Fortify ソフトウェア セキュリティ コンテンツ

2023 年更新版 2
2023 年 6 月 30 日

OpenText 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) や Fortify WebInspect 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、Fortify ソフトウェア セキュリティ コンテンツは、31 以上の言語における 1,552 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 (英語版、バージョン 2023.2.0)、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。

Fortify Secure Coding Rulepacks [Fortify Static Code Analyzer]

このリリースにより、Fortify Secure Coding Rulepacks は 31 以上の言語で脆弱性に関する 1,329 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。

Dart のサポート (サポートされているバージョン: 2.19.6)[1]

Google によって開発された Dart ソフトウェア開発キット (SDK) は、デスクトップ、モバイル、Web アプリケーションを構築するための、厳密に型指定されたクラスベースのガベージ コレクション型プログラミング言語を提供します。Dart は、意図したユース ケースに応じて、アプリケーションをアーキテクチャ固有のマシン コード、ポータブル モジュール、または JavaScript にコンパイルできるようにすることで、汎用性を実現します。開発者は Dart を使用して、グラフィカル ユーザー インターフェイス (GUI) を伴うアプリケーションを作成できるため、Dart は幅広いソフトウェア ソリューションを構築する際の柔軟な選択肢となっています。サポートされるカテゴリは次のとおりです。

- 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

Flutter の初期サポート (サポートされているバージョン: 3.7.11)[1]

Google が作成したオープンソースのユーザー インターフェイス (UI) SDK である Flutter は、Dart プログラミング言語の能力を活用しています。クロスプラットフォーム アプリケーションを簡単に作成できるツール、ライブラリ、およびパッケージの包括的なセットを開発者に提供します。開発者は Flutter を使用して、単一のコードベースからモバイル、Web、デスクトップのアプリケーションを構築できるため、開発プロセスが簡素化され、時間と労力を削減できます。Flutter の機能を活用すると、複数のプラットフォーム間でシームレスに実行されて、視覚的に魅力がありパフォーマンスの高いアプリケーションを作

[1] Fortify Static Code Analyzer 23.1.0 が必要です。最良の結果を得るには、Fortify Static Code Analyzer 23.1.1 を使用してください。

成できます。Flutter のサポートには、ユーザーが指定した入力の追跡、Dart プログラミング言語でサポートされているすべてのカテゴリの検出、および Flutter GUI 専用の次のカテゴリが含まれます。

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

Android 13 (API レベル: 33)

Android プラットフォームは、モバイル デバイス用に設計されたオープンソース ソフトウェア スタックです。Android の主なコンポーネントは Java API フレームワークで、このフレームワークによって Android の機能をアプリケーション開発者に公開します。このリリースでは、Android の Java API フレームワークを利用する Java または Kotlin で記述されたネイティブ Android アプリケーションの脆弱性検出が拡張されています。また、Android アプリケーション用に、このリリースでは 5 つの新しい脆弱性カテゴリが導入されています。

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

次の名前空間における既存の脆弱性カテゴリの検出をサポートするために、追加の Android アップデートが含まれています。

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

Java SE JDK (サポートされているバージョン: 17)

Java Platform, Standard Edition (SE) Java Development Kit (JDK) は、Java アプリケーションとコンポーネントの開発に使用するツールとライブラリが含まれたソフトウェア開発パッケージです。このリリースでは、Java SE JDK 15、16、および 17 で導入された新しい API に対して、次の名前空間における既存の脆弱性カテゴリのサポートの更新が含まれています。

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

スキャン範囲の向上には、次のカテゴリで特定された追加の問題が含まれる場合があります。

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

Kotlin 標準ライブラリの更新 (サポートされているバージョン: 1.7.21)

Kotlin は、Java の相互運用性を特徴とする、静的に型指定された汎用言語です。このリリースには、Java 仮想マシン (JVM) を対象とした Kotlin バージョン 1.6 および 1.7 で導入された新しい標準ライブラリ API のサポートの更新が含まれています。

シークレット スキャンの更新

シークレット スキャンは、ソース コードと構成ファイルのシークレットを自動的に検索するための手法です。この文脈において、「シークレット」とはパスワード、API トークン、暗号化キー、およびそれに類似する秘密にしておくべきアーティファクトを指します。このリリースには、次のカテゴリのシークレット スキャンのサポートの更新が含まれています。

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

さらに、次のカテゴリでは、PowerShell スクリプトでシークレット スキャンがサポートされるようになりました。

- Password Management: Hardcoded Password
- Privacy Violation

Cloud Infrastructure as Code (IaC)

Infrastructure as Code は、さまざまな手動プロセスを実行するのではなく、コードを介してコンピューター 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す。サポートされるテクノロジーの適用範囲が拡大され、Amazon Web Services (AWS) および Google Cloud Platform (GCP) にデプロイするための Terraform 構成や、AWS CloudFormation の構成が含まれるようになりました。これらのサービスの構成に関連する共通の問題は、開発者に報告されるようになりました。

AWS Terraform 構成

Terraform は、クラウド インフラストラクチャを構築、変更、およびバージョン管理するための、オープンソース IaC ツールです。これは、HashiCorp 構成言語 (HCL) と呼ばれる独自の宣言型言語を使用します。クラウド インフラストラクチャは、構成ファイルに体系化されて、目的の状態を記述します。Terraform プロバイダーは、AWS インフラストラクチャの構成と管理をサポートします。このリリースでは、Terraform 構成について次の追加カテゴリを報告しています。

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

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

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

GCP Terraform 構成

Terraform は、クラウド インフラストラクチャを構築、変更、およびバージョン管理するための、コード ツールとしてのオープンソース インフラストラクチャです。これは、HashiCorp 構成言語 (HCL) と呼ばれる独自の宣言型言語を使用します。クラウド インフラストラクチャは、構成ファイルに体系化されて、目的の状態を記述します。Terraform プロバイダーは、GCP インフラストラクチャの構成と管理をサポートします。このリリースでは、GCP Terraform 構成について次の脆弱性カテゴリを報告しています。

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

AWS CloudFormation 構成

CloudFormation は、Amazon が提供するサービスで、AWS リソースのプロビジョニングと構成を自動化するために使用します。CloudFormation を使用すると、ユーザーが JSON または YAML テンプレートを使用して AWS リソースを管理できます。このリリースでは、AWS CloudFormation 構成について次の脆弱性カテゴリを報告しています。

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

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

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

カスタマイズ可能なパスワード管理の正規表現の更新

Salesforce Apex、Dart、および PowerShell スクリプトのカスタマイズ可能なパスワード管理の正規表現を、次のプロパティを使用して指定できるようになりました。

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

これらのプロパティを使用すると、Salesforce Apex ソース コード、Dart ソース コード、または PowerShell スクリプトをスキャンする際に、パスワードの識別に使用されるデフォルトの正規表現を上書きできます。

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

OWASP MASVS v2.0.0 標準は、OWASP Mobile Application Security (MAS) プロジェクトの一環として 2023 年 4 月にリリースされました。この標準は、モバイル アプリケーションのセキュリティ要件のベースラインを提供し、モバイル ソフトウェア アーキテクト、開発者、テスターが使用することを目的としています。OWASP MASVS 2.0 は、モバイル デバイス上で実行される「クライアント」モバイル アプリケーションのアプリケーション セキュリティに焦点を当てることを目的としています。そのため、リモート エンドポイントの制御に関連するサーバー側アプリケーションのセキュリティ リスクを評価するには、OWASP ASVS と組み合わせて使用する必要があります。お客様が安全なモバイル アプリケーションを開発し、セキュリティ制御の適用範囲とリスク軽減を目的としてモバイル アプリケーションを評価できるようサポートするために、Fortify Taxonomy と OWASP MASVS v2.0.0 の相関関係が追加されました。

その他の正誤情報

このリリースでは、誤検知の数を減らし、一貫性を確保するためにリファクタリングを行い、お客様の側で問題をより深く調査いただけるようにするため、継続的に力を注いできました。お客様は、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。

「Access Control」カテゴリの廃止

このリリースでは、Salesforce Apex の *Access Control* カテゴリが削除されました。フィールドレベルのセキュリティ チェックの欠如は、*Access Control: Database* および *SOQL Injection* などの他のカテゴリを通じて間接的にキャプチャされるようになりました。

「Link Injection: Auto Dial」カテゴリの廃止

Link Injection: Auto Dial カテゴリは古くなったため削除されました。このカテゴリは、iOS アプリでのサニタイズされていないユーザー入力が攻撃者によって電話番号の自動ダイヤルや Facetime 通話に悪用される可能性があるという脆弱性 CVE-2017-2484 に対処するために導入されました。この悪用は iOS 10.3 アップデートで修正されたため、現在の iOS アプリには関係なくなりました。

廃止された標準マッピング

次の標準とベスト プラクティスは廃止されたものとしてマークされているため、デフォルトでは表示されません。

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

PHP 動的関数[2]

最新の Fortify Static Code Analyzer では PHP サポートが更新されており、サニタイズされていない外部入力によって参照される動的関数に対する*Dynamic Code Evaluation: Code Injection*問題のレポートが可能になります。

Java の安全でないクラス

Java JDK 内には、インスタンス化するのにリフレクションが必要で、開発者が通常利用できなく、本質的に安全でないアクションを実行するための隠しクラスがあります。Java プロジェクト内で `sun.misc.Unsafe` クラスを使用すると、スキャン結果で使用状況が *Often Misused: sun.misc.Unsafe* として報告されるようになりました。

[2] SCA 23.1 以降が必要

誤検知の改善

このリリースでは、誤検知を排除する取り組みが引き続き行われています。他の改善点に加え、次の分野で誤検知の排除が進んでいます。

- *Access Control: Unenforced Sharing Rules* - Salesforce トリガー、Visualforce ページ、およびコンポーネントでの誤検知を排除
- *Command Injection* - JavaScript で正規表現にフラグを付けるときの誤検知を排除
- *Cookie Security: Cookie not Sent Over SSL* - 推奨される修正方法が適用された場合の Swift での誤検知を排除
- *Credential Management: Hardcoded API Credentials* - ベアラー トークンの識別時の誤検知を排除
- *Dead Code: Expression is Always false* - Java switch ステートメントに表示される場合の誤検出を排除
- *Dockerfile Misconfiguration: Dependency Confusion* - Dockerfile 内の「apt」および「apt-get」コマンドでの誤検知を排除
- *Log Forging (debug)* - HTTP リクエスト ヘッダー値を出力する場合の Salesforce Apex アプリケーションでの誤検知を排除
- *Race Condition: Signal Handling* - `sigaction()` を呼び出す場合の C/C++ での誤検出を排除
- *String Termination Error* - C++ のプリミティブ型でトリガーする場合の誤検知を排除
- *Unused Method* - 実装された Serializable メソッドによってメソッドが呼び出される Java コードでの誤検出を排除
- Boolean 値でトリガーされた可能性のある JavaScript のデータフロー誤検知を排除

カテゴリの変更

脆弱性カテゴリ名が変更された場合、以前のスキャンを新しいスキャンとマージしたときの分析結果では、カテゴリが追加または削除されています。

整合性向上のため、次のカテゴリの名前を変更しました。

- *Azure Terraform Misconfiguration: Improper CosmosDB CORS Policy* は、*Azure Terraform Misconfiguration: Improper Cosmos DB CORS Policy として報告されるようになりました*
- *Kubernetes Misconfiguration: Missing ServiceAccount Admission Controller* は、*Kubernetes Misconfiguration: Missing Service Account Admission Controller として報告されるようになりました*
- *NoSQL Injection: CosmosDB* は、*NoSQL Injection: Cosmos DB として報告されるようになりました*

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。

脆弱性のサポート

Insecure Deployment: Unpatched Application:

エンタープライズ モバイル アプリケーションおよび Web アプリケーションの作成に使用するオープンソース Java ライブラリである ZK Framework には、CVE-2022-36537 で特定されたセキュリティ脆弱性が含まれています。攻撃者はこの脆弱性を悪用して、Web コンテキストにあるファイルのコンテンツを取得する可能性があります。悪用に成功すると、攻撃者は機密情報を取得したり、他の方法では到達できないエンドポイントを標的にしたりすることができます。このリリースには、影響を受ける ZK Framework バージョンを使用するターゲット サーバーで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。

その他の正誤情報

このリリースでは、誤検知の数を減らし、お客様の側で問題をより深く調査いただけるようにするため、継続的に力を注いできました。以下の分野に関連して報告された内容にも、問題の変化を実感いただけるはずです。

Command Injection:

ID 11722 および 11723 で識別されるチェックは、Out-of-band Application Security Testing (OAST) 機能[3]をサポートするペイロードを使用するように追加されました。これらにより、誤検知が減少し、WebInspect スキャン結果の精度が向上します。

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。

OWASP MASVS v2.0.0

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 MASVS v2.0.0 をサポートする Fortify Software Security Center の新しいレポート バンドルも含まれています。

[3] 11723 チェックは大量のリクエストを送信するため、標準ポリシーからは除外されます。「すべてのチェック」ポリシーを使用するか、チェックを含めるように既存のポリシーをカスタマイズするか、カスタム ポリシーを作成してこのチェックを実行します。

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。
上記のライブ サイトと一致する Fortify Taxonomy サイトの新しいオフクラウド バージョンを、お客様が Fortify サポート ポータルからダウンロードできるようになりました。

Fortify 技術サポートへの問い合わせ

OpenText Fortify
https://softwaresupport.softwaregrp.com/
+1 (800) 509-1800

SSR へのお問い合わせ

Alexander M. Hoole
Software Security Research、シニア マネージャー
OpenText Fortify
hoole@opentext.com
+1 (650) 427-9973

Peter Blay
Software Security Research、マネージャー
OpenText Fortify pblay@opentext.com
+1 (669) 309-1634