Micro Focus

Fortify Software Security Content

2020 年第 1 四半期のアップデート

2020 年 3 月 27 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、26 のプログラミング言語における 1,019 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 2020.1.0)、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 26 のプログラミング言語で脆弱性に関する 810 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。

Go 言語標準ライブラリ サポート [1]

Go 標準ライブラリのサポートが拡張されました。Go は Google が設計したオープンソースの静的型付け言語であり、その目的はシンプルで信頼性が高く効率的なソフトウェアを構築しやすくすることです。Go は構文的には C 言語と似ていますが、メモリ安全性メカニズム、ガベージ コレクション、構造的型付けという特徴を持ちます。今回の更新でカバーするのは、標準ライブラリ名前空間と、次の 19 の追加カテゴリを含む 53 の脆弱性のタイプです。

- Denial of Service:Regular Expression
- Formula Injection
- Insecure Randomness
- JSON Injection (JSON インジェクション)
- Key Management:空の HMAC キー
- Key Management:ハードコードされた HMAC キー
- Log Forging
- Log Forging (debug)
- Resource Injection
- Weak Cryptographic Hash
- Weak Cryptographic Hash:Hardcoded Salt
- Weak Cryptographic Hash:User-Controlled Salt
- Weak Cryptographic Signature:Insufficient Key Size
- Weak Cryptographic Signature:User-Controlled Key Size
- Weak Encryption:Inadequate RSA Padding
- Weak Encryption:Insecure Initialization Vector
- Weak Encryption:Stream Cipher
- Weak Encryption:User-Controlled Key Size
- XML Injection (XML インジェクション)

[1] 最適なスキャン結果が得られるように SCA v20.1.0 以降を推奨します。

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。

- JavaScript では、セルフ XSS としてより細かく識別されていた「Cross-Site Scripting: DOM」のインスタンスが新しいサブカテゴリ「Cross-Site Scripting: Self」に変更され、低優先度でフラグ付けされました。
- Java では、モデリング エンジンの機能強化が原因で、特に if 条件のまわりでデッド コードの誤検出の数が意図せず増加していました。このルールが改善され、無効な問題の数がかなり削減されました。
- JSP および Spring MVC アプリケーションに関してまれに起こっていたパフォーマンスの問題が解消されました。
- 外部メタデータを更新し、Common Weakness Enumeration (CWE™) と Micro Focus Fortify: Software Security Errors Taxonomy (7 Pernicious Kingdoms とも呼ばれる) との相関関係を改善しました。改善点には、Software Security Errors Taxonomy の 935 のカテゴリにわたる 41 の追加 CWE-ID の調整が含まれ、その結果、CWE マッピングと CWE Top 25 2019 マッピングの両方の更新があります。必然的に、関連するすべてのレポート作成機能と CWE による「Group By」フィルタリングが影響を受けます。追加 CWE ID には次のものが含まれます。

  CWE-88、CWE-97、CWE-119、CWE-147、CWE-192、CWE-203、CWE-212、CWE-266、CWE-267、CWE-276、CWE-279、CWE-280、CWE-346、CWE-347、CWE-436、CWE-506、CWE-527、CWE-529、CWE-530、CWE-531、CWE-536、CWE-540、CWE-541、CWE-548、CWE-550、CWE-705、CWE-775、CWE-799、CWE-917、CWE-921、CWE-923、CWE-925、CWE-926、CWE-937、CWE-942、CWE-1004、CWE-1021、CWE-1069、CWE-1173、CWE-1188、CWE-1236

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

危険なファイルの取り込み: ローカル

Tomcat に影響を及ぼす深刻な脆弱性は、AJP プロトコル機能を使用してサーバー側ファイルにアクセスします。これを悪用すると、攻撃者が Apache Tomcat Web アプリディレクトリにあるファイルを読み取ったり、ファイルを入れたりすることができるようになります。この脆弱性は GhostCat と呼ばれており、CVE-2020-1938 で特定されています。また、任意のコードの実行攻撃が可能になります。この問題は、Apache Tomcat 9.x (9.0.31 より前)、8.x (8.5.51 より前)、7.x (7.0.100 より前)、およびそれ以前のすべてのバージョンに影響します。今回の Securebase の更新には、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。

Common Weakness Enumeration (CWE™) マッピング:

Common Weakness Enumeration (CWE™) はソフトウェアの脆弱性につながるおそれがあるソフトウェア エラーの分類体系です。この分類体系は、SDLC のさまざまな段階でソフトウェアのリスクと脆弱性の評価に関する各種の方法論の成果を統合して整理する方法を提供します。このリリースの Securebase には、チェックと CWE の最新情報との更新されたマッピングが含まれています。CWE は、階層的な分類体系です。チェックは、チェックの目的と一致する最も近いリーフ ノードにマッピングされます。

コンプライアンス レポート

Common Weakness Enumeration (CWE™) Top 25:

Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Errors (CWE Top 25) は、MITRE が作成しているリストです。このリストは、ソフトウェアの脆弱性につながるおそれがある最も一般的な 25 のソフトウェア脆弱性カテゴリを示しています。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ました。

ポリシーの更新

Common Weakness Enumeration (CWE™)

Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Errors (CWE Top 25) は、MITRE が作成しているリストです。このリストは、ソフトウェアの脆弱性につながるおそれがある最も一般的な 25 のソフトウェア脆弱性カテゴリを示しています。今回のリリースでは、CWE Top 25 にマッピングされた脆弱性を評価するチェックのリストを含んだポリシーを含めました。

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。

- HTTP Request Smuggling チェックのバグ修正により、チェック ID 11621 での検出結果に関係する誤検出が少なくなります。このチェックは HTTP 405 をこの脆弱性の有効な検証とは見なさなくなりました。
- Insecure Transport:Weak SSL Cipher レポート コンテンツに、構成文字列に !SHA246 および !SHA384 を含めることによって CBC モード暗号を除外する例を含めました。ただし、サーバー管理者に連絡して、強力な暗号スイートの選択をホワイトリストに入れた構成を作成してもらうことをおすすめします。

- Insecure Transport のその他の修正:Weak SSL Cipher 検出の追加の修正を実施し、サーバーが TLS1.2 と強い暗号のみをサポートしている場合にチェックで正しい暗号を検出できなかったケースでの構成の検出を改善しました。

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。

OWASP Application Security Verification Standard (ASVS):

Application Security Verification Standard (ASVS) は、アプリケーションのセキュリティ要件と、ソフトウェア開発ライフサイクル (SDLC) の間と構成時に安全なソフトウェアを作成するために実行するテストのリストです。この標準の該当する要件に対して、チェックのマッピングと SCA ルールを作成しました。しかし、当社製品との相関関係の作成プロセスにおいて、この標準によって提供されている CWE マッピングを Securebase のチェックと SCA ルールにさらに正確に合わせるために改善できることが判明しました。当社はこれらの改善に取り組み、評価とコラボレーションに関心をお持ちのお客様がこれらのアーティファクトを利用できるようにしています。ご関心があれば、以下の SSR の連絡先にお問い合わせいただき、WebInspect のコンプライアンス テンプレートとポリシー、SSC シード バンドルをお取り寄せください。

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 3 月 27 日