Micro Focus

Fortify Software Security Content

2019 年第 1 四半期のアップデート

2019 年 3 月 29 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、25 のプログラミング言語における 999 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。

詳細については以下を参照してください。

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 2019.1.0)、Fortify WebInspect SecureBase (SmartUpdate で利用可能)、Fortify Application Defender、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 25 のプログラミング言語で脆弱性に関する 796 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。

Angular 7[1]

7.0.0 までのバージョンを含む Angular のサポートでは、ブラウザーからの入力ソースが識別され、デフォルトで Angular によって実行されるセキュリティ検証をモデリングします。Angular テンプレートは、Cross-Site Scripting: DOM、Privacy Violation、Dynamic Code Evaluation の問題などのカテゴリを見つける機能を含め、すべての正規の JavaScript シンクが Angular プロジェクトでサポートされるようにモデリングされています。

AWS Lambda 関数のサポート

新しい Amazon Web Services (AWS) Lambda 関数は Java および Python 言語をサポートします。 この機能により、Lambda が API ゲートウェイに接続されているときに発生する可能性のある XSS の問題を含め、Lambda トリガー イベントから Lambda 関数ロジックへのデータフローが可能になります。

AWS Java SDK v2

S3 および DynamoDB サービス用の AWS Java SDK v2 の新しいサポート。 新しくサポートされるカテゴリ：

- Access Control: ACL Manipulation
- Insecure Storage: S3 Full Anonymous Access
- Insecure Storage: S3 Read ACP Anonymous Access
- Insecure Storage: S3 Read Anonymous Access
- Insecure Storage: S3 Write Anonymous Access
- Insecure Storage: S3 Write ACP Anonymous Access
- NoSQL Injection: DynamoDB

Python Django[1]

2.1.7 までのバージョンのサポートを含む、Python Django Web Framework のサポートの更新。変更には、クラスベースのビューと関連するデータフローのサポートの改善および Django 1.8 以降に導入された Django 関数/メソッドのサポートが含まれます。

[1] Angular 7、Django、および Wicket のサポートには、最適な結果を得るために Fortify SCA バージョン 19.1.0 以降が必要です。

Apache Wicket[1]

フレームワークのバージョン 6、7、および 8 のサポートを含む、Apache Wicket Web Framework のサポートの改善。

DISA STIG 4.9

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

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

Often Misused: File Upload

Blueimp の jQuery File Upload ウィジェットには CVE-2018-9206 で特定されたリモート コード実行に対する脆弱性があることが判明しました。 この脆弱性は、攻撃者に任意の PHP ファイルをアップロードして実行する機会を与えます。 このリリースには、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。

SQL Injection

このリリースには、Microsoft Azure SQL Database を使用するアプリケーションをサポートするための SQL インジェクション チェックの拡張機能が含まれています。

Sensitive Information Leak:External

このリリースには、Magento CMS が開発者モードで実行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。 開発者モードは、開発またはテスト環境での使用を目的としています。 実稼働環境で開発者モードを有効にすると、重要なアプリケーションとシステム データが潜在的な攻撃者に露出され、セキュリティ上のリスクが生じる可能性があります。

Cross-Frame Scripting

Content Security Policy の *frame-ancestors* ディレクティブ ヘッダーは、Cross-Frame Scripting の脆弱性に対するポリシー保護を提供します。 現在使用されている X-Frame-Options HTTP ヘッダーは廃止されます。 このリリースでは既存の Cross-Frame

Scripting チェックが強化され、Content Security Policy の frame-ancestors ディレクティブのサポートが含まれています。

Content Management System (CMS) Fingerprinting

このリリースには、WebInspect スキャン中にターゲット サーバー上で次のいずれかの CMS の存在をフィンガープリントによってチェックするための機能強化が含まれています: WordPress、Drupal、Django、Joomla、Liferay、Magento、Sitecore、Sitefinity[2]、Umbraco。 検出結果を報告するために情報チェックがトリガーされます。

コンプライアンス レポート

DISA STIG 4.9

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 4.9 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 4.9

DISA STIG 4.9 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。

Micro Focus Fortify Application Defender

Fortify Application Defender は、自社開発製アプリケーションまたはサードパーティ製アプリケーションのリスクを組織が管理し、軽減できるようにする RASP (runtime application self-protection) ソリューションです。ソリューションは、アプリケーションの使用と悪用を一元的に視覚化し、ソフトウェアの脆弱性の利用およびその他の違反からリアルタイムで保護します。このリリースでは、Micro Focus Fortify Software Security Research チームにより次のような機能強化が提供されます。

OGNL Expression Injection:Struts 2

Apache Struts 2 での OGNL Expression Injection 検出のサポートを拡張しました。これには、CVE-2018-11776 で特定されている重大な Struts の脆弱性がカバーされています。 Apache Struts2 バージョン 2.3.x から 2.3.34 まで、またはバージョン 2.5.x から 2.5.16 までを使用するアプリケーションでは、ネームスペースなしで、またはワイルドカード ネームスペースを使用して設定されたアクション結果が OGNL 式に含まれていて、struts.mapper.alwaysSelectFullNamespace プロパティが Struts 設定で true に設定されている場合、攻撃者はその OGNL 式を任意に実行できます。

[2] Sitefinity の検出には WebInspect 19.1.0 以降が必要です。

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 4.9[3]

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 4.9 をサポートする Fortify SSC 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。

[3] DISA STIG 4.9 レポートのサポートには Fortify SSC バージョン 18.20 以降が必要です。

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

2019 年 3 月 29 日