Micro Focus

Fortify Software Security Content

2020 年第 3 四半期のアップデート

2020 年 9 月 25 日

Micro Focus 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、Micro Focus Fortify Software Security Content は、27 のプログラミング言語における 1,032 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。

詳細: https://software.microfocus.com/en-us/software/security-research

Fortify Software Security Research (SSR) は、Fortify Secure Coding Rulepacks (英語、バージョン 2020.2.0)、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。

Micro Focus Fortify Secure Coding Rulepacks [SCA]

このリリースにより、Fortify Secure Coding Rulepacks は 27 のプログラミング言語で脆弱性に関する 815 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 System.Text.Json サポート (バージョン 3.1)[1]

System.Text.Json 名前空間は、Newtonsoft の Json.NET パッケージに代わる、高速で組み込みの標準準拠の代替手段を提供します。System.Text.Json 名前空間は、UTF-8 としてエンコードされた JSON テキストを読み書きするためのタイプも提供します。このサポートには、各種シリアル化または逆シリアル化方法によるデータフローと、次のカテゴリの適用範囲の拡大が含まれます。

- Cross-Site Scripting: Reflected
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Privacy Violation
- System Information Leak: External
- System Information Leak: Internal

Kotlin コルーチンと標準ライブラリのサポート [2]

コルーチンのサポートを含む、Kotlin 標準ライブラリの適用範囲が拡張されました。コルーチンは、同時および非同期コードを開発するための高機能で柔軟な API を提供します。この更新により、コルーチンを使用するアプリケーションのデータフロー分析が改善されます。

Kotlin Java の相互運用性と Android の機能強化 [3]

Java と Kotlin の両方のソースコードを含むプロジェクト、および Kotlin を使用して開発された Android アプリケーションの既存の脆弱性カテゴリ全体での言語サポートが機能強化されます。

Java 14 機能強化 [4]

Java 14 までのバージョンの変更をサポートするための、既存の脆弱性カテゴリ全体が機能強化されます。

ECMAScript バージョンの更新 [5]

ECMAScript バージョンのルール適用範囲がアップグレードされ、ECMAScript 2020 までのすべてのバージョンがサポートされるようになりました。

---

[1] System.Text.Json 名前空間の設計のため、Newtonsoft Json.NET パッケージで報告されているのと同じ JSON Injection の問題に対して脆弱ではありません。
[2] 選択式を使用する API などの実験的なコルーチン API は、この更新ではサポートされていません。
[3] SCA 20.2 以降が必要です。
[4] SCA 20.2 以降が必要です。
[5] 完全なサポートには SCA 20.2 以降が必要です。

Go Logrus (バージョン 1.6.0)

Logrus は Go の構造化ロガーであり、標準ライブラリ ロガーと完全な API 互換性があります。Logrus はエンタープライズ アプリケーションにログ記録関連のリスクをもたらす可能性がある一般的なログ記録パッケージです。サポートされるカテゴリは次のとおりです。

- Poor Logging Practice: Use of a System Output Stream
- Privacy Violation
- System Information Leak

Dockerfile のサポート [6]

Docker を使用すると、サンドボックス環境 (コンテナーとも呼ばれる) でのパッケージ化コードとその依存関係を任意のコンピューティング環境で実行できます。Dockerfile は、コンテナーイメージの構成です。この更新は、Dockerfile の最も一般的な脆弱性を扱います。
初期サポートは、既存の「パスワード管理: 構成ファイル内のパスワード」カテゴリおよび次の新しいカテゴリを適用範囲とします。

- Dockerfile の誤った構成: デフォルトのユーザー権限
- Dockerfile の誤った構成: 権限を持つコンテナー
- Dockerfile の誤った構成: 権限を持つポート
- Dockerfile の誤った構成: 機密性の高いホスト検出
- Dockerfile の誤った構成: SSH サービス

DISA STIG 4.11

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目的で、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 4.11 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。

17.x より前の SCA バージョンでのサポート廃止に関する通知:
これは、17.x より前の SCA 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になることをお知らせします。次のリリースでは、17.x より前のバージョンの SCA 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、SCA 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、SCA 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。

廃止されたマッピング - セキュリティ技術実装ガイド バージョン 3.x (STIG 3.x):
Software Security Research チームは、Fortify カテゴリから外部標準およびベスト プラクティスへのマッピングを長年にわたって作成し続けてきました。そのように、多くの古いバージョンは使用されないにもかかわらず、現在、サポートされているさまざまな標準のバージョンが非常に大きくなっています。
そのため、externalmetadata.xml ファイル内で新しい XML 属性を使用して、バージョン 4.0 より前のバージョンの STIG を廃止としてマークしました。この変更は、バージョン 20.2 以降の Fortify Software Security Center および SCA アプリケーションでは、これらの古いバージョン

[6] SCA 20.2 以降が必要です。

がデフォルトで表示されなくなることを意味します。これらの古いバージョンを確認する必要がある場合、この回避策は、マッピングを変更して廃止を「false」に設定するか、属性を完全に削除することです。

「ブラックリスト」と「ホワイトリスト」に代わる用語:
この分野の傾向に従い、Micro Focus Fortify の一部である Software Security Research チームは、総括して「ブラックリスト」および「ホワイトリスト」という用語を使わず、より中立的で意味を明確にする用語に移行することを決定しました。代わりに、より説明的な用語である「拒否リスト」と「許可リスト」をそれぞれ使用することにしました。
この変更は、次のカテゴリ名が変更されたことを意味し、削除または新しい問題が発生する可能性があります。

- 「逆シリアル化の好ましくない習慣: ブラックリスト」は「逆シリアル化の好ましくない習慣: 拒否リスト」
- 「Django バッド プラクティス: ブラックリストされた属性」は「Django バッド プラクティス: 拒否リストの属性」
- 「Setting Manipulation: 「ユーザー管理のホワイトリスト」は「Setting Manipulation: ユーザー制御の許可リスト」

Weak Encryption: 安全性の低い操作モードに関する更新情報
現在では、対称暗号化の暗号ブロック連鎖 (CBC) モードを使用することは安全ではないと考えています。このリリース以降、CBC の使用はすべて現在サポートされているライブラリの「Weak Encryption: 安全性の低い操作モード」として報告されます。BEAST、POODLE、Zombie POODLE、GOLDENDOODLE、LUCKY13 および Padding Oracle 攻撃を考慮し、現在知られている暗号化の調査に基づいて、CBC は安全ではなくなったと判断しました。

誤検知の改善：
私たちはお客様の声に耳を傾け、誤検知率の改善に努めています。このリリースでは、誤検知の数を減らすために次のことに取り組んでいます。

- Cross-Site Request Forgery
  他の種類の CSRF トークン、および ASP.NET の非表示フィールド内を考慮した削減
- Server-Side Request Forgery
  一部の Spring アプリケーション内での削除
- Poor Logging Practice: Use of a System Output Stream
  コンテキストがコマンドライン アプリケーションまたはユーティリティに基づいている場合は削除されました。
- デッド コード: 未使用フィールド
  内部 lambda
- Privacy Violation
  Java、Scala、および Kotlin lambda 内のパスワードに関連する重複する問題を削除
- Java システム プロパティは、組み込みプロパティに対して個別に処理されるようになり、多くの場合、誤検知が減少し、新しい System Information Leak が見つかる可能性があります。

プレビュー: [7]
誤検出率を減らすために、Null 間接参照と冗長 Null チェックのルールが作り直されました。特に、内部 Null チェック機能を処理するカスタム ルールを作成する機能が追加されました。
ただし、このメリットが本質的に普遍的であるかどうかは不明です。そのため、SCA 20.2 で利用可能なこれらの機能強化は、デフォルトでオフになっています。これらの機能強化をテストしたい場合は、カスタマー サポートにお問い合わせください。

[7] SCA 20.2 以降が必要です。

Micro Focus 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

Weak Cryptographic Signature: ユーザー管理のキー ソース

主要な混乱攻撃は、JSON Web Tokens (JWT) の整合性を脅かします。クライアントから受信したトークンを検証するためにキー ソースを慎重に選択しない JWT 実装の場合、攻撃者がトークン ペイロードを偽造することを許してしまい、このような実装は攻撃に対して脆弱です。このリリースには、主要な混乱攻撃に対する JWT の使用を評価するためのチェックが含まれています。

JSON Web Token: 保護クレームがない

「jti」、「exp」、「aud」などの保護クレームを実装していない JSON Web Token は、なりすまし攻撃やリプレイ攻撃の影響を受けやすい可能性があります。このリリースには、スキャン中に検出されたトークンにこれらのクレームがないかどうかを検出する複数のチェックが含まれています。

Access Control: Authorization Bypass

JSON Web Token (JWT) は、これにに含まれる情報を HMAC または RSA アルゴリズムのいずれかでデジタル署名することで、データの改ざんに対する保護を提供します。署名の検証に失敗したアプリケーションは、不正アクセスやなりすまし攻撃の影響を受けやすい可能性があります。このリリースには、欠落した任意の署名攻撃に対して JWT 実装を評価するための複数のチェックが含まれています。

OAuth2: 不十分な状態パラメータ エントロピー

十分なエントロピーを持つ「state」パラメーター値を使用しない OAuth2 プロトコルの実装は、なりすまし攻撃の影響を受けやすくなります。このリリースには、状態パラメーターが十分なエントロピー要件を満たしていないかどうかを評価するためのチェックが含まれています。

OAuth2: 不十分な更新トークンの取り消し

新しいアクセス トークンを再発行する前に、クライアント ID、クライアント シークレット、および更新トークンの有効期限を確認しない認証サーバーは、なりすまし攻撃に対して脆弱である可能性があります。このリリースには、更新トークンを使用して、クライアント ID とクライアント シークレットなしで複数のアクセス トークンを生成でき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。

OAuth2: 不十分な認証コードの有効期限

適時に認証コードの有効期限が失効しない OAuth2 認証サーバーは、盗まれた認証コードに対して新しい有効なアクセス トークンを付与し続ける可能性があるため、なりすまし攻撃を受けやすい可能性があります。このリリースには、この認証コードの悪用を検出するためのチェックが含まれています。

Cross-Site Request Forgery

OAuth2 認証フローで「state」パラメーターの使用に失敗したアプリケーションは、クライアントになりすます認証を受けない操作の影響を受けやすくなります。さらに、JSON Web Tokens (JWT) に Cookie ストレージを使用するアプリケーションは、同様の CSRF 攻撃のリスクにさらされています。これらのリリースには、CSRF に対して脆弱である JWT インスタンスおよび OAuth2 インスタンスを検出する複数のチェックが含まれています。

Weak Cryptographic Signature: Insufficient Key Size

JSON Web Token には、ペイロードの整合性を証明するためにデジタル署名された情報が含まれています。 シークレットが脆弱な HS256 などの対称アルゴリズムは、Brute-Force 攻撃を受ける可能性があり、攻撃者は任意のペイロードを生成し、有効なキーで署名することが可能になります。このリリースには、HS256 などの脆弱なアルゴリズムがトークンの署名に使用されてい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。

SQL Injection[8]

SQLite は、個別のサーバー プロセスを必要とせず、SQL クエリ言語の非標準バリアントを使用してデータベースにアクセスできる軽量のディスクベースのデータベースを提供する C ライブラリです。このリリースには、SQLite ライブラリ バージョン 3.16.0 以降を使用する Web アプリケーション内での SQL Injection の脆弱性を検出するための WebInspect SQL Injection チェックの機能拡張が含まれています。

コンプライアンス レポート

DISA STIG 4.11

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目的で、このリリースには米国国防情報システム局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 4.11 に対応した WebInspect チェックが含まれています。

ポリシーの更新

DISA STIG 4.11

DISA STIG 4.11 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 WebInspect SecureBase の既存のポリシー リストに追加されました。

Web API

API セキュリティ評価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 WebInspect SecureBase の既存のポリシー 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。

Insecure Transport: 弱い SSL 暗号:
ID 11285 で識別されるチェックは、SSLv3 または TLS1.0 が CBC 暗号とともに検出された場合に、脆弱な SSL プロトコルでコンテンツ広告を報告するのと比較して、CBC モード暗号のすべてのインスタンスを脆弱であるとして報告するように変更されました。POODLE、GoldenPOODLE、ZombieDOODLE などの脆弱性を考慮し、トランスポート層のセキュリティには CBC モードの暗号は推奨されなくなりました。

[8] レポート コンテンツの一部として SQLite のデータベースの種類情報を含めるには、WebInspect 20.2 以降が必要です。

「ブラックリスト」と「ホワイトリスト」に代わる用語:
この分野の傾向に従い、Micro Focus Fortify の一部である Software Security Research チームは、総括して「ブラックリスト」および「ホワイトリスト」という用語を使わず、より中立的で意味を明確にする用語に移行することを決定しました。代わりに、セキュリティ コンテンツのチェックで、より説明的な用語である「拒否リスト」と「許可リスト」をそれぞれ使用することにしました。

Micro Focus 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 4.11

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 4.11 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。

Micro Focus 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/ja 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、Micro Focus Fortify Support Portal で見つかる場合があります。

Contact Fortify 技術サポート
Micro Focus Fortify
https://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

SSR へのお問い合わせ
Alexander M. Hoole
Software Security Research マネージャー
Micro Focus Fortify
hoole@microfocus.com
+1 (650) 258-5916

2020 年 9 月 25 日