Micro Focus

Fortify Software Security Content

2018 年第 4 四半期のアップデート

2018 年 12 月 14 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 992 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 2018.4.0)、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 789 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。

SQLite および iOS の機能強化

Swift、Objective-C、C、および C++ に対する SQLite API のサポートが拡張されました。 拡張の適用範囲は 16 の既存の脆弱性カテゴリに及び、これには SQL Injection、Access Control : Database、およびパスワードとキー管理の両方に関連する問題が含まれます。 いかなるタイプのデータベースとのインタラクションにおいても、コーディングの弱点が存在すれば機密情報のリーク、意図しない変更、さらにはデータの損失につながる可能性があります。 そのため、Privacy Violation (Heap Inspection for Swift) を対象としたプライバシーに関連する iOS の機能強化が追加されました。

Akka HTTP

Scala Akka HTTP モジュールのサポート。これは、Akka Streams に基づく Reactive Streams 準拠のツールキットで、サーバー側とクライアント側の完全な HTTP スタックを実装します。脆弱性カテゴリの適用範囲には、既存の 22 の弱点のタイプが含まれます。

JAX-RS の機能強化

JAX-RS の最新バージョンとそのリファレンス実装である Jersey のサポートを修正しました。2.1 で追加された新機能のサポートに加え、この Rulepack にはクライアントサイド API のサポートも含まれます。 影響を受ける脆弱性のカテゴリには、Privacy Violation、Server-Side Request Forgery、および System Information Leak が含まれます。 さらに、Cross-Site Scripting の特殊なサブカテゴリに新しい脆弱性カテゴリが追加されました。この脆弱性は、応答が XSS セーフのコンテンツ タイプを使用して送信された場合に発生します。 この場合、特定のブラウザが「コンテンツ スニッフィング」を行い、応答内でスクリプトを実行する可能性があるため、「Cross-Site Scripting: Content Sniffing」の問題をレポートします。

Python six

Python ライブラリ six のサポート。 six は、Python 2 と 3 の両方と互換性のあるコードベースを変更なしでサポートすることを目的とした Python 互換性ライブラリです。 サポートされる脆弱性カテゴリは次のとおりです。

- Command Injection
- Dynamic Code Evaluation: Unsafe Pickle Deserialization
- Privacy Violation
- Server-Side Request Forgery
- System Information Leak:External
- Unsafe Reflection

DISA STIG 4.8

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

PCI DSS 3.2.1

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 Security Fortify Taxonomy カテゴリと最新バージョンの Payment Card Industry Data Security Standard バージョン 3.2.1 で指定された要件の相関関係をサポートしています。

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

LDAP Injection

LDAP Injection は、ユーザー入力に基づいて LDAP ステートメントを作成する Web ベースのアプリケーションを利用するために使用される攻撃です。 アプリケーションがユーザー入力を正しくサニタイズできなかった場合、SQL Injection と同様の方法で LDAP ステートメントを変更することが可能です。 LDAP Injection 攻撃により、認証を受けずに機密データにアクセスできる場合があります。 このリリースには、Web アプリケーションの LDAP Injection の脆弱性を特定するチェックが含まれています。

Open Redirect

Open Redirect の脆弱性により、攻撃者は既知のサイトにおけるユーザーの信頼を簡単に利用することができます。 ベンダー アドバイザリー SA-CORE-2018-006 によると、Drupal 7 および 8 にはこの弱点に対する脆弱性があります。

Drupal Destination Parameter Anonymous Open Redirect

Drupal 8 では、「ターゲット」パラメータ値の不適切なサニタイズが利用され、攻撃者が制御する悪意のある URL への Open Redirect が引き起こされる可能性があります。 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。

Drupal Path Alias Open Redirect

Drupal 7 および Drupal 8 では、Path Module の脆弱性により攻撃者はパスの別名を作成、編集、および管理することができ、攻撃者が制御する悪意のある URL への Open Redirect が引き起こされる可能性があります。

Access Control: Authorization Bypass

JSON Web Token (JWT) は、2 者間でデータを転送するための URL セーフな方法を構築するための標準です。 トークン内の情報は、HMAC または RSA アルゴリズムを使用してデジタル署名されています。 ただし、この標準では、JWT のハッシュ アルゴリズムで「none」を選択できます。 「none」でエンコードされた JWT を受け入れたサーバーは、データの保全性について検証を行うことなくすべての JWT が有効であると見なします。 悪意のあるユーザーはこれを利用して任意のデータをサーバーに送信することができます。 その結果、システム データとユーザー データの両方が認証なしでア

クセスされ、危険にさらされる可能性があります。 このリリースには、JWT アルゴリズム「none」の認証バイパスの脆弱性を検出するためのチェックが含まれています。

Privacy Violation

JSON Web Token (JWT) は、2 者間でデータを転送するために使用されます。 適切に暗号化されていないと、機密データが認証を受けないユーザーに公開される可能性があります。 このリリースには、クレジット カード番号の開示、社会保障番号の開示、および HTML 5 クライアントサイド ストレージの機密情報の保存の検出に関連するプライバシー違反を検出する既存のチェックに対する更新が含まれています。

Dynamic Code Evaluation:Code Injection

Pivotal の Spring Framework には CVE-2018-1270 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。 この脆弱性により、攻撃者は WebSocket エンドポイントを介して悪意のあるメッセージを公開された STOMP に送信することができ、その結果リモート コードが実行される可能性があります。 このリリースには、Spring Framework 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。 チェックには WebSocket ポリシーを介してアクセスできます。

WebSocket Discovered

このリリースには、スキャンされたアプリケーションに WebSocket が存在することを示すための情報チェックが含まれています。 さらにこのチェックは、WebSocket の脆弱性に関連するすべてのチェックを含む新しい WebSocket ポリシーを使用してアプリケーションをスキャンするよう顧客に促す役割も果たします。

コンプライアンス レポート

DISA STIG 4.8

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 4.8 に対応した WebInspect チェックが含まれています。

PCI DSS 3.2.1

このリリースには、最新バージョンの Payment Card Industry Data Security Standard (DSS) コンプライアンス テンプレート、バージョン 3.2.1 が含まれています。

ポリシーの更新

DISA STIG 4.8

DISA STIG 4.8 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。

WebSocket

新しい WebSocket ポリシーは、WebSocket 関連の脆弱性に対するアプリケーションのセキュリティ評価を実行します。

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。

DISA STIG 4.8[1]

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 4.8 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。

PCI DSS 3.2.1[1]

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 DSS 3.2.1 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。

[1] DISA STIG 4.8 および PCI DSS 3.2.1 レポートのサポートを受けるには、Fortify SSC バージョン 18.20 以上が必要です。

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

2018 年 12 月 14 日