Fortify ソフトウェア セキュリティ コンテンツ

2023 年更新版 4
2023 年 12 月 15 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 OpenText™ Fortify Static Code Analyzer (SCA) や OpenText™ 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 1,657 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 2023.4.0)、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。

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 1,432 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 Python のサポート (サポートされているバージョン: 3.12)

Python は、動的な型付けと効率的な高レベル データ構造を備えた、強力な汎用プログラミング言語です。構造化プログラミング、オブジェクト指向プログラミング、関数型プログラミングなど、複数のプログラミング パラダイムをサポートしています。このリリースでは、Python の最新バージョンへの対応範囲を広げて、Python の標準ライブラリ API の変更に対するサポートを拡大しています。次のモジュールについて、既存のルールの対象範囲を更新しています。

- os
- pathlib
- tomllib

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: 4.2)

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、次のリリースをサポートしています: 4.0、4.1、および 4.2。

改善された対象範囲には、次の名前空間が含まれます: *asyncio*、*django.core.cache.backends.base.BaseCache*、*django.db.models.Model*、および *django.middleware.security.SecurityMiddleware*。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。

- Header Manipulation
- Insecure Cross-Origin Opener Policy
- Resource Injection
- Setting Manipulation

PyCryptodome と PyCrypto (サポートされているバージョン: 3.19.0)

PyCryptodome は、暗号化のアルゴリズムとプロトコルの包括的なコレクションを提供する自己完結型の Python パッケージです。これは、拡張され、よりアクティブに管理される PyCrypto ライブラリのバージョンとして機能します。PyCryptodome は幅広い暗号化機能を提供するように設計されており、安全な通信、データ保護、暗号化操作を Python アプリケーションに実装する必要がある開発者にとって多用途の選択肢となります。

脆弱性カテゴリの初期対象範囲には以下が含まれます。

- Key Management: Empty Encryption Key
- Key Management: Empty PBE Password
- Key Management: Hardcoded Encryption Key
- Key Management: Hardcoded HMAC Key
- Key Management: Hardcoded PBE Password
- Key Management: Unencrypted Private Key
- Password Management: Hardcoded Password
- Password Management: Lack of Key Derivation Function
- Password Management: Password in Comment
- Weak Cryptographic Hash
- Weak Cryptographic Hash: Hardcoded PBE Salt
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Cryptographic Hash: Predictable Salt
- Weak Cryptographic Signature: Insufficient Key Size
- Weak Encryption
- Weak Encryption: Insecure Initialization Vector
- Weak Encryption: Insecure Mode of Operation
- Weak Encryption: Insufficient Key Size
- Weak Encryption: Stream Cipher
- Weak Encryption: User-Controlled Key Size

機械学習 (ML) および人工知能 (AI) モデルに起因するリスクの検出

生成 AI と大規模言語モデル (LLM) の使用により、ソフトウェア業界のソリューション領域が急速に変化しており、新たなリスクが生じています。Fortify の初期サポートは、OpenAI API、Amazon Web Services (AWS) SageMaker、または LangChain を使用する Python プロジェクトを対象としています。サポートは、AI/ML モデル API からの応答の暗黙的な信頼に起因する脆弱性を検出するだけでなく、次のような独自の機能も検出します。

Python OpenAI API の初期サポート (サポートされているバージョン: 1.3.8)

OpenAI Python ライブラリを使用すると、開発者は OpenAI REST API に簡単にアクセスして、GPT-4 や DALL-E などの OpenAI モデルと対話できるようになります。OpenAI API を使用すると、アプリケーションは OpenAI モデルにプロンプトを送信し、生成された応答を受信したり、既存のモデルを微調整したりすることができます。OpenAI Python モジュールは、*httpx* を利用して非同期リクエストと同期リクエストの両方を送受信する機能をサポートしています。サポートには、モデルからの危険性のある出力の特定、および次の新しいカテゴリが含まれます。

- Cross-Site Scripting: AI

Python AWS SageMaker (Boto3) の初期サポート (サポートされるバージョン: 1.33.9)

AWS SageMaker は、Amazon AWS の広範なサービス群に含まれる製品の 1 つです。AWS SageMaker は、カスタムモデルのトレーニングから MLOps がサポートする完全な開発パイプラインのセットアップに至るまで、さまざまな ML プロジェクトをサポートする幅広いツールセットを提供します。

Amazon の SDK for Python (Boto3) を使用すると、AWS SageMaker を含むさまざまな AWS 製品との通信が可能になります。サポートには、モデルからの危険性のある出力の特定、および次の新しいカテゴリが含まれます。

- Cross-Site Scripting: AI

Python LangChain の初期サポート (サポートされているバージョン: 0.0.338)[1]

LangChain は、大規模言語モデル (LLM) を使用したアプリケーション開発のための人気のあるオープンソース オーケストレーション フレームワークです。LangChain は、チャットボットや仮想エージェントなど、LLM 駆動のアプリケーションを簡単に作成できるツールと API を提供します。これらは、Python と JavaScript に基づいたライブラリとして利用できます。サポートには、モデルからの危険性のある出力の特定、*Path Manipulation* の検出、および次の新しいカテゴリが含まれます。

- Cross-Site Scripting: AI

.NET 8 のサポート (サポートされているバージョン: 8.0.0)

.NET 7 の後継である .NET 8 は、クロスプラットフォームのオープンソース開発フレームワーク (無償) で、プログラマーは標準化された一連の API を使用して C# や VB などのさまざまな言語でアプリケーションを作成できます。このリリースでは、対象範囲が .NET の最新バージョンに拡張され、新規および既存の API の脆弱性の検出が強化されています。

拡張された対象範囲には、次の名前空間が含まれます。

- System.Collections.Frozen
- System.Net.Http.Json
- System
- System.Security
- System.Text
- System.Text.Unicode
- System.Net.Http

Java Simplified Encryption (Jasypt) (サポートされているバージョン: 1.9.3)

Java Simplified Encryption (Jasypt) は、パスワードベースの暗号化を実行し、保存用のパスワード ダイジェストを作成するために使用される小さい Java ライブラリです。Spring、Wicket、Hibernate などの一般的な Java フレームワークと統合されています。

脆弱性カテゴリの初期対象範囲には以下が含まれます。

- Insecure Randomness
- Key Management: Empty PBE Password
- Key Management: Hardcoded PBE Password
- Key Management: Null PBE Password
- Password Management: Lack of Key Derivation Function
- Privacy Violation: Heap Inspection

[1] LangChain は非常に新しい機能です。運用環境で使用する場合は、事前にセキュリティを慎重に考慮して評価する必要があります。

- Setting Manipulation
- Weak Cryptographic Hash
- Weak Cryptographic Hash: Empty PBE Salt
- Weak Cryptographic Hash: Hardcoded PBE Salt
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Cryptographic Hash: User-Controlled PBE Salt
- Weak Encryption
- Weak Encryption: Insecure Mode of Operation

ECMAScript 2023

ES2023 または ES14 とも呼ばれる ECMAScript 2023 は、JavaScript 言語の ECMAScript 標準の最新バージョンです。ES2023 の主な機能には、コピーによる変更と、末尾からの検索を可能にする新しい配列関数があります。ES2023 のサポートにより、関連するすべての JavaScript 脆弱性カテゴリの対象範囲が ECMAScript 標準の最新バージョンにまで拡張されます。

プロトタイプ汚染

プロトタイプ汚染は、JavaScript アプリケーションの脆弱性であり、これにより、悪意のあるユーザーがビジネス ロジックをバイパスしたり影響を与えたり、独自のコードを実行したりする可能性があります。

このルールパック更新は、攻撃者が次の NPM パッケージに対してオブジェクトのプロトタイプを汚染できるかどうかを検出します。

- assign-deep
- deap
- deep-extend
- defaults-deep
- dot-prop
- hoek
- lodash
- merge
- merge-deep
- merge-objects
- merge-options
- merge-recursive
- mixin-deep
- object-path
- pathval

Kubernetes の構成

Kubernetes は、コンテナー化されたアプリケーションの展開、スケーリング、管理を自動化するためのオープンソースのコンテナー管理ソリューションです。これは、基盤となるインフラストラクチャへの依存関係を削除するコンテナー中心のインフラストラクチャ抽象化を提供することで、ポータブルな展開を可能にし、複雑な分散システムの管理を簡素化します。以下は、拡張された脆弱性カテゴリの対象範囲の一部です。

- Kubernetes Misconfiguration: Improper API Server Network Access Control
- Kubernetes Misconfiguration: Improper CronJob Access Control
- Kubernetes Misconfiguration: Improper DaemonSet Access Control
- Kubernetes Misconfiguration: Improper Deployment Access Control
- Kubernetes Misconfiguration: Improper Job Access Control
- Kubernetes Misconfiguration: Improper Pod Access Control
- Kubernetes Misconfiguration: Improper RBAC Access Control
- Kubernetes Misconfiguration: Improper ReplicaSet Access Control
- Kubernetes Misconfiguration: Improper Replication Controller Access Control
- Kubernetes Misconfiguration: Improper StatefulSet Access Control
- Kubernetes Misconfiguration: Insecure Secret Transport
- Kubernetes Misconfiguration: Insufficient Kubelet Logging
- Kubernetes Misconfiguration: Scheduler System Information Leak
- Kubernetes Misconfiguration: Uncontrolled Kubelet Resource Consumption
- Kubernetes Terraform Misconfiguration: Improper Daemon Set Access Control
- Kubernetes Terraform Misconfiguration: Improper Deployment Access Control
- Kubernetes Terraform Misconfiguration: Improper Job Access Control
- Kubernetes Terraform Misconfiguration: Improper Pod Access Control
- Kubernetes Terraform Misconfiguration: Improper Pod Network Access Control
- Kubernetes Terraform Misconfiguration: Improper RBAC Access Control
- Kubernetes Terraform Misconfiguration: Improper Replication Controller Access Control
- Kubernetes Terraform Misconfiguration: Improper Stateful Set Access Control
- Kubernetes Terraform Misconfiguration: Insecure Secret Transport

DISA STIG 5.3

コンプライアンスの分野で当社の政府機関顧客をサポートするため、米国国防情報システム局 (DISA) のアプリケーション セキュリティおよび開発の STIG バージョン 5.3 に対応した Fortify Taxonomy が追加されました。

OWASP Mobile Top 10 Risks 2023

Open Worldwide Application Security Project (OWASP) Mobile Top 10 Risks 2023 は、モバイルのセキュリティ リスクに対する意識を高め、モバイル アプリケーションの開発と保守に携わる人々を教育することを目的としています。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、OWASP Mobile Top 10 2023 の初期リリースに対応した Fortify Taxonomy が追加されています。

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、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

2023.3 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、20.x より前の 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、20.x より前のバージョンの Static Code Analyzer はルールパックをロードしません。これには、ルールパックをダウングレードするか、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、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。

誤検知の削減および検出機能に関するその他の改善点

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。誤検知がさらに減っており、以下の分野で著しい改善が見られることを実感いただけるはずです。

- *ASP.NET Misconfiguration: Persistent Authentication* - フォーム認証サービスを使用する ASP.NET アプリケーションで誤検知を排除
- *Credential Management: Hardcoded API Credentials* - HTTP ベアラー トークンに関連するシークレットスキャンから誤検知を排除
- *Credential Management: Hardcoded API Credentials* - Avature API キーの新しい問題を検出
- *Cross-Site Request Forgery* -「Express.js」JavaScript フレームワークを使用する NodeJS アプリケーションで新しい問題を検出
- *Cross-Site Scripting* -「html/template」パッケージを使用する Go アプリケーションで新しい問題を検出
- *Cross-Site Scripting: Reflected* - 次を使用する ASP.NET アプリケーションで誤検知を排除:「ListControl」クラス
- *Denial of Service: Format String* - OWASP Top 10 カテゴリに対する誤ったマッピング
- *Insecure Transport* - ASP.NET アプリケーションで、プライベート ユーザー データを処理するコントローラー メソッドに関連する誤検知を排除
- *Insecure Transport: Mail Transmission* - 次を使用する Python アプリケーションから誤検知を排除:「smtplib.SMTP」クラス
- *Key Management: Hardcoded Encryption Key* -「RSAKeyGenParameterSpec」クラスを使用する Java アプリケーションで誤検知を排除
- *Link Injection: Missing Validation* -「WKNavigationDelegate」プロトコル[2] を使用する Swift および Objective-C アプリケーションで誤検知を排除
- *Mass Assignment: Insecure Binder Configuration* - Jakarta EE API を使用する Java アプリケーションから誤検知を排除
- *Password Management: Password in Configuration File* - 構成ファイルで誤検知を排除
- *Path Manipulation* - PHP アプリケーションでファイルのアップロードに関する新しい問題を検出
- *SQL Injection* - marsdb データベースを使用する NodeJS アプリケーションで新しい問題を検出
- *SQL Injection: MyBatis Mapper* - MyBatis マッパー XML ファイルで新たな問題を検出
- *String Termination Error* -「printf()」およびそのバリアントを使用する C/C++ アプリケーションで誤検知を排除
- *System Information Leak: Incomplete Servlet Error Handling* - Java アプリケーションで誤検出を排除
- *Weak Encryption: Insecure Initialization Vector* -「Pycryptodome」ライブラリを使用する Python アプリケーションで誤検知を排除
- *Unreleased Resource: Streams* -「java.nio.file」API を使用する Java アプリケーションで検出漏れを特定
- ユーザー プロファイル情報に関連する Visualforce アプリケーションでさまざまなデータフロー誤検知を検出

[2] Fortify Source Code Analyzer 23.1 以降が必要

カテゴリ名の変更

脆弱性カテゴリの名前が変更された場合、以前のスキャンの分析結果を新しいスキャンとマージすると、カテゴリが追加または削除される場合があります。

整合性向上のため、次の 2 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
Azure ARM Misconfiguration: Insecure DataBricks Storage	Azure ARM Misconfiguration: Insecure Databricks Storage
Azure ARM Misconfiguration: Insecure Redis Enterprise Transport	Azure ARM Misconfiguration: Insecure Redis Transport

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

Access Control: 管理インターフェイス

このリリースには、ゲートウェイ アクチュエーター エンドポイントが有効化されている、公開されている、またはセキュリティで保護されていないときに、Spring Cloud Gateway の安全でない構成を検出するチェックが含まれています。このような状況では、攻撃者が新しいルートを作成し、アプリケーションの代わりに内部資産や機密資産にアクセスできてしまいます。この結果、クラウド メタデータ キーの盗難、内部アプリケーションの公開、またはサービス拒否 (DoS) 攻撃が発生する可能性があります。

Expression Language Injection: Spring

Spring Cloud Gateway バージョン 3.1.0、3.0.0 ～ 3.0.6、および 3.0.0 より古いバージョンには、CVE-2022-22947 で特定されるセキュリティ脆弱性が含まれています。この脆弱性により、ゲートウェイ アクチュエーター エンドポイントが有効化されている、公開されている、またはセキュリティで保護されていない場合に、コード インジェクション攻撃が可能になります。このリリースには、影響を受ける Spring Cloud Gateway バージョンを使用するターゲット サーバーにこの脆弱性があるかどうかを検出するためのチェックが含まれています。

Insecure Deployment: Unpatched Application

バージョン 2023.05.3 以前の TeamCity On-Premises サーバーは認証をすり抜けやすいため、認証されていない攻撃者がサーバー上でリモート コード実行 (RCE) を実行するおそれがあります。この脆弱性は CVE-2023-42793 で特定されています。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。

情報の発見: 文書化されていない API

API エンドポイントのドキュメントが文書化されていない、または限定的にしかない場合、セキュリティの脆弱性について十分にテストされていない攻撃対象領域を攻撃者に提供することになります。攻撃者は偵察を実行して、廃止されたエンドポイント、パッチ未適用のエンドポイント、およびメンテナンスされていないエンドポイントを見つけ、機密情報や危険な機能にアクセスする可能性があります。このリリースには、アクセスは可能だが API 仕様のドキュメントで定義されていない、バージョン管理された API エンドポイントを検出することを目的としたチェックが含まれています。

コンプライアンス レポート

DISA STIG 5.3

当社の政府機関顧客のコンプライアンス ニーズに対応するため、このリリースには、米国国防情報システム局 (DISA) のアプリケーション セキュリティおよび開発のための STIG の最新バージョン 5.3 に対する WebInspect チェックの相関関係が含まれています。

ポリシーの更新

DISA STIG 5.3

DISA STIG 5.3 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。

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。

Insecure Transport: SSLv3/TLS 再ネゴシエーション ストリーム

TLS 1.3 は再ネゴシエーションをサポートしていません。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、再ネゴシエーション時におけるストリーム インジェクションのチェックが改善されています。

HTML5: Cross-Site Scripting Protection

X-XSS-Protection ヘッダーは、すべての最新ブラウザーで廃止されました。このリリースでは、欠落している、または誤って設定された X-XSS-Protection ヘッダーのチェックが廃止されました。

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。

DISA STIG 5.3 および OWASP Mobile 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、DISA STIG 5.3 および OWASP Mobile Top 10 2023 をサポートする OpenText™ 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 Customer Support 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