Fortify ソフトウェア セキュリティ コンテンツ

2023 年更新版 3
2023 年 9 月 29 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、33 以上の言語における 1,627 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 2023.3.0)、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 33 以上の言語で脆弱性に関する 1,403 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。

改善された Android 13 のサポート (サポートされているバージョン: 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、このリリースでは次の 3 つの新しい脆弱性カテゴリが導入されています。

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

Android Jetpack (AndroidX) の初期サポート

Android Jetpack は、開発者が Android アプリケーションをより簡単に作成できるようにするライブラリ、ツール、ガイダンスのセットです。Jetpack は androidx.* パッケージを対象としており、プラットフォーム API からバンドル解除されているため、下位互換性が促進され、より頻繁な更新が可能です。このリリースでは、このソフトウェア スイートの初期対象範囲を提供します。

Android Jetpack の初期対象範囲では、次のライブラリの脆弱性の検出がサポートされています。

- 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)

カテゴリの対象範囲の改善例には次のようなものがあります。

- Access Control: Database
- Command Injection
- Denial of Service

- Denial of Service: Regular Expression
- Header Manipulation
- 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

MySQL Connector/Python のサポート (サポートされているバージョン: 8.1.0)

MySQL Connector/Python は、Python アプリケーションと MySQL データベース間の対話を容易にするソフトウェア ライブラリです。これは、Python プログラミング言語と MySQL データベース管理システムの間のブリッジまたはコネクタとして機能し、開発者が Python コードを使用して MySQL データベースのデータに簡単に接続し、クエリの実行や操作を行えるようにします。

改善されたカテゴリの対象範囲には、以下が含まれます。

- 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

改善された Django のサポート (サポートされているバージョン: 3.2)

Django は、安全かつ迅速な Web 開発を促進するように設計された、Python で記述された Web フレームワークです。開発の速度と安全性は、コードの構築と生成を使用して定型コードを大幅に縮小する、フレームワークの高度な抽象化によって実現されます。このリリースでは、既存の Django の対象範囲を更新し、バージョン 3.2 までのリリースをサポートしています。

改善された対象範囲には、*Django.contrib.auth.models*、*Django.db.models*、、および *Django.http.response* の名前空間が含まれます。さらに、脆弱性カテゴリの対象範囲が改善され、以下が含まれます。

- 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

Bicep の初期サポート (サポートされているバージョン: 0.21.1)[1]

Microsoft Bicep は、Azure リソースの展開を簡素化および合理化するために Microsoft によって開発された、Infrastructure-as-Code (IaC) ソリューション用のオープンソースのドメイン固有言語 (DSL) です。これは、Azure Resource Manager (ARM) テンプレート上の抽象化レイヤーとして機能し、Azure インフラストラクチャを定義および管理するためのより直感的で読み取りやすい方法を提供します。Bicep を使用すると、ユーザーは簡潔で人が読めるコードを記述して、Azure のリソース、構成、依存関係を表現できます。

脆弱性カテゴリの初期対象範囲には以下が含まれます。

- 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] Fortify Static Code Analyzer 23.2.0 以降が必要です。Bicep の初期セキュリティ コンテンツは、Fortify Static Code Analyzer 23.2.x とともに配布されます。

- 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

Solidity の初期サポート (サポートされているバージョン: 0.8.x)[2]

Solidity は、さまざまな分散型ブロックチェーン環境、特にイーサリアム ブロックチェーンでスマート コントラクトを開発するために使用されるオブジェクト指向プログラミング言語です。Solidity で記述されたスマート コントラクトは、主にイーサリアム仮想マシン (EVM) 上で実行されますが、他の互換性のある仮想マシン上でも実行できます。

脆弱性カテゴリの初期対象範囲には以下が含まれます。

- 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] Fortify Static Code Analyzer 23.2.0 以降が必要です。 Solidty の初期セキュリティ コンテンツは、Fortify Static Code Analyzer 23.2.x とともに配布されます。

- 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

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範囲が拡大され、Microsoft Azure に展開するための Terraform 構成や AWS Ansible 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。

Microsoft Azure 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、Microsoft Azure インフラストラクチャの構成と管理をサポートします。脆弱性カテゴリの対象範囲が改善され、Terraform 構成については以下が含まれます。

- 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

Amazon Web Services (AWS) Ansible の構成
Ansible は、構成管理、アプリケーション展開、クラウド プロビジョニング、およびノード オーケストレーションをさまざまな環境に提供するオープンソースの自動化ツールです。Ansible には、Amazon Web Services (AWS) の構成と管理をサポートするモジュールが含まれています。脆弱性カテゴリの対象範囲が改善され、AWS Ansible 構成については以下が含まれます。

- 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
2019 年に、SANS Top 25 に代わる Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) が導入されました。2023 年 6 月にリリースされた 2023 CWE Top 25 はヒューリスティック式を使用して判定され、過去 2 年間にわたって National Vulnerability Database (NVD) へ報告された脆弱性の頻度と重大度を正常化します。NVD で最も一般的に報告される重大な脆弱性の周辺を監査することを優先する顧客をサポートするため、2023 CWE Top 25 に対応した Fortify Taxonomy が追加されています。

OWASP API Security Top 10 2023

Open Worldwide Application Security Project (OWASP) API Security Top 10 2023 は、API に最も影響を与える 2023 年度のセキュリティ リスクの一覧を示すものです。これは、API のセキュリティ上の脆弱性についての意識を高め、Web API を保護する必要がある開発者、デザイナー、アーキテクト、マネージャー、組織全般など、API の開発とメンテナンスに携わる人々を教育することを目的としています。

OWASP API Security Top 10 は、Web API に影響を与える脆弱性に焦点を当てており、単独で使用するのではなく、関連するあらゆるリスクを徹底的に把握するために、他の標準やベスト プラクティスと組み合わせて使用することを目的としています。たとえば、インジェクションなどの入力検証に関連する問題を特定するには、OWASP Top 10 と組み合わせて使用する必要があります。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 OWASP API Security Top 10 2023 に対応した Fortify Taxonomy が追加されています。

Center for Internet Security (CIS) のベンチマーク

Center for Internet Security (CIS) のベンチマークは、CIS Critical Security Controls に対応する、コミュニティによって開発された安全な構成の推奨事項を集めたものです。これらの推奨事項は、クラウド インフラストラクチャの保護を可能にし、業界標準への準拠を実証することを目的としています。CIS ベンチマークは、対象となる 25 以上のベンダー製品ファミリーに対する、サイバーセキュリティの進化に適応するために継続的に更新されます。サポートされる製品ファミリーには次のものが含まれます。

- 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]

Smart Contract Weakness Classification (SWC) は、スマート コントラクトの脆弱性を分類して説明する体系的なフレームワークです。これは、イーサリアムなどのブロックチェーン上で実行される自己実行コード部分の脆弱性を理解し、それに対処するための標準化された方法を提供します。特に、SWC レジストリの内容は 2020 年以降包括的に更新されておらず、その結果、既知の不完全さ、エラー、重要な欠落が生じています。スマート コントラクトのリスク軽減を求める顧客をサポートするために、SWC の現在のバージョンに対応する Fortify Taxonomy が追加されています。

[3] Fortify Static Code Analyzer 23.2.0 以降からのスキャンが必要です。

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、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。

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

2022.4 リリースで行われたように、Fortify Static Code Analyzer の最新の 4 つのメジャー リリースを引き続きサポートします。したがって、これは、20.x より前のバージョンの Fortify Static Code Analyzer をサポートする Rulepack の最後のリリースになります。次のリリースでは、20.x より前のバージョンの Fortify Static Code Analyzer は最新の Rulepack をロードしません。これには、Rulepack をダウングレードするか、Fortify Static Code Analyzer のバージョンをアップグレードするかのいずれかの必要があります。今後のリリースでは、Fortify Static Code Analyzer の最新の 4 つのメジャー リリースを継続してサポートします。

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。

- *ASP.NET MVC Bad Practices: Optional Submodel With Required Property* - ASP.NET アプリケーションの仮想フィールドに関連する誤検知を排除
- *Code Correctness: Double-Checked Locking* - Java アプリケーションでの誤検知を排除
- *Cross-Site Request Forgery* - .NET アプリケーションの "AntiForgery.GetHtml()" または "Html.AntiForgeryToken()" を使用した HTML フォームの誤検知を排除
- *Cross-Site Scripting: Persistent* - Django アプリケーションの "cycle" タグに関連する誤検知を排除
- *Double Free* - ブーストライブラリからの "throw_error()" を使用する C/C++ アプリケーションでの誤検知を排除
- *HTML5: Missing Content Security Policy* - Java アプリケーションでの誤検知を排除
- *JSON Injection* - PHP アプリケーションでの誤検知を排除
- *Mass Assignment: Insecure Binder Configuration* - .NET アプリケーションの列挙型に関連する誤検知を排除
- *Often Misused: File System* - C++ アプリケーションの "GetFullPathNameW()" および同様の関数呼び出しに関連する誤検知を排除
- *Path Manipulation* - Amazon AWS SDK を使用した Java アプリケーションでの誤検知を排除
- *Type Mismatch: Signed to Unsigned* - C/C++ アプリケーションのブール値に関連する誤検知を排除
- *Unreleased Resource* - C++ アプリケーションで "CreateFileW()" を使用するときの誤検知を排除

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 14 件のカテゴリの名前を変更しました。

削除されたカテゴリ	追加されたカテゴリ
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

Fortify Priority Order の変更

顧客管理による暗号化キーの欠落に関連する脆弱性カテゴリ全体の一貫性を向上するため、次の 20 件のカテゴリの Fortify Priority Order が「低」に変更されました。

- *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]

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

vBulletin バージョン 5.6.0 ～ 5.6.8 での事前認証のリモート コード実行 (RCE) の脆弱性が CVE-2023-25135 で特定されました。ダイナミックなオンライン コミュニティやフォーラムを構築するための人気ソフトウェアである vBulletin は、ユーザーが提供した入力を不適切にサニタイズし、不正な逆シリアル化を招きます。この問題により、攻撃者はサーバー上で任意のコードを実行し、アプリケーション ロジックを悪用し、Denial of Service (DoS) 攻撃を仕掛けることができます。このリリースには、対象のサーバー上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。

プロトタイプ汚染: サーバー側

サーバー側のプロトタイプ汚染は、攻撃者がオブジェクトのプロトタイプを操作できる場合に発生します。これは、JavaScript などのプロトタイプベースの言語で可能であり、これにより、実行時にプロパティやメソッドを変更できてしまいます。この悪用の重大度は、汚染されたオブジェクトがアプリケーション内のどこで使用されるかによって異なります。攻撃には、Denial of Service、アプリケーション構成の変更、および、場合によってはリモート コード実行があります。このリリースには、Web アプリケーションのプロトタイプ汚染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

2023 Common Weakness Enumeration (CWE™) Top 25

2019 年に、SANS Top 25 に代わる Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) が導入されました。6 月にリリースされた 2023 CWE Top 25 はヒューリスティック式を使用して判定され、過去 2 年間にわたって National Vulnerability Database (NVD) へ報告された脆弱性の頻度と重大度を正常化します。この SecureBase の更新には、CWE Top 25 で特定されているカテゴリに直接マッピングするか、または Top 25 の CWE-ID と関連する CWE-ID に「ChildOf」関係を通してマッピングするチェックが含まれています。

OWASP API Security Top 10 2023

Open Worldwide Application Security Project (OWASP) API Security Top 10 2023 は、API に最も影響を与える 2023 年度のセキュリティ リスクの一覧を示すものです。これは、API のセキュリティ上の脆弱性についての意識を高め、Web API を保護する必要がある開発者、デザイナー、アーキテクト、マネージャー、組織全般など、API の開発とメンテナンスに携わる人々を教育することを目的としています。OWASP API Security Top 10 は、Web API に影響を与える脆弱性に焦点を当てており、単独での使用を目的とはしていません。そうではなく、関連するあらゆるリスクを徹底的に把握するために、他の標準やベスト プラクティスと組み合わせて使用することを目的としています。たとえば、OWASP API Security Top 10 2023 を OWASP Top 10 と組み合わせて使用し、インジェクションなどの入力検証に関連する問題を特定します。この SecureBase アップデートには、OWASP API Security Top 10 2023 のカテゴリと 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

2023 CWE Top 25

2023 CWE Top 25 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。

OWASP API Security Top 10 2023

OWASP API Security Top 10 2023 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。

LDAP Injection

このリリースでは、誤検知を減らし、結果の精度を上げるため、LDAP Injection チェックが改善されています。

SSL 証明書のホスト名の不一致

SSL 証明書のホスト名の不一致についてのチェック レポート コンテンツには、顧客がこのセキュリティ問題に適切な修正を適用するのに役立つ、より詳細な情報が含まれるようになりました。

チェック入力によるアグレッシブ カバレッジ

一部の WebInspect チェックでは、より広範囲のエンドポイントを対象とする攻撃の長いリストを送信するように WebInspect をガイドする、アグレッシブ カバレッジを有効にすることができます。このリリースでは、これらのチェックが改善がされており、これにより顧客は、スキャン ポリシーに個別のチェックを追加するのではなく、チェック入力を変更することで アグレッシブ カバレッジを設定できるようになります。アグレッシブ カバレッジ機能があるチェックには次のものが含まれます。*Log4Shell*、*JNDI Reference Injection*、*Server-Side Request Forgery*、*OS Command Injection*、および *Server-Side Prototype Pollution*。アグレッシブ カバレッジを有効にしたチェックでは、より正確なスキャンを実行できます。ただし、リクエストの数とスキャン時間が大幅に増加する可能性があることを考慮することが重要です。したがって、Fortify では、別のポリシーで他のチェックを指定せずにアグレッシブ カバレッジを有効にして、チェックを実行することを強くお勧めします。

Web Server Misconfiguration: 保護されていないファイル

このリリースには、Java 関連の構成ファイルの検出を改善する、軽微なバグ修正が含まれています。

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。

2023 CWE Top 25

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 2023 CWE Top 25 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。

OWASP API Security Top 10 2023

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 API Security Top 10 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。

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。

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