Micro Focus

Fortify Software Security Content

2020 年更新版 4

2020 年 12 月 18 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 1,039 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/software/security-research

Fortify Software Security Research (SSR) は、Fortify Secure Coding Rulepacks (英語、バージョン 2020.4.0)、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。

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 817 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。

Dapper サポート (バージョン 2.0.78)

Dapper オブジェクト リレーショナル マッピング (ORM) のサポート。Dapper は、.NET IDdbConnection インターフェイスを拡張して、ネイティブ クエリ出力を厳密に型指定された C# オブジェクトにマッピングするために使用されます。新規サポートでは、Dapper をユーザー管理のデータのソースとして扱うほか、次のようなカテゴリのトリガーとしても扱います。

- Access Control: Database
- SQL Injection

Kotlin 標準ライブラリの更新 (バージョン 1.3)

Kotlin 標準ライブラリのサポートが拡張され、次のパッケージがカバーされるようになりました。

- kotlin.concurrent
- kotlin.jvm
- kotlin.reflect
- kotlin.system

XML Pull (バージョン 1)

Android での XML Pull パッケージの実装のサポート。XML Pull は、アプリケーションで解析を制御する場合に (中断と再開が可能)、XML ファイルを解析してシリアライズするためのシンプルなストリーミング API です。サポートされるカテゴリは次のとおりです。

- XML Entity Expansion Injection
- XML Injection (XML インジェクション)

AIOPG (バージョン 1.0.0)[1]

Python aiopg ライブラリのサポート。aiopg は、PostgreSQL データベースに非同期で接続する手段です。サポートされるカテゴリは次のとおりです。

- Access Control: Database
- Password Management

[1] aiopg に関連する問題が完全に検出されるかは、「async with」に関連する SCA の今後の改善で決まります。

- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- SQL Injection

JavaScript Promise

- JavaScript Promise のデータフロー分析のサポートが改善されました。

Azure Resource Management テンプレート

Azure Resource Management (ARM) テンプレートの初期サポート。ARM テンプレートは、Azure ソリューションのコードとしてのインフラストラクチャを実装するために使用されます。ARM テンプレートは、宣言型の構文を利用してユーザーのプロジェクトを定義および設定する JSON ファイルです。サポートされるカテゴリは次のとおりです。

- Azure Resource Manager Misconfiguration: HTTPS Not Required
- Azure Resource Manager Misconfiguration: Public Access Allowed

DISA STIG 5.1

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 5.1 に対応した Micro Focus Fortify Taxonomy が追加されました。

NIST SP 800-53 Rev. 5

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、最新バージョンの National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 に記載されているセキュリティ管理策とプライバシー管理策に対応した Micro Focus Fortify Taxonomy が追加されました。次の管理策群に及ぶ 30 の基本管理策がカバーされています。

- アクセス制御 (AC)
- 監査および責任追跡性 (AU)
- 評価、認可、および監視 (CA)
- 構成管理 (CM)
- 識別および認証 (IA)
- PII 処理および透明性 (PT)
- システム保護および通信の保護 (SC)
- システムおよび情報の整合性 (SI)

2020 Common Weakness Enumeration (CWE™) Top 25

2019 年に、SANS Top 25 に代わる Common Weakness Enumeration (CWE™) Top 25 が導入されました。8 月にリリースされた 2020 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、Micro Focus Fortify Taxonomy と 2020 CWE Top 25 との相関関係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 バージョンのサポート廃止

2020.3 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、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でした。このリリースでは、17.x より前のバージョンの SCA は最新のルールパックをロードしません。17.x より前のバージョンの SCA を使用しているお客様は、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を行う必要があります。

今後のリリースでは、SCA の最新の 4 つのメジャー リリースをサポートします。

マッピングの廃止

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くなるにもかかわらず、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、次の標準を廃止としてマークしました。

- ペイメント カード業界データ セキュリティ基準 (PCI) 1.1
- ペイメント カード業界データ セキュリティ基準 (PCI) 1.2
- ペイメント カード業界データ セキュリティ基準 (PCI) 2.0
- ペイメント カード業界データ セキュリティ基準 (PCI) 3.0
- ペイメント カード業界データ セキュリティ基準 (PCI) 3.1
- ペイメント カード業界データ セキュリティ基準 (PCI) 3.2
- セキュリティ技術実装ガイド (STIG) 4.1
- セキュリティ技術実装ガイド (STIG) 4.2
- セキュリティ技術実装ガイド (STIG) 4.3
- セキュリティ技術実装ガイド (STIG) 4.4

- セキュリティ技術実装ガイド (STIG) 4.5
- セキュリティ技術実装ガイド (STIG) 4.6
- セキュリティ技術実装ガイド (STIG) 4.7
- セキュリティ技術実装ガイド (STIG) 4.8

この変更は、バージョン 20.2 以降の Fortify SCA アプリケーションでは、これらの古いマッピング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への準拠を確認する必要がある場合は、マッピングを変更して *obsolete* 属性を「false」に設定するか、この属性を完全に削除する必要があります。

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。

- 構成ファイルに保護が適用されている場合の HTTP Verb Tampering の誤検知を取り除きました。
- .NET で JSONIGNORE 属性を使用している場合の Mass Assignment の誤検知を取り除きました。
- URLSessionConfiguration オブジェクトでキャッシュが明示的に無効になっている場合の Insecure Storage: HTTP Response Cache Leak の誤検知を取り除きました。
- Swift Privacy Violation: Http Get の誤検知を URLRequest から取り除きました。
- Poor Logging Practice: Use of a System Output Stream の重複が Python で取り除かれました。
- 追加の Apache Commons closeQuietly バリアントを使用する場合にリソースが解放されない問題が取り除かれました。

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: Predictable Secret Key

JSON Web Token のペイロードの整合性は、多くの場合、HMAC シグネチャを使用して確保されます。ただし、HMAC アルゴリズムで脆弱なシークレットが使用されている場合は、悪意のあるユーザーが Brute-Force 攻撃で秘密鍵を入手し、任意のペイロードを含む JWT に再署名する可能性があります。このリリースには、よく使用されるシークレットの文字列が JWT トークンの署名に使用されているかどうかを特定するためのチェックが含まれています。

Password Management: 弱いパスワード ポリシー

安全な Web サイトを展開するためには、ユーザーが強力なパスワードを作成するためのパスワード ポリシーが重要です。パスワードを検証して、よく使用されるパスワードのいずれかと一致しないことや、パスワードの文字列が NIST 800-53、NIST 800118、および OWASP によって定められたガイドラインを満たすことを確認する必要があります。このリリースには、ログイン マクロで設定されたパスワードがよく使用されるパスワードのいずれかと一致するかどうかを検出するための新しいチェックが含まれています。また、このリリースには、前述の NIST 標準や OWASP ガイドラインで定められているパスワード強度に関する改訂版ガイドラインを満たすための脆弱なパスワード ポリシー チェックの更新も含まれています。

Cache Management: Web Cache Poisoning

Web キャッシュには、ユーザーが Web サイトに初めてアクセスしたときにページのコピーが保存されます。次にユーザーが同じページにアクセスしたときには、キャッシュされたコピーが提供されます。ただし、このような Web キャッシュにリクエスト本文を含む GET リクエストを受け入れるなどの実装または設計上の欠陥がある場合は (ファット GET リクエストやキーのない入力など)、Web キャッシュ ポイズニング攻撃を受けやすくなります。Web キャッシュ ポイズニングは、攻撃者が正当なユーザーのリクエストに対して悪意のある応答をキャッシュするために使用する高度な手法です。このリリースには、Web サイトがキーのないヘッダーやファット GET リクエストを介した Web キャッシュ ポイズニングに対して脆弱であるかどうかを特定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

DISA STIG 5.1

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 5.1 に対応した WebInspect チェックが含まれています。

NIST SP 800-53 Rev. 5

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、このリリースには最新バージョンの National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 に記載されている管理策に対応した WebInspect チェックが含まれています。

2020 Common Weakness Enumeration (CWE™) Top 25

2019 年に、SANS Top 25 に代わる Common Weakness Enumeration (CWE™) Top 25 が導入されました。8 月にリリースされた 2020 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。今回の Securebase の更新には、これらの CWE カテゴリへのマッピングが含まれています。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を含めています。

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。

- HTTP Request Smuggling チェックが再設計され、誤検出の削減、効率の向上、その結果の精度改善を実現しています。チェック ID 11621 で、脆弱性の検証に時間ベースのアプローチが使用されなくなりました。

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 5.1、NIST SP 800-53 Rev. 5、および 2020 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 DISA STIG 5.1、NIST SP 800-53 Rev. 5、および 2020 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。

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 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 12 月 18 日