Micro Focus

Fortify ソフトウェア セキュリティ コンテンツ

2021 年第 1 四半期のアップデート

2021 年 3 月 26 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 ソフトウェア セキュリティ コンテンツは、27 のプログラミング言語における 1,038 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 2021.1.0)、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。

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 816 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。

Micro Focus Visual COBOL のサポート (バージョン 6)[1]

このリリースでは、Micro Focus Visual COBOL バージョン 6 のサポートが追加されました。特に、このリリースには、Micro Focus COBOL Runtime System (RTS) のサポートと、既に COBOL でサポートされている Path Manipulation カテゴリと以下の追加のカテゴリの拡張サポートが含まれています。

- Command Injection
- Memory Leak
- Memory Leak: Reallocation
- Unreleased Resource
- Unreleased Resource: Synchronization

Android 11

最新バージョンの Android (API バージョン 30) をサポートするための継続的な取り組みの一環として、以下の名前空間が対象となっています。

- android.accounts
- android.app
- android.database
- android.database.sqlite

追加の *SQL Injection* および *Access Control: Database* 検出とともに全般的に結果を改善する、Android アプリケーションの優れたモデリングが実現されます。

iOS の更新

iOS のサポートを改善するための継続的な取り組みの一環として、以下のクラスに新しい Swift ルールが追加されました。

- Foundation.NSCache
- Foundation.URLFileProtection

データ保護と Privacy Violation に関連した結果の改善と、その他の脆弱性タイプやフレームワークの全般的な改善が行われています (「その他の正誤情報 - iOS のバグ修正」を参照)。

[1] SCA 21.1 以降が必要です。

Angular サポートの更新 (バージョン 11.2.3)

このリリースで、Angular のサポートが 11.2.3 になります。特に、ブラウザーからの、ユーザー管理の情報の新しいソースが特定されました。これにより、以前は行われなかった多くのカテゴリがトリガーできるようになります。

Apache Commons の更新

Apache Commons は、再利用可能な Java コンポーネントを提供します。このリリースで、SSR は以下のコンポーネントのサポートを更新しました。

- beanutils (1.9.4)
- collections4 (4.4)
- dbutils (1.7)
- fileupload (1.4)
- lang (3.11)
- math (3.6.1)
- io (2.8.0)
- text (1.9)

これらの更新により、これらのコンポーネントを使用したアプリケーションのモデリングが改善されます。また、以下の脆弱性タイプが現れる可能性のある新しい場所を特定するとともに、Log Forging や JSON Injection などのカテゴリに対する保護が特定されます。

- Access Control: Database
- Denial of Service
- Insecure Randomness: User-Controlled Seed
- Path Manipulation
- Privacy Violation
- Setting Manipulation
- SQL Injection
- System Information Leak (バリアント)

Python (バージョン 3.9)

Python の最新バージョンのサポートが更新され、コア言語 API のモデリングが改善されました。

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。

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。

- *Code Correctness:* Java および Kotlin アプリケーションにおける*誤ったクラスの比較*
- *Dynamic Code Evaluation:* Python 3 スキャンにおける*コードインジェクション*の問題が取り除かれました。
- *キー管理*の問題が改善され、全言語にわたって誤検知が取り除かれました。
- *Cross-Site Scripting:* jQuery に関連した *DOM* の問題が、入力ボックスからの場合は *Cross-Site Scripting: Self* として正しくカテゴライズされるようになりました。

- パスワードとして利用できないコンテンツを照合する場合の、構成ファイルにおける *Password Management* の問題が取り除かれました。
- ローカライズ データに対して照合する場合の、*Password Management* の誤検知が改善されました。
- Java Spring アプリケーションで無関係な機能に対する *XML External Entity Injections* の検出が取り除かれました。
- *ASP.NET MVC Bad Practices: Controller Not Restricted to POST* で、追加の動詞 (PATCH、DELETE、PUT) を安全なものとして扱えるようになりました。

iOS のバグ修正:
分析に対する改善のため、ルールの更新が必要でした。これにより、以下の脆弱性タイプにおける改善がみられる場合があります。
- Input Interception: Keyboard Extensions Allowed
- Privacy Violation: HTTP Get
- Privacy Violation: Keyboard Caching
- Privacy Violation: Screen Caching
- Privacy Violation: Shoulder Surfing

以下のいくつかのフレームワークでも、精度を高める軽微な更新が行われました:
Foundation、UIKit、WebKit、HealthKit、WatchKit、MessageUI、CoreLocation、CoreData。

削除されたカテゴリ:
結果の関連性を高めるために、以下のカテゴリはこのリリースで削除されました。
- Privilege Management: Android Network

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

OGNL Expression Injection: Struts 2

CVE-2019-0231 と CVE-2020-17530 で特定されている OGNL Expression Language Injection の重大な脆弱性は、Struts バージョン 2.0 から 2.5.25 に影響します。これらの脆弱性の悪用は、サーバー上での任意のリモート コードの実行につながる可能性があります。このリリースには、Struts 2 を使用する Web アプリケーションでこれらの脆弱性を検出するためのチェックが含まれています。

WAF の検出 [2]

このリリースには、チェック「WAF の検出」が含まれています。これは、スキャン中に Web アプリケーション ファイアウォールが検出された場合に、情報検出結果にフラグを立てます。これらの検出結果は、スキャン リクエストがアプリケーションに到達する前にブロックされたため、スキャン品質が危険にさらされている可能性があることを示しています。

ハッカー レベルの洞察 [2]

ハッカー レベルの洞察は、開発者とセキュリティの専門家に、アプリケーションの全体的なセキュリティの姿勢に関するコンテキストを提供します。このリリースには、スキャン中にアプリケーションで検出されたライブラリにフラグを立てるチェックが含まれています。これらの検出結果が必ずしもセキュリティ上の脆弱性を表しているとは限りませんが、攻撃者は通常、既知の脆弱性やパターンを特定しようとして、これらのタイプのターゲットの偵察を行うことに注意する必要があります。

ポリシーの更新

NIST SP 800-53 Rev. 5

NIST SP 800-53 Rev. 5 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。

CWE Top 25 2020

CWE Top 25 2020 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。

DISA STIG 5.1

DISA STIG 5.1 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。

Web Cache Poisoning
このリリースには、*Web Cache Poisoning: Unkeyed Headers* の更新済みチェックが含まれています。キャッシュキーの一部であると疑わせるカスタム ヘッダーを追加できるようになりました。

安全でない Spring Boot アクチュエーター

[2] WebInspect 21.1 以降が必要です。

このリリースには、権限のないユーザーでも利用可能な機密性の高い Spring Boot アクチュエーターを検出するための更新済みのチェックが含まれています。これにより、より高い精度の結果が得られます。

XSS の改善
このリリースには、Vue 3 および Angular JS 1.5.9 以降用の、改善された XSS 攻撃チェックが含まれています。

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。

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

2021 年 3 月 26 日