Fortify ソフトウェア セキュリティ コンテンツ

2024 年更新版 1
2024 年 3 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 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 1,654 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 2024.1.0)、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 1,429 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 Angular のサポート (サポートされているバージョン: 16.0.0)

Angular は、SPA (シングル ページ アプリケーション) の作成に特化した、Typescript ベースの無償のオープン ソース Web アプリケーション開発フレームワークであり、データを動的かつ効率的に操作するために主にフロントエンドで使用されます。Angular のサポート対象はバージョン 11.2.4 から 16.0.0 (初期サポートのみ) まで拡大されました。Angular の結果が強化され、*Cross-Site Request Forgery*、*Privacy Violation*、*System Information Leak* などのカテゴリでより良い結果が期待できるようになりました。JavaScript DOM ドキュメントと次のモジュールの対象範囲が拡大されました。

- @angular/common/http
- @angular/core
- @angular/platform-browser

改善された PHP のサポート (サポートされているバージョン: 8.2)

PHP は広く使用されている汎用スクリプト言語であり、Web 開発に最もよく使用されます。最新の SSR リリースでは、PHP のサポートがバージョン 8.2 までを対象とするように更新されました。特に、このリリースには、次の追加の PHP ベース拡張機能の初期サポートが含まれています。

- Sodium (サポートされているバージョン: 8.3.1)

  PHP Sodium 拡張機能は、Libsodium ライブラリの実装です。Sodium は、暗号化、復号化、署名、パスワード ハッシュ、およびその他の暗号化操作の機能を提供します。お客様は、Privacy Violation の問題に関する変更や、暗号化とデジタル署名に関連する追加の問題に気付く可能性があります。

- Zip (サポートされているバージョン: 1.22.3)

  PHP Zip 拡張機能は、Libzip ライブラリの実装です。Zip は、ファイル/データのグループ化と圧縮を実現するために使用される一般的な構造である zip アーカイブの作成、変更、および読み取り機能を提供します。拡張機能の初期サポートには、基本的なファイルシステム データフローに固有の ZipArchive クラスの対象範囲と、次のカテゴリの PHP 対象範囲の拡張が含まれます。

  - Key Management: Empty PBE Password
  - Path Manipulation: Zip Entry Overwrite

改善された Golang のサポート (サポートされているバージョン: 1.21)[1]

Go (Golang とも呼ばれる) は、Google で作成されたコンパイル型の静的型付けプログラミング言語です。シンプルさ、効率性、並行処理の強力なサポートで知られており、スケーラブルな Web サービス、データ パイプライン、分散システムの構築に最適です。Go は、コンパイル言語のパフォーマンス上の利点と、インタープリタ言語に見られるプログラミングの容易さを兼ね備えています。簡潔な構文と強力な標準ライブラリによって、開発者は堅牢なコードをすばやく記述できます。以下のパッケージの適用範囲が拡大されています。

- context
- crypto/ecdh
- html/template
- net
- reflect
- Runtime
- time

Cloud Infrastructure as Code (IaC)[2]

Cloud Infrastructure as Code のサポートが拡張されました。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。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。Fortify Static Code Analyzer 24.2 では、Azure ARM および AWS CloudFormation の構成の問題が新しい手法を使用して報告されます。この結果、Fortify Static Code Analyzer の以前のバージョンで生成された FPR をマージするときに、一連の問題が追加および削除されることになります。Fortify Static Code Analyzer 24.2 以降では、重複する IaC の問題を防ぐために 2024.1 ルールパックが必要です。

Azure Resource Manager (ARM) 構成

ARM は、Azure の展開および管理サービスです。ARM は、Azure アカウントでリソースを作成、更新、および削除するための管理レイヤーを提供します。

Amazon Web Services (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。これらのテンプレートを利用することで、ユーザーはスタックと呼ばれるリソースのコレクションを単一のユニットとして作成、削除、および変更できます。このリリースでは、AWS CloudFormation 構成について次の追加の脆弱性カテゴリを報告しています。

- AWS CloudFormation Misconfiguration: Insecure SageMaker Transport
- AWS CloudFormation Misconfiguration: SageMaker Network Isolation Disabled
- AWS CloudFormation Misconfiguration: Weak SecretsManager Generated Password

[1] 最適な結果を得るには、Fortify Static Code Analyzer 24.2 以降にアップグレードしてください。
[2] Fortify Static Code Analyzer 24.2 以降が必要です。

改善された Kotlin のサポート (サポートされているバージョン: 1.9.2)[3]

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、Kotlin 名前空間を対象とした Kotlin バージョン 1.7.2、1.8、および 1.9 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: *jvm.optional*、*math*、*io.path*、*coroutines.cancellation*、および *kotlinx.serialization.json*。既存のカテゴリで、次のような追加の問題が検出される可能性があります。

- Denial of Service: Regular Expression
- Path Manipulation
- Privacy Violation
- System Information Leak

JavaScript/TypeScript Node.js の改善点[4]

Fortify Static Code Analyzer 24.2 を使用するときに型解決のメリットが得られるように、Node.js ルールが更新されました。この変更により、ほとんどのカテゴリで Node.js アプリケーションで誤検知が減り、正検知が改善され、検出結果の精度が向上します。具体的には、お客様は次の Node.js モジュールに関連する結果の改善を期待できます。

- child_process
- dgram
- dns
- fs
- http
- https
- net
- querystring
- tls
- url
- util
- v8

次の NPM パッケージの部分的な初期サポートも含まれています。

- Bluebird
- child-process-promise

改善された DISA STIG 5.3 のサポート

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 が更新され、次の 45 種類の追加 STIG ID が含まれるようになりました: APSC-DV-000010、APSC-DV-000210、APSC-DV-000230、APSC-DV-000240、APSC-DV-000330、APSC-DV-000380、APSC-DV-000390、APSC- DV-000400、APSC-DV-000410、APSC-DV-000430、APSC-DV-000450、APSC-DV-

[3] Kotlin 1.9 のサポートには、Fortify Static Code Analyzer 24.2 以降が必要です。

[4] Fortify Static Code Analyzer 24.2 以降が必要です。

000580、APSC-DV- 000590、APSC-DV-000710、APSC-DV-001120、APSC-DV-001130、APSC-DV-001280、APSC-DV-001290、APSC-DV-001300、APSC-DV-001310、APSC-DV-001320、APSC-DV-001330、APSC-DV-001410、APSC-DV-001520、APSC-DV-001530、APSC-DV-001540、APSC-DV-001610、APSC-DV-001760、APSC-DV-001770、APSC-DV-001780、APSC-DV-001790、APSC-DV-001795、APSC-DV-001820、APSC-DV-001970、APSC-DV-002290、APSC-DV-002310、APSC-DV-002320、APSC-DV-002410、APSC-DV-002530、APSC-DV-002890、APSC-DV-002950、APSC-DV-002960、APSC-DV-003100、APSC-DV-003310、および APSC-DV-003320。

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。

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。

- *Access Control: Anonymous LDAP Bind* – C/C++ アプリケーションで誤検知を排除
- *Command Injection* – C ランタイム ライブラリ関数の Windows バリアントを使用する C/C++ アプリケーションで新しい問題を検出
- *Credential Management: Hardcoded API Credentials* – YAML ファイルで誤検知を排除
- *Dockerfile Misconfiguration: Dependency Confusion* – npm に関連する Dockerfile で誤検知を排除
- *Dynamic Code Evaluation: Code Injection* – Azure Cosmos DB API を使用する ASP.NET アプリケーションで新しい問題を検出
- *GCP Terraform Misconfiguration: Insecure Supply Chain* – AWS Terraform 構成ファイルで誤検知を排除
- *Insecure SSL: Server Identity Verification Disabled* – `Requests` ライブラリを使用する Python アプリケーションで新しい問題を検出
- *Mass Assignment: Insecure Binder Configuration* – ASP.NET MVC アプリケーションで誤検知を排除
- *Mass Assignment: Request Parameters Bound into Persisted Objects* – Spring アプリケーションから誤検知を排除
- *Password Management: Hardcoded Password* – ODBC 接続文字列で新しい問題を検出
- *Poor Style: Identifier Contains Dollar Symbol ($)* – Java アプリケーションで誤検知を排除
- *Privacy Violation* – Razor Pages を使用する ASP.NET アプリケーションで新しい問題を検出
- *Privacy Violation* – Dart/Flutter アプリケーションで新しい問題を検出
- *Privacy Violation* – ExpressJS ライブラリとともに `csurf` ミドルウェアを使用する JavaScript アプリケーションで新しい問題を検出
- *String Termination Error* – C/C++ アプリケーションで新しい問題を検出
- *System Information Leak: External* – Razor Pages を使用する ASP.NET アプリケーションで新しい問題を検出
- *System Information Leak: External* – C/C++ アプリケーションで新しい問題を検出

- *Weak Encryption: Inadequate RSA Padding* - OpenSSL を使用する PHP アプリケーションで誤検知を排除
- Python Django アプリケーションでさまざまなデータフロー誤検知を排除
- Java Spring アプリケーションでさまざまな新しいデータフローの問題を検出
- Java スキャンの main() エントリ ポイントから発生するさまざまなデータフローの問題が、新規および排除済みとして表示される場合があります。これにより、Kotlin および Scala アプリケーションで見つかった重複や不正確なトレースも排除されます。

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 4 件のカテゴリの名前を変更しました。

2023 R4 カテゴリ名	2024 R1 カテゴリ名
Insecure Cross-Origin Opener Policy	HTML5: Insecure Cross-Origin Opener Policy
Insecure Transport: Client Identity Verification Disabled	Insecure SSL: Server Identity Verification Disabled
Kubernetes Terraform Misconfiguration: Improper Daemon Set Access Control	Kubernetes Terraform Misconfiguration: Improper DaemonSet Access Control
Kubernetes Terraform Misconfiguration: Improper Stateful Set Access Control	Kubernetes Terraform Misconfiguration: Improper StatefulSet Access Control

"Header Checking Disabled" カテゴリの廃止

名前の類似した他のカテゴリとの混乱を避けるために、このカテゴリは削除されました。このカテゴリの以前のルールは、次のように報告されるようになりました。

- ASP.NET Misconfiguration: Header Checking Disabled
- ASP.NET Misconfiguration: Unsafe Header Parsing

特定の "Dead Code" カテゴリの廃止

次の "Dead Code" カテゴリは標準のルールパックから削除されました。

- Dead Code: Empty Try Block
- Dead Code: Expression is Always false
- Dead Code: Expression is Always true
- Dead Code: Unused Field
- Dead Code: Unused Method
- Dead Code: Unused Parameter

これらの脆弱性の検出を継続したいお客様は、Fortify Support Portal から個別のルールパックでルールをダウンロードできます。

OWASP Mobile Top 10 2023 の名前変更と廃止

2023 年 9 月に「OWASP Top 10 Mobile Risks - Initial Release 2023」がリリースされた後、プロジェクトは完了し、2024 年 1 月に「OWASP Top 10 Mobile Risks - Final Release 2024」に名前が変更されました。その結果、このリリースには、「OWASP Mobile Top 10 Risks 2024」の追加および名前変更されたマッピングが含まれています。マッピング自体には機能的な変更はありません。

Fortify Software Security Content の次のリリースでは、OWASP Mobile Top 10 2023 マッピングは廃止され、更新された OWASP Mobile Top 10 2024 のみが残ります。

Fortify SecureBase [Fortify WebInspect]

SmartUpdate を使用してすぐに入手できる以下の更新を実行すると、Fortify SecureBase で、お客様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 (CVE-2024-23897)

Jenkins は、ソフトウェアの構築、テスト、および展開に使用される Java ベースの自動化サーバーです。Jenkins コマンド ライン インターフェイス (CLI) は、Jenkins サーバーと対話する方法を提供する Jenkins の組み込み機能であり、デフォルトで有効になっています。CVE-2024-23897 で特定された重大なファイル読み取り脆弱性により、Jenkins で任意のファイル読み取り機能が可能になります。この脆弱性は、CLI に提供されるコマンド引数とオプションを解析するために使用される args4j ライブラリに存在します。コマンド パーサーには、引数内のアットマーク (@) 文字とそれに続くファイル パスを、指定されたファイルのコンテンツに置き換える機能があります。影響を受ける Jenkins のバージョンには、2.441 以前と LTS 2.426.2 以前が含まれます。このリリースには、対象のサーバー上で CVE-2024-23897 を検出するためのチェックが含まれています。

Insecure Deployment: Unpatched Application (CVE-2023-22515)

Atlassian Confluence Data Center と Confluence Server は、コラボレーションのベスト プラクティスを組織に提供することで知られる自己管理型ソリューションです。CVE-2023-22515 で特定された重大なアクセス制御破損の脆弱性により、悪意のある行為者が不正な管理者アカウントを作成し、Confluence プラットフォームへの無制限のアクセスを許可できるようになります。攻撃者は認証がない場合でも、CVE-2023-22515 を利用して不正な管理者アカウントを作成し、Confluence インスタンスにアクセスすることができます。攻撃者は、Confluence Server の設定を操作して、セットアップ プロセスが完了していないように見せかけることもできます。影響を受ける Confluence Server および Confluence Data Center のバージョンは、8.0.0 から 8.0.4、8.1.0 から 8.1.4、8.2.0 から 8.2.3、8.3.0 から 8.3.2、8.4.0 から 8.4.2、および 8.5.0 から 8.5.1 です。このリリースには、対象のサーバー上で CVE-2023-22515 を検出するためのチェックが含まれています。

Insecure Deployment: Unpatched Application (CVE-2023-22518)

CVE-2023-22518 で特定された重大な不適切な認証の脆弱性は、Atlassian Confluence Data Center および Confluence Server に影響を及ぼします。この脆弱性により、認証されていない攻撃者が Confluence をリセットし、Confluence インスタンス管理者アカウントを作成できるようになります。このアカウントを使用すると、攻撃者は Confluence インスタンス管理者が実行可能なすべての管理アクションを実行できるため、機密性、整合性、可用性が完全に失われる可能性があります。影響を受ける Confluence Server および Confluence Data Center のバージョンは、7.19.16 より前のすべてのバージョンと、バージョン 8.3.4、8.4.4、8.5.3、および 8.6.1 です。このリリースには、対象のサーバー上で CVE-2023-22518 を検出するためのチェックが含まれています。

OGNL Expression Injection: Double Evaluation (CVE-2023-22527)

CVE-2023-22527 で特定された重大な脆弱性である OGNL Expression Injection は、Atlassian Confluence Server および Data Center に影響を与えます。この脆弱性により、認証を受けていない攻撃者が、脆弱なアプリケーションで任意のコードを実行する可能性があります。影響を受ける Confluence Data Center および Confluence Server のバージョンは、8.0.x、8.1.x、8.2.x、8.3.x、8.4.x、および 8.5.0 から 8.5.3 です。このリリースには、影響を受ける Atlassian 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。

コンプライアンス レポート

改善された 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 が更新され、次の 8 種類の追加 STIG ID が含まれるようになりました: APSC-DV-000210、APSC-DV-000230、APSC-DV-000240、APSC-DV-000450、APSC-DV-001280、APSC-DV-001300、APSC-DV-002530、および APSC-DV-003320。

ポリシーの更新

改善された DISA STIG 5.3

DISA STIG 5.3 ポリシーが更新され、DISA STIG 5.3 に関連する追加のチェックが含まれるようになりました。

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。

XPath インジェクション

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、*XPath インジェクション* チェックが改善されています。

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。

OWASP Mobile Top 10 2024

名前が変更された OWASP Mobile Top 10 Risks 2024 相関関係に伴い、このリリースには、Fortify Customer Support Portal の Premium Content からダウンロード可能な OWASP Mobile Top 10 2024 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