Software Security Research のリリースに関するお知らせ

Fortify ソフトウェア セキュリティ コンテンツ

2021 年更新版 4

2021 年 12 月 17 日

CyberRes Fortify Software Security Research について

Fortify Software Security Research チームの役割は、最新のセキュリティ調査をもとに Fortify Static Code Analyzer (SCA)、Fortify WebInspect および Fortify Application Defender を含む Fortify 製品ポートフォリオを強化するセキュリティ インテリジェンスをもたらすことです。現在、CyberRes Fortify ソフトウェア セキュリティ コンテンツは、29 の言語における 1,137 もの脆弱性カテゴリをサポートし、100 万を超える API を網羅しています。
Fortify Software Security Research (SSR) は、Fortify Secure Coding Rulepacks (英語、バージョン 2021.4.0)、Fortify WebInspect SecureBase (SmartUpdate で利用可能)、および Fortify Premium Content への更新をまもなくリリースいたします。

CyberRes Fortify Secure Coding Rulepacks [SCA]

このリリースにより、Fortify Secure Coding Rulepacks は 29 のプログラミング言語で脆弱性に関する 917 の固有のカテゴリを検出し、100 万を超える個々の API を網羅します。今回のリリースで追加された主な機能は次のとおりです。

.NET Core および ASP.NET の更新 (サポートされるバージョン: .NET Core 3.1)

以下を含む、.NET Core および ASP.NET Core のさまざまな名前空間に対するサポートを向上しました。

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

このサポートにより、以下のカテゴリの適用範囲が改善されます。

- 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

Azure は、コンピューティング、コンテナー、IoT、AI、機械学習などのさまざまなクラウド サービスを提供する、Microsoft のパブリック クラウド コンピューティング プラットフォームです。

このリリースでは、いくつかの主要な Azure サービスに対する最初のサポートが提供されます。 Functions、Identity、および CosmosDB がこれに該当します。 さらに、以下の特定の Azure の技術についてもサポートするようになりました。

Azure Functions (サポートされるバージョン: Java 1.3.1、C# 3.x)

Functions は、Microsoft Azure のサーバーレス コンピューティング ソリューションです。Azure Functions は、アプリケーションの実行、Web API の構築、データベースの変更への応答、およびメッセージ キューの管理に対応するために、継続して最新のインフラストラクチャを提供します。この更新により、C# および Java 用の以下のトリガー タイプに対する最初のサポートが提供されます。

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

Azure Functions では、以下のカテゴリがサポートされます。

- 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 (サポートされるバージョン: C# 1.5.0、Java 1.4.1)

Azure Identity は、Microsoft のクラウドベースのアイデンティティおよびアクセス管理サービスです。組織内のリソースへの認証および権限を提供します。この更新により、以下の名前空間に対する最初のサポートが提供されます。

C#

- Azure.Identity (version 1.5.0)

Java

- com.azure.identity (version 1.4.1)

Azure Identity では、以下のカテゴリがサポートされます。

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

Azure Cosmos DB (サポートされるバージョン: 3.x)

Azure Cosmos DB は全世界に展開されている、マルチモデル データベース サービスです。Azure Cosmos DB では、API とプログラミング モデルを使用して、ドキュメント型データベース、キーバリュー型データベース、ワイドカラム型データベース、グラフ型データベースの保存と、それらへのアクセスが可能です。この更新により、以下の C# 用の名前空間に対する最初のサポートが提供されます。

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

Azure Cosmos DB では、以下のカテゴリがサポートされます。

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

AWS

Amazon Web Services (AWS) は、コンピューティング、ストレージ、ネットワーキング、データベース、IoT、機械学習など、さまざまなクラウド サービスを提供するパブリック クラウド コンピューティング プラットフォームです。

このリリースでは、いくつかの主要な AWS サービスに対する最初のサポートが提供されます。IAM、DynamoDB、および RDS がこれに該当します。このリリースにより、C# 用の Lambda に対する初期サポートと、Java 用の更新されたサポートも追加されます。さらに、以下の特定の AWS の技術についてもサポートするようになりました。

AWS Lambda のアップデート (サポートされるバージョン: .NET AWS SDK 3.7.x、Java AWS SDK v2 2.17.x) [1]

Lambda は、Amazon Web Services (AWS) の一部として Amazon が提供する、サーバーのプロビジョニングや管理を行わずにコードを実行するコンピューティング サービスです。Lambda サービスはイベントに応答してコードを実行し、コードが必要とするコンピューティング リソースを自動的に管理します。この更新により、C# 用の最初のサポートと、Java 用の追加サポートが提供されます。この更新により、以下の C# 用および Java 用の名前空間に対するサポートが提供されます。

C#

[1] 解析を改善するために、AWS SAM または CloudFormation YAML/JSON テンプレートを変換に含めてください。

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

Java

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

この更新により、以下のイベント タイプに対する最初のサポートが提供されます。

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

AWS Lambda では、以下のカテゴリがサポートされます。

- 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 (サポートされるバージョン: .NET AWS SDK 3.7.x、Java AWS SDK v2 2.17.x)

AWS Identity and Access Management (IAM) は、AWS リソースへのアクセスを制御する Web サービスです。IAM を使用することで、AWS リソースについての認証済みで許可された使用を制御することができます。.この更新により、C# 用および Java 用のサポートが提供されます。この更新により、以下の C# 用および Java 用の名前空間に対するサポートが提供されます。

C#

- Amazon.IdentityManagement.Model

Java

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

機密情報を識別することに加えて、 AWS IAM では以下のカテゴリについてもサポートします。

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

AWS DynamoDB (サポートされるバージョン: .NET AWS SDK 3.7.x、Java AWS SDK v2 2.17.x)

AWS DynamoDB は、フルマネージド NoSQL データベース サービスで、キーバリュー型およびドキュメント型のデータ構造をサポートします。DynamoDB はデータの保存と取得のために使用でき、任意の量のリクエスト トラフィックに対処できます。この更新により、C# 用の最初のサポートと、Java 用の更新されたサポートが提供されます。サポートする名前空間は次のとおりです。

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

AWS DynamoDB では、以下のカテゴリがサポートされます。

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

AWS Relational Database Service (RDS) Data API for Aurora Serverless (サポートされるバージョン: .NET AWS SDK 3.7.x、Java AWS SDK v2 2.17.x)

Amazon Aurora は、MySQL および PostgreSQL 互換のリレーショナル データベース エンジンで、マネージド Amazon Relational Database Service (Amazon RDS) の一部です。AWS RDS Data API により、Web サービス インターフェイスが提供され、アプリケーションが SQL ステートメントにアクセスしてそれらを Aurora Serverless データベース クラスターに対して実行できるようになります。 この更新により、以下の C# 用および Java 用の名前空間に対するサポートが提供されます。

C#

- Amazon.RDSDataService.Model

Java

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

AWS RDS では、以下のカテゴリがサポートされます。

- Access Control: Database
- Setting Manipulation
- SQL Injection

シークレット スキャン

シークレット スキャンに対するサポート。シークレット スキャンは、テキスト ファイル内のシークレットを自動的に検索する技術です。この状況における「シークレット」とは、パスワード、API トークン、暗号化キー、および非開示を意図した同様のアーティファクトを指します。主な目的は、ソース コードと構成ファイルの中に、誤ってハード コーディングされたシークレットを見つけることです。新しい Regex 解析を介して、すべての言語と追加のファイ

ル タイプに対応するようにサポートが拡張されました。[2]サポートされるカテゴリは次のとおりです。

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

Trojan Source

Trojan Source[3] は、脆弱性カテゴリの 1 つで、Nick Boucher 氏と Ross Anderson 氏が論文「Trojan Source: Invisible Vulnerabilities」で発表したものです。彼らによって、開発者の肉眼でコードが見えるようにするための Unicode 特殊文字の 5 つの使用方法が明解に示されていますが、それらを実行した場合、異なる形で機能します。Trojan Source は内部脅威シナリオとして考慮する必要がありますが、その一方で、悪意のある個人が意図的に Unicode 文字を挿入する可能性も考えられます。カテゴリの 1 つの精度のために、次の言語のコア ルールパックに検出サポートを含めています。C、C++、C#、Go、Java、JavaScript、Python、および Rust です。新しくサポートされるカテゴリは次のとおりです。

- Encoding Confusion: BiDi Control Characters

静的問題/動的問題の相関付け[4]

Fortify Software Security Center (SSC) for Java Spring プロジェクトで、静的スキャン結果と動的スキャン結果の相関付けを可能にするためのデータ エクスポートのサポート。サポートされるカテゴリは次のとおりです。

- 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

拡張された IBM メインフレーム COBOL のサポート (サポートされるバージョン: 6.3)

この更新により、IBM メインフレーム COBOL コード内の整数オーバーフローに関する脆弱性の検出が提供されます。

Cloud Infrastructure as Code

クラウドの Infrastructure as Code (IaC) に対するサポート。IaC は、さまざまな手動プロセスではなく、コードを使用してコンピュータ リソースを管理およびプロビジョニングするプロセスで

---

[2] Fortify Static Code Analyzer v21.2.0 以降が必要です。
[3] Fortify Static Code Analyzer v21.2.0 以降が必要です。
[4] Fortify Static Code Analyzer v21.2.0 以降が必要です。相関出力を有効にするには、スキャン時に「com.fortify.sca.rules.enable_wi_correlation」を渡します。これを行うには、コマンドライン引数を使用するか、SCA プロパティ ファイルを変更します。

す。サポートされている技術は、AWS、AWS CloudFormation、Azure ARM、Kubernetes K8S、Azure Kubernetes Service などです。以下のサービスの設定に関連する一般的な問題が、開発者に報告されるようになりました。

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

2021 年 OWASP トップ 10

2021 年の Open Web Application Security Project (OWASP) トップ 10 により、Web アプリケーションのセキュリティに関する強力な啓発文書が提供されています。ここでは、最も一般的で、かつ最も重要な Web アプリケーションのセキュリティ リスクの影響についてコミュニティに周知することに焦点を当てられています。OWASP トップ 10 は、データ収集と調査の結果から得られた知見に基づき、Web アプリケーションのセキュリティ上の最も重大な欠陥が何であるか

について広範な合意を提示しています。Web アプリケーションのリスク軽減を求める顧客をサポートするために、新たに発表された 2021 年 OWASP トップ 10 に対応した Micro Focus Fortify Taxonomy が追加されました。

その他の正誤情報

このリリースでは、誤検出の問題の数を減らし、顧客が問題を監査する能力を向上できるよう、リソースの投資を継続しました。顧客は、以下に関連して報告された問題の変化を確認することもできます。

18.x より前のバージョンの Fortify Static Code Analyzer のサポート廃止

2021.3 リリースに関するお知らせで言及されているように、そのリリースが、18.x より前の Fortify Static Code Analyzer バージョンをサポートするルールパックの最後のリリースでした。このリリースでは、18.x より前のバージョンの Fortify Static Code Analyzer はルールパックをロードしません。これにより、ルールパックをダウングレードするか、SCA のバージョンをアップグレードするかのいずれかを行う必要があります。今後のリリースでは、Fortify Static Code Analyzer の最近 4 つのメジャー リリースを継続してサポートします。

PHP の改善

キー管理におけるパスワードおよび暗号化キーの識別に対するサポートを改善しました。これに該当するのは、Empty/Hardcoded/Null Encryption キー カテゴリです。

Python の改善

サブプロセス モジュールに対するサポートを改善し、Command Injection などの、問題の検出が向上しました。

誤検知の改善:

このリリースでも引き続き、誤検知の除去に取り組みました。他の改善点に加えて、次の領域で誤検知がさらに減ったことを確認できます。

- アプリケーションが Play を使用していない場合に、Scala プロジェクトの Akka アクターから生じる問題。
- URL に対する制御を部分的にしか得られない場合の、JavaScript におけるクロスサイト スクリプティングに関する問題。
- 文字列のローカライズを参照する際の、JSON ファイルでのパスワード管理に関する問題。
- Java および .NET プロジェクトにおける、HTTP メソッドからのデータフローの問題。

CyberRes Fortify SecureBase [Fortify WebInspect]

SmartUpdate からすぐに入手できる以下の更新を実行すると、Fortify SecureBase で、ユーザーをガイドするポリシーと組み合わせて数千の脆弱性のチェックを行うことができます。

API 検出

このリリースには、API 検出に対するチェックが含まれています。API 検出チェックは、WebInspect が、チェック入力によって提供されたユーザー指定の場所で、Swagger の記述 (仕様書) 内の API 定義を検出したときにフラグが立てられます。これらの仕様書ファイルは、どのページにおいても直接参照されない可能性があるため、クロールで検出されません。Swagger 仕様書に対するチェックに加えて、ユーザー指定の場所においては、スキャン中に検出された、チェック入力で明示的に指定されていない定義についても、フラグが付けられてテストされます。これらの検出は必ずしもセキュリティの脆弱性を示すものではありませんが、攻撃に対する潜在的な脆弱性のあるリソースを増加させます。

脆弱性のサポート

OGNL Expression Injection: 二重評価

CVE-2021-26084 によって特定された OGNL Expression Injection の重大な脆弱性が、Atlassian Confluence Server および Data Center に影響します。この脆弱性により、認証されていない攻撃者が、脆弱なアプリケーションに対して任意のコードを実行できます。影響を受ける Atlassian サーバーのバージョンは、バージョン 6.13.23 以前、バージョン 6.14.0 から 7.4.11 以前、バージョン 7.5.0 から 7.11.6 以前、およびバージョン 7.12.0 から 7.12.5 以前になります。このリリースには、影響を受ける Atlassian サーバーにおいて、この脆弱性を検出するためのチェックが含まれています。

ディレクトリ トラバーサル

Apache HTTP サーバーは、CVE-2021-41773 および CVE-2021-42013 によって特定されるディレクトリ トラバーサル攻撃に対して脆弱であることが判明しています。この脆弱性により、攻撃者は、Alias-like ディレクティブによって設定されたディレクトリ以外のファイルに URL をマッピングする URL を操作できるようになります。攻撃者によってサーバー上のファイルの内容が回復され、機密データの漏洩、専有のビジネス ロジックの回復、および一部の構成においては、リモート コードの実行につながる可能性があります。これらの問題の影響を受けるのは、Apache HTTP サーバーのバージョン 2.4.49 および 2.4.50 のみです。このリリースには、Apache HTTP サーバーでこれらの脆弱性を検出するためのチェックが含まれています。

Path Manipulation: 特殊文字

CVE-2021-28164 で特定された Path Manipulation の脆弱性が Eclipse Jetty に影響します。影響を受けるバージョンのデフォルトのコンプライアンス モードで、特殊文字を持つセグメントを含んだ URI を伴うリクエストが、WEB-INF ディレクトリ内の保護されたリソースにアクセスできるようになります。これにより、Web アプリケーションの実装に関する機密情報が開示され、一部のセキュリティ制約が回避されます。このリリースには、脆弱性のある Jetty インスタンスを検出するためのチェックが含まれています。

Dynamic Code Evaluation: Unsafe XStream Deserialization

XStream は、Java オブジェクトと XML の間でデータを変換するためによく使用されるツールです。アンマーシャル時に処理されるストリームには、以前に書き込まれたオブジェクトを再作成するためのタイプ情報が含まれています。攻撃者は、処理された入力ストリームを操作し、オブジェクトを置き換えたり挿入したりすることができます。その結果、リモート サーバから

ロードされた任意のコードが実行されます。このリリースには、ターゲットの Web サーバー上で CVE-2021-39149 の脆弱性である、最新の安全でない XStream デシアライズの脆弱性を検出するためのチェックが含まれています。

Path Manipulation: 特殊文字

0x09 などの制御文字は、URL パスでは使用せず、クライアントによってパーセント エンコーディングされる必要があります。プロキシサーバとバックエンドサーバの間で、これらの制御文字が一貫性なく解析されると、さまざまな脅威が発生する可能性があります。このリリースには、いくつかの一般的な制御文字が URL パスへの挿入を許可される場合に、バックエンドの Web サーバーに悪影響を及ぼすデシアライズの脆弱性を検出するためのチェックが含まれています。

コンプライアンス レポート

2021 年 OWASP トップ 10

2021 年の Open Web Application Security Project (OWASP) トップ 10 により、Web アプリケーションのセキュリティに関する強力な啓発文書が提供されています。ここでは、最も一般的で、かつ最も重要な Web アプリケーションのセキュリティ リスクの影響についてコミュニティに周知することに焦点を当てられています。OWASP トップ 10 は、データ収集と調査の結果から得られた知見に基づき、Web アプリケーションのセキュリティ上の最も重大な欠陥が何であるかについて広範な合意を提示しています。この SecureBase の更新には、OWASP Top 10 2021 のカテゴリおよび WebInspect チェックの相関関係を提供する、新しいコンプライアンス レポートのテンプレートが含まれています。

ポリシーの更新

2021 年 OWASP トップ 10

OWASP Top 10 2021 に関連するチェックを含むようにカスタマイズされたポリシーが、サポートされるポリシーの WebInspect SecureBase リストに追加されました。このポリシーには、顧客がコンプライアンス固有の WebInspect スキャンを実行するために使用できる WebInspect チェックのサブセットが含まれています。

その他の正誤情報

このリリースでは、誤検出の問題の数を減らし、顧客が問題を監査する能力を向上できるよう、リソースの投資を継続しました。顧客は、以下に関連して報告された問題の変化を確認することもできます。

SSL チェックの改善

SSL 暗号リストチェックが改善され、次の設定で完全転送秘密をサポートしていないことを反映するようになりました。TLS_DH_RSA_WITH_AES_128_GCM_SHA256.

CyberRes Fortify Premium Content

リサーチ チームは、コア セキュリティ インテリジェンス製品以外の各種リソースの構築、拡張、保守管理を行います。

2021 年 OWASP トップ 10

新しい相関関係に伴い、このリリースには、Fortify Customer Portal の Premium Content からダウンロード可能な OWASP Top 10 2021 をサポートする新しいレポート バンドルも含まれています。

CyberRes Fortify Taxonomy: ソフトウェア セキュリティ エラー

新たに追加されたカテゴリのサポートに関する説明が記載されている Fortify Taxonomy サイトは、https://vulncat.fortify.com にあります。前回サポートされた更新を含む以前のサイトを探している場合は、CyberRes Fortify Support Portal で見つかる場合があります。

Contact Fortify 技術サポート

CyberRes Fortify
http://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

SSR へのお問い合わせ

Alexander M. Hoole
Software Security Research シニア マネージャー
CyberRes Fortify
hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
Software Security Research マネージャー
CyberRes Fortify
peter.blay@microfocus.com