Micro Focus

Fortify Software Security Content

2019 年第 2 四半期のアップデート

2019 年 6 月 28 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 1,005 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 2019.2.0)、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 799 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 の更新

.NET Framework バージョン 4.7.1 および 4.7.2 で導入された追加の API のサポート。更新には、.NET Framework と同じカテゴリをカバーする .NET Standard 2.0 および .NET Core 2.0 のルールのサポートが含まれます。.NET Framework の更新バージョンのルールには、次のカテゴリに対するサポート強化が含まれています。

- Header Manipulation:Cookies
- Insecure SSL:Server Identity Verification Disabled
- Insecure Transport:Weak SSL Protocol
- Weak Cryptographic Hash
- Weak Cryptographic Signature:Insufficient Key Size
- Weak Encryption

Realm データベース

モバイル アプリケーション専用に設計されたオープン ソースの軽量データベースである Realm データベースは、Android (Java) の他に iOS (Swift および Objective-C) でもサポートされるようになりました。サポートされるカテゴリは次のとおりです。

- Access Control:Database
- Key Management:Empty Encryption Key
- Key Management:Hardcoded Encryption Key
- Key Management:Null Encryption Key
- Path Manipulation

さらに、2 つの新しいカテゴリがサポートされています。

- Insecure Storage:Missing Database Encryption
- NoSQL Injection:Realm

Python urllib3

一般的に使用されている強力な HTTP クライアントである Python urllib3 ライブラリがサポートされるようになりました。カテゴリの適用範囲には、以下が含まれます。

- Header Manipulation
- Insecure SSL:Server Identity Verification Disabled
- Password Management
- Password Management:Empty Password
- Password Management:Hardcoded Password
- Password Management:Null Password
- Password Management:Weak Cryptography
- Server-Side Request Forgery

Java SE 10 および 11 更新版

Java SE の適用範囲は、新しい HTTP クライアント API のサポートを含め、バージョン 10 および 11 に拡張されました。

Cross-Site Scripting: SOP Bypass

JavaScript および TypeScript 内で新しいカテゴリ「Cross-Site Scripting: SOP Bypass」をサポート。この新しいカテゴリは、脆弱性により攻撃者が Same-Origin Policy (SOP) を回避してクロスサイト スクリプティング攻撃を可能にする特定の状況に対応します。

PCI SSF 1.0

コンプライアンス分野の e コマースおよび金融サービスの顧客をサポートするために、このリリースでは Micro Focus Fortify Taxonomy カテゴリと、新しい Software Security Framework (SSF)、バージョン 1.0 の一部として Payment Card Industry (PCI) の Secure Software Standard (SSS) で定義された、新しい「Secure Software Requirements and Assessment Procedures」に規定されている制御目標の相関関係をサポートしています。この新しい規格は、2020 年中旬に終了する新しい Payment Application (PA) DSS 申請と 2022 年に期限切れとなる既存の PA-DSS での変更により、最終的に PCI Data Security Standard (DSS) を置き換える予定です。

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、リソースの消費を継続しました。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:

ログの偽造

ログの偽造およびログの偽造 (デバッグ) の問題を防ぐために新しい行を削除する API をより正確に認識することで、すべての言語で誤検出が減少します。

リリースされないリソース:データベース

Java では、ResultSet を作成した Statement が最初にクローズされた場合、ResultSet が自動的にクローズされることをアルゴリズムが正しく識別していませんでした。関連する誤検出がなくなりました。

安全でない JNI と安全でない JSNI

SCA v19.1.x にアップグレードした顧客は、Java アプリケーションで新たな「安全でない JNI」と「安全でない JSNI」の問題の急増を経験した可能性があります。これはエンジンの改善によるものです。これは、多くの API で、顧客が修正を管理できないことを示すフラグが立てられていたことを意味します。これが修正され、SCA はユーザーがソースを制御している API にのみフラグを立てるようになりました。この問題の減少により、顧客は「Access Control: SecurityManager Bypass」の問題が減少したことに気づくかもしれません。

Lambda の動的コード評価とその他のシンク

JavaScript アプリケーションでは、Lambda の呼び出しで問題が発生した場合に混乱を招く結果が生じる可能性がありました。その一般的な例は setTimeout() です。これらの無関係な問題は現在取り除かれています。また、これらの問題が今後も発生するケースについては、発生の頻度を減らすために積極的に取り組んでいます。問題の減少は、SCA v18.20 以降を使用している場合にのみ確認できます。

Cross-Site Scripting: Content Sniffing のサポート

以前は、SCA は、レスポンスの content-type によってブラウザが HTML/JS コンテンツ (application/json など) を処理できなかった場合に Cross-Site Scripting の問題を報告していました。その理由は、Web アプリケーションのユーザーが content-sniffing 攻撃を可能にする古いブラウザを使用している可能性があったためです。今回のリリースでは、これらの問題が「Cross-Site Scripting: Content Sniffing」として報告されるように修正しました。これにより、監査担当者や開発者はすぐにそれらの問題を認識し、より深刻な Cross-Site Scripting のケースとは別に判断することができます。Java Rulepack の Spring フレームワークと JAX-RS の両方がこの新しいカテゴリをサポートしています。

感染に基づく Fortify Priority Order の低下

以前は、SCA は、HTTP リクエスト パラメータから発生した SQL Injection を、システム環境変数から発生したのと同じ重大度で報告していました。攻撃者がシステム変数を制御する可能性は非常に低いか、少なくともリクエスト パラメータを制御する可能性よりも低いと考えられます。特定のシナリオでは、これに基づいてすでに問題の Fortify Priority Order の値を下げていましたが、今回のリリース以降、SCA は問題の Fortify Priority Order の値を計算するときに感染の要因を新しい要素としてより一貫した方法で適用します。

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

WebSocket の更新[1]

このリリースには、WebSocket トラフィックにおける情報のリークおよび安全でないシリアライズ解除 (.NET の場合) の脆弱性を検出するための機能強化が含まれています。特に、次のカテゴリが WebSocket をサポートするように機能強化されました。

- Dynamic Code Evaluation:Unsafe Deserialization

[1] WebSocket Update には WebInspect 19.1.0 以降が必要です。

- Poor Error Handling:Unhandled Exception
- Privacy Violation
- Privacy Violation:Credit Card Number
- Privacy Violation:National ID Disclosure
- Privacy Violation:Social Security Number
- System Information Leak:Internal IP

セキュア応答ヘッダーの構成の更新

サーバーは、一連の HTTP 応答ヘッダーを使用してアプリケーションのセキュリティを強化するブラウザ構成を提供できます。これらのヘッダーは詳細な防御メカニズムと見なされ、設定されると脆弱性を適切に防ぐことができます。このリリースでは、以下のヘッダーおよび関連するカテゴリのサポートが強化されています。

- Cache-Control
  - Cache Management:Insecure Policy
- Content-Security-Policy
  - HTML5: Missing Content Security Policy
  - HTML5: Deprecated Content Security Policy
  - HTML5: Misconfigured Content Security Policy
- X-Content-Type-Options
  - Web Server Misconfiguration:Insecure Content-Type
- X-XSS-Protection
  - HTML5: Cross-Site Scripting Protection

Web Server Misconfiguration:Deprecated SSL/TLS Certificate

2017 年 12 月 1 日以前にシマンテック認証局によって発行されたすべての SSL/TLS 証明書 (Thawte、VeriSign、Equifax、GeoTrust、RapidSSL などのシマンテック所有のブランドを含む) は信頼できなくなり、Chrome、Internet Explorer、Firefox、および Safari を含むすべての主要ブラウザで使用できなくなりました。このリリースには、廃止予定のシマンテック証明書の使用にフラグを立てるためのチェックが含まれています。

Insecure Deployment:Unpatched Application

CVE-2019-6340 によって特定される Drupal コンテンツ管理システム (CMS) における重大なリモート コード実行の脆弱性により、リモートの攻撃者はサーバー上で任意のコードを実行できます。このリリースには、Drupal CMS を展開するアプリケーションで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。

コンプライアンス レポート

PCI SSF 1.0

コンプライアンス分野の e コマースおよび金融サービスの顧客をサポートするために、このリリースには Micro Focus Fortify Taxonomy カテゴリを、新しい Software Security Framework (SSF)、バージョン 1.0 の一部として Payment Card Industry (PCI) の Secure Software Standard (SSS) で定義された、新しい「Secure Software Requirements and Assessment Procedures」に規定されている制御目標に相関付ける新しいコンプライアンス テンプレートが含まれています。この新しい規格は、2020 年

中旬に終了する新しい Payment Application (PA) DSS 申請と 2022 年に期限切れとなる既存の PA-DSS での変更により、最終的に PCI Data Security Standard (DSS) を置き換える予定です。

ポリシーの更新

PCI SSF 1.0

PCI SSF 1.0 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

Cache Management:Insecure Policy

機能拡張により ID 11306 のチェックが行われ、手動検証で誤検出として最も頻繁に監査されていた特定の content-type の HTML 応答のフラグを除外するようになりました。

Expression Language Injection:Spring

SecureBase チェック ID 11579 の脆弱性検出アルゴリズムの精度が改善されました。

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。

PCI SSF 1.0

新しい相関関係に伴い、このリリースには、Fortify Customer の Premium Content からダウンロード可能な PCI SSF 1.0 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。

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 6 月 28 日