.amazonaws.services.lambda.runtime.events.models.dynamodb
- software.amazon.awssdk.enhanced.dynamodb
- software.amazon.awssdk.enhanced.dynamodb.model

O suporte do AWS DynamoDB inclui as seguintes categorias:

- Access Control: Database
- NoSQL Injection: DynamoDB
- SQL Injection: PartiQL

API de Dados do AWS Relational Database Service (RDS) para Aurora Serverless (Versões Suportadas: .NET AWS SDK 3.7.x, Java AWS SDK v2 2.17.x)

O Amazon Aurora é um mecanismo de banco de dados relacionais compatível com MySQL e PostgreSQL que faz parte do Amazon Relational Database Service (Amazon RDS) gerenciado. O API de dados AWS RDS oferece uma interface de serviço na web permitindo que aplicativos acessem e executem instruções SQL em cluster de banco de dados do Aurora Serverless. Esta atualização inclui suporte para os seguintes namespaces para C# e Java:

C#

- Amazon.RDSDataService.Model

Java

- software.amazon.awssdk.services.rdsdata.model (V2)

O suporte do AWS RDS inclui as seguintes categorias:

- Access Control: Database
- Setting Manipulation
- SQL Injection

Varredura Secreta

Suporte para Varredura Secreta. A varredura secreta é uma técnica para procurar automaticamente por segredos em arquivos de texto. Neste contexto “segredos” refere-se a senhas, tokens API, chaves de codificação e artefatos similares que não devem ser divulgados. A principal finalidade é encontrar segredos codificados acidentalmente no código fonte e em arquivos de configuração. Suporte ampliado para todos as linguagens de programação e tipos de arquivo adicionais, por meio da nova análise Regex[2]. As categorias suportadas incluem:

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

[2] Requer Fortify Static Code Analyzer v21.2.0 ou superior.

Trojan Source

Trojan Source[3] é uma categoria de vulnerabilidades publicadas por Nick Boucher e Ross Anderson no documento “Trojan Source: Invisible Vulnerabilities” [Trojan Source: vulnerabilidades invisíveis]. Eles demonstram cinco maneiras diferentes de como os caracteres especiais Unicode podem ser usados para fazer com que o código pareça ser um ao olho nu de um desenvolvedor, mas que ao serem executados funcionam de uma maneira distinta. O Trojan Source deve ser considerado como um cenário de ameaça interna considerando que um indivíduo mal-intencionado pode inserir propositalmente os caracteres Unicode. Em razão da precisão de uma das categorias, estamos incluindo suporte a detecção nas principais Rulepacks para as seguintes linguagens de programação: C, C++, C#, Go, Java, JavaScript, Python e Rust. As categorias com suporte incluem:

- Encoding Confusion: BiDi Control Characters

Correlação de Problema Estático/Dinâmico[4]

Suporte para dados exportados para habilitar a correlação dos resultados de varredura estática e dinâmica no Fortify Software Security Center (SSC) para projetos Java Spring. As categorias suportadas incluem:

- Cross-Site Scripting: Content Sniffing
- Cross-Site Scripting: Inter Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- SQL Injection
- SQL Injection: Hibernate

Suporte ampliado ao IBM Mainframe COBOL (Versão suportada: 6.3)

Esta atualização inclui detecção de vulnerabilidade Integer Overflow no código COBOL do Mainframe IBM.

Infraestrutura como Código em nuvem

Suporte para Infraestrutura como Código (IaC) em nuvem. IaC é o processo de gerenciar e provisionar recursos computacionais por meio de código, ao invés de fazê-lo por meio de processos manuais. Tecnologias suportadas incluem AWS, AWS CloudFormation, Azure ARM, Kubernetes K8S, e Azure Kubernetes Service. Problemas comuns relacionadas à configuração dos serviços mencionados, agora, são comunicados ao desenvolvedor, incluindo:

- Access Control: Azure Blob Storage
- Access Control: Azure Container Registry
- Access Control: Azure Network Group

---

[3] Requer Fortify Static Code Analyzer v21.2.0 ou superior.
[4] Requer Fortify Static Code Analyzer v21.2.0 ou superior. Para habilitar a saída de correlação, aprove a propriedade `com.fortify.sca.rules.enable_wi_correlation` at scan time. Isto pode ser feito com os argumentos da linha de comando ou modificando os arquivos de propriedades SCA.

- Access Control: Azure SQL Database
- Access Control: Azure Storage
- Access Control: Cosmos DB
- Access Control: EC2
- Access Control: Kubernetes Admission Controller
- Access Control: Kubernetes Image Authorization Bypass
- Access Control: Overly Broad IAM Principal
- Access Control: Overly Permissive S3 Policy
- AKS Bad Practices: Missing Azure Monitor Integration
- Ansible Bad Practices: Missing CloudWatch Integration
- Ansible Bad Practices: Redshift Publicly Accessible
- Ansible Misconfiguration: Log Validation Disabled
- AWS CloudFormation Bad Practices: Missing CloudWatch Integration
- AWS CloudFormation Bad Practices: Redshift Publicly Accessible
- AWS CloudFormation Bad Practices: User-Bound IAM Policy
- AWS CloudFormation Misconfiguration: API Gateway Unauthenticated Access
- AWS CloudFormation Misconfiguration: Insecure Transport
- AWS CloudFormation Misconfiguration: Insufficient CloudTrail Logging
- AWS CloudFormation Misconfiguration: Insufficient DocumentDB Logging
- AWS CloudFormation Misconfiguration: Insufficient Neptune Logging
- AWS CloudFormation Misconfiguration: Insufficient RedShift Logging
- AWS CloudFormation Misconfiguration: Insufficient S3 Logging
- AWS CloudFormation Misconfiguration: Log Validation Disabled
- AWS CloudFormation Misconfiguration: root User Access Key
- AWS CloudFormation Misconfiguration: Unrestricted Lambda Principal
- Azure Monitor Misconfiguration: Insufficient Logging
- Azure Resource Manager Bad Practices: Cross-Tenant Replication
- Azure Resource Manager Bad Practices: Remote Debugging Enabled
- Azure Resource Manager Bad Practices: SSH Password Authentication
- Azure Resource Manager Misconfiguration: Insecure Transport
- Azure Resource Manager Misconfiguration: Overly Permissive CORS Policy
- Azure Resource Manager Misconfiguration: Security Alert Disabled
- Azure SQL Database Misconfiguration: Insufficient Logging
- Insecure SSL: Inadequate Certificate Verification
- Insecure Storage: Missing DocumentDB Encryption
- Insecure Storage: Missing EBS Encryption
- Insecure Storage: Missing Elasticache Encryption
- Insecure Storage: Missing Neptune Encryption
- Insecure Storage: Missing RDS Encryption
- Insecure Storage: Missing Redshift Encryption
- Insecure Storage: Missing S3 Encryption
- Insecure Storage: Missing SNS Topic Encryption
- Insecure Transport: Azure Storage
- Insecure Transport: Database
- Insecure Transport: Missing Elasticache Encryption
- Key Management: Excessive Expiration

- Kubernetes Bad Practices: API Server Publicly Accessible
- Kubernetes Bad Practices: Default Namespace
- Kubernetes Bad Practices: Host Write Access
- Kubernetes Bad Practices: Missing API Server Authorization
- Kubernetes Bad Practices: Missing Kubelet Authorization
- Kubernetes Bad Practices: Missing Node Authorization
- Kubernetes Bad Practices: Missing RBAC Authorization
- Kubernetes Bad Practices: NamespaceLifecycle Enforcement Disabled
- Kubernetes Bad Practices: readOnlyPort Enabled
- Kubernetes Bad Practices: Static Authentication Token
- Kubernetes Bad Practices: Unconfigured API Server Logging
- Kubernetes Misconfiguration: API Server Anonymous Access
- Kubernetes Misconfiguration: API Server Logging Disabled
- Kubernetes Misconfiguration: HTTP Basic Authentication
- Kubernetes Misconfiguration: Insecure Transport
- Kubernetes Misconfiguration: Kubelet Anonymous Access
- Kubernetes Misconfiguration: Missing Garbage Collection Threshold
- Kubernetes Misconfiguration: Missing Kubelet Client Certificate
- Kubernetes Misconfiguration: Overly Permissive Capabilities
- Kubernetes Misconfiguration: Privileged Container
- Kubernetes Misconfiguration: Server Identity Verification Disabled
- Kubernetes Misconfiguration: Unbound Controller Manager
- Kubernetes Misconfiguration: Unbound Scheduler
- Poor Logging Practice: Excessive Cloud Log Retention
- Poor Logging Practice: Insufficient Cloud Log Retention
- Poor Logging Practice: Insufficient Cloud Log Rotation
- Poor Logging Practice: Insufficient Cloud Log Size
- Privacy Violation: Exposed Default Value
- Privilege Management: Overly Broad Access Policy
- Privilege Management: Overly Permissive Role
- System Information Leak: Kubernetes Profiler

OWASP Top 10 2021

O Top 10 de 2021, da Open Web Application Security Project oferece um poderoso documento para conscientização sobre a segurança de aplicativos para web, direcionado para informar a comunidade sobre as consequências dos riscos de segurança dos mais comuns e críticos aplicativos para web. O Top 10 da OWASP representa um acordo amplo sobre quais são as falhas de segurança mais críticas dos aplicativos para web, com o consenso inferido da coleta de dados e resultados de pesquisas. Para dar suporte a clientes que desejam mitigar o risco de Aplicativos para Web, foi adicionada a correlação do Micro Focus Fortify Taxonomy ao recém-lançado OWASP Top 10 2021.

Erratas diversas

Nesta versão, continuamos a investir recursos para garantir que possamos reduzir o número de problemas de falso-positivos e melhorar a capacidade dos clientes de auditar problemas. Os clientes também podem esperar alterações nos problemas relatados relacionadas com o que segue:

Suspensão de uso das versões anteriores à versão 18.x, do Fortify Static Code Analyzer:

Conforme mencionado em nosso anúncio da versão 2021.3, aquele seria o último lançamento de Rulepacks compatíveis com o Fortify Static Code Analyzer anteriores à versão 18.x. Para este lançamento, o Fortify Static Code Analyzer em versões anteriores à versão 18.x não carregará os Rulepacks. Será necessário fazer o downgrade dos Rulepacks ou atualizar a versão do SCA. Em versões futuras, continuaremos a oferecer suporte para as últimas quatro versões principais do Fortify Static Code Analyzer.

Melhorias para PHP

Melhorado o suporte para identificar chaves de senha e criptografia no Gerenciamento de chaves: Categorias de chave de criptografia Vazia/Codificada/Nula.

Melhorias para Python

Melhorado o suporte para o módulo de *subprocesso*, resultando em uma melhor detecção de problemas, como Command Injection.

Melhorias referentes a falso-positivos:

O trabalho continua com o esforço para remover falso-positivos nesta versão. Além de outras melhorias, os clientes podem esperar ver a remoção de certos falso-positivos nas seguintes áreas:

- Falhas vindas de atores do Akka, nos projetos Scala, quando o aplicativo não está usando Play.
- Falhas de Cross-Site Scripting em JavaScript quando é obtido apenas controle parcial dos URLs.
- Falhas de Gerenciamento de senhas em arquivos JSON quando referenciam à localização de strings
- Falhas de fluxo de dados em projetos Java e .NET vindas de métodos HTTP`.

CyberRes 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:

API Discovery

Esta versão inclui uma verificação pela API Discovery. A verificação da API Discovery está sinalizado quando o WebInspect detecta uma definição de API na especificação do swagger, no local especificado pelo usuário, fornecida por meio de uma entrada de verificação. Estes arquivos de especificação podem não ser referenciados diretamente em qualquer página e, portanto, não são detectados no rastreamento. Além de verificar pelas especificações do swagger nos locais especificados pelo usuário, as definições encontradas durante a varredura que não são explicitamente especificadas com a entrada de verificação, também serão sinalizadas e testadas. Mesmo que estas descobertas não necessariamente indiquem uma vulnerabilidade da segurança, elas aumentam os recursos que possivelmente estão vulneráveis a ataques.

Suporte a vulnerabilidades

OGNL Expression Injection: Avaliação dupla

Uma vulnerabilidade crítica, OGNL Expression Injection [Injeção de Expressão OGNL], identificada pelo CVE-2021-26084, afeta o Servidor de Confluência Atlassian e o Data Center. A vulnerabilidade permite que um invasor não autenticado execute um código arbitrário em aplicações vulneráveis. As versões do servidor Atlassian afetadas são anteriores à versão 6.13.23, da versão 6.14.0 até a versão anterior à 7.4.11, da versão 7.5.0 até a versão anterior à 7.11.6 e da versão 7.12.0 até a versão anterior à 7.12.5. Esta versão inclui uma verificação para detectar essa vulnerabilidade em servidores Atlassian afetados.

Passagem de Diretório

Foi descoberto que o servidor Apache HTTP é vulnerável a ataques de passagem de diretório, identificado pelo CVE-2021-41773 e CVE-2021-42013. As vulnerabilidades permitem que um invasor manipule URLs que mapeiam URLs para arquivos fora dos diretórios configurados por diretivas alias-like. Os invasores podem recuperar o conteúdo dos arquivos no servido, resultando na divulgação de dados confidenciais, possível recuperação de lógica de negócio patenteada e, para algumas configurações, execução de código remoto. Estas falhas afetam apenas o as versões 2.4.49 e 2.4.50 do Servidor Apache HTTP. Esta versão contém uma verificação para detectar essas vulnerabilidades no servidor do Apache HTTP.

Path Manipulation: Caracteres especiais

Uma vulnerabilidade Path Manipulation, identificada pelo CVE-2021-28164 afeta o Eclipse Jetty. O modo de conformidade padrão nas versões afetadas permitem solicitações com URIs que contêm segmentos com caracteres especiais para acessar recursos protegidos no diretório WEB-INF. Isso pode revelar informações confidencias em relação à implementação de uma aplicação da web e ignorar algumas restrições de segurança. Esta versão contém uma verificação para detectar instâncias Jetty vulneráveis.

Dynamic Code Evaluation: Desserialização XStream insegura

XStream é uma ferramenta comumente usada para converter dados entre objetos Java e XML. O fluxo processado no momento de unmarshalling contém informações de tipo para recriar os objetos escritos anteriormente. Um invasor pode manipular o fluxo de entrada processado e substituir ou injetar objetos, o que leva a execução de código arbitrário carregado de um servidor remoto. Esta versão inclui uma verificação para detectar a mais recente vulnerabilidade de desserialização XStream insegura CVE-2021-39149 nos servidores web de destino.

Path Manipulation: Caracteres especiais

Caracteres de controle como 0x09 não devem ser permitidos em um caminho de URL e devem ser codificados com porcentagem pelos clientes. A análise inconsistente destes caracteres de controle entre o proxy e o servidor backend pode apresentar diversas ameaças. Esta versão inclui uma verificação para detectar se alguns caracteres de controle comuns podem ter a sua inserção permitida no caminho do URL e impactar negativamente o servidor web do backend.

Relatórios de conformidade

OWASP Top 10 2021

O Top 10 de 2021, da Open Web Application Security Project oferece um poderoso documento para conscientização sobre a segurança de aplicativos para web, direcionado para informar a comunidade sobre as consequências dos riscos de segurança dos mais comuns e críticos aplicativos para web. O Top 10 da OWASP representa um acordo amplo sobre quais são as falhas de segurança mais críticas dos aplicativos para web, com o consenso inferido da coleta de dados e resultados de pesquisas. Esta atualização SecureBase inclui um novo modelo de relatório de conformidade que fornece correlação entre categorias do OWASP Top 10 2021 e verificações do WebInspect.

Atualizações da política

OWASP Top 10 2021

Uma política personalizada para incluir verificações relevantes para OWASP Top 10 2021 foi adicionada à lista WebInspect SecureBase de políticas com suporte. Essa política contém um subconjunto das verificações do WebInspect disponíveis, que permitem aos clientes executarem varreduras do WebInspect específicas para conformidade.

Erratas diversas

Nesta versão, continuamos a investir recursos para garantir que possamos reduzir o número de problemas de falso-positivos e melhorar a capacidade dos clientes de auditar problemas. Os clientes também podem esperar alterações nos problemas relatados relacionadas com o que segue:

Melhoria na verificação de SSL

A verificação do SSL Cipher List foi melhorada para refletir que a seguinte configuração não suporta Perfect Forward Secrecy: TLS_DH_RSA_WITH_AES_128_GCM_SHA256.

CyberRes 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 Top 10 2021

Para acompanhar as novas correlações, esta versão também contém um novo pacote de relatórios com suporte para o OWASP Top 10 2021, que está disponível para download no Portal de Suporte ao Cliente do Fortify em Conteúdo Premium.

CyberRes Fortify Taxonomy: Software Security Errors

O site do Fortify Taxonomy, que contém descrições para suporte de categoria recém-adicionadas, está disponível em https://vulncat.fortify.com. O site anterior, que contém a última atualização com suporte, está disponível no Portal de Suporte do CyberRes 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, Software Security Research
CyberRes Fortify
hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
Gerente, Software Security Research
CyberRes Fortify
peter.blay@microfocus.com