Micro Focus

Fortify Software Security Content

2019 年第 4 四半期のアップデート

2019 年 12 月 13 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に基づいて 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提供することです。現在、Micro Focus Fortify Software Security Content は、26 のプログラミング言語における 1,018 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 2019.4.0)、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 807 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 Initial Support[1]

Go の初期サポートです。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 は構文上は C に類似していますが、メモリ安全性メカニズム、ガベージ コレクション、構造的型に対応します。今回の更新でカバーするのは、10 のコア標準ライブラリ名前空間と、次の 34 カテゴリのサポートです。

- Access Control: Database
- Command Injection
- Connection String Parameter Pollution
- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set
- Cookie Security: Overly Broad Domain
- Cookie Security: Overly Broad Path
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- File Permission Manipulation
- Header Manipulation
- Header Manipulation: Cookies
- HTML5: MIME Sniffing
- Insecure Transport
- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key
- Open Redirect
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Path Manipulation
- Path Manipulation: Zip Entry Overwrite
- Privacy Violation
- Server-Side Request Forgery

[1] SCA v19.2.0 以降が必要。

- Setting Manipulation
- SQL Injection
- System Information Leak: External
- System Information Leak: Internal
- Weak Encryption
- Weak Encryption: Insufficient Key Size

Spring Security

Spring Security は認証とアクセス コントロールのフレームワークです。セキュリティの層 (セキュリティ ヘッダーなど) も追加することで、セッション フィクセーション、クリックジャッキング、クロスサイト リクエスト フォージェリといった攻撃からも保護します。Spring ベースのアプリケーションのセキュリティを保護するためのデファクト スタンダードです。今回の更新により、バージョン 5.2.1 までは次の 21 カテゴリがサポートされます。

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: Overly Broad Domain
- Cross-Site Request Forgery
- Header Manipulation
- HTML5: Cross-Site Scripting Protection
- HTML5: MIME Sniffing
- HTML5: Missing Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- HTML5: Overly Permissive CORS Policy
- HTML5: Overly Permissive Referrer-Policy
- Insecure Transport: HSTS Does Not Include Subdomains
- Insecure Transport: HSTS not Set
- Insecure Transport: Insufficient HSTS Expiration Time
- Password Management
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- Password Management: Weak Cryptography
- Privacy Violation
- Session Fixation
- System Information Leak

加えて、次の 7 つの弱点のタイプが新たに導入されました。

- HTML5: Missing Framing Protection
- HTML5: Unenforced Content Security Policy
- Spring Security Misconfiguration: Default Permit
- Spring Security Misconfiguration: Disabled Security Headers
- Spring Security Misconfiguration: Incorrect Request Matcher Type
- Spring Security Misconfiguration: Lack of Fallback Check
- Spring Security Misconfiguration: Overly Permissive Firewall Policy

Spring Boot

Spring Boot はスタンドアロンの Spring アプリケーションを構築し、可能な場合は Spring とサードパーティのライブラリを自動構成します。メトリック、健全性チェック、構成外部化といった実働可能な機能も提供します。以前からサポートされているカテゴリに加えて、今回の更新により、バージョン 2.2.1 までは次の 9 カテゴリがサポートされます。

- Cookie Security: HTTPOnly not Set on Session Cookie
- Cookie Security: Overly Broad Session Cookie Domain

- Cookie Security: Overly Broad Session Cookie Path
- Cookie Security: Persistent Session Cookie
- Cookie Security: Session Cookie not Sent Over SSL
- Password Management: Empty Password in Configuration File
- Insecure Transport
- Insecure Transport: Server Identity Verification Disabled
- System Information Leak: External

また、以前の Rulepack では Properties 構成ファイルと Maven 構築システムのみをサポートしていましたが、今回のリリースには YAML 構成ファイルと Gradle のサポートも含まれています。

Java 12[2]

Java 12 の新しい API のサポートです。そのルールには、新しい Java 12 構文 (新しい Switch ステートメントなど) が使用される場合、SCA バージョン 19.1 以降が必要です。

JSTL XML Library

JavaServer Pages (JSP) Standard Tag Library (JSTL) は JSP を中心として XML ドキュメントを操作し作成する方法を提供するライブラリです。JSTL v1.1 の次のカテゴリがサポートの適用範囲になりました。

- XSLT Injection
- XML External Entity Injection
- Privacy Violation
- System Information Leak: External

OpenXML SDK .NET の機能強化

OpenXML SDK v2.9.0 のサポートが更新され、次の 3 つのカテゴリのサポートが追加されました。

- Access Control: Database
- Connection String Parameter Pollution
- SQL Injection

React Router のサポート

React Router はナビゲーション用コンポーネントのコレクションであり、アプリケーションを宣言型の構成にします。必要とするものが、Web アプリケーションでブックマーク可能な URL であっても、あるいは React でナビゲートするための構成可能な方法であっても、React Router は React がレンダリング中であれば機能します。React Router 5.1.2 では次のカテゴリがサポートされます。

- Open Redirect
- Privacy Violation
- System Information Leak: External

2019 CWE Top 25

Common Weakness Enumeration (CWE) Top 25 は、SANS Top 25 と呼ばれていた頃と比較すると、判定のされ方が根本的に変更されています。9 月にリリースされた新しい Top 25 はヒュ

[2] SCA v19.2.0 以降が必要。

ーリスティック式を使用して判定され、過去 2 年間にわたって National Vulnerability Database (NVD) へ報告された脆弱性の頻度と重大度を正常化します。NVD で最も一般的に報告される重大な脆弱性の周辺を監査することを優先する顧客をサポートするため、Micro Focus Fortify Taxonomy と CWE Top 25、2019 バージョンとの相関関係が追加されています。

DISA STIG 4.10

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

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、リソースの消費を継続しました。顧客は、次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。

- 安全でないデシリアライズの一貫性:以前は、一部のルールでは情報がブラウザからのものである場合のみフラグを付けていました。現在は、他に可能性のあるシナリオでフラグを付けるよう対応されています。
- 説明のリファレンスを検証: リファレンスされた資料の中には、古くなっているものや無効なリンクを指すものがありました。こうしたインスタンスが修正されており、適切なリファレンスが配置されています。

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

SSO Bad Practices: Authentication Token Replay

認証トークンがシングル サインオン プロセス中に交換されると、再生攻撃を受けやすくなり、攻撃者が有効なユーザーになりすまして認証なしでサービスへアクセスすることが可能になります。今回のリリースには、Windows Identity Framework と SAML プロトコルを使用するサービス プロバイダに対して再生攻撃を実行するチェックが含まれています。

Cache Management: Headers

HTTP Vary 応答ヘッダーには、正しくキャッシュされた応答であるかを判断して着信要求に対応するのに使用される HTTP ヘッダーのリストが含まれます。 「Origin」が

Vary ヘッダーにないと、特にオリジン間要求が実行された場合、アプリケーションがクライアント側とサーバー側の両方のキャッシュ ポイズニング攻撃に対してオープンになります。今回のリリースには、「Origin」ヘッダーが Vary ヘッダー値にない場合に検出するチェックが含まれています。

HTML5: CORS Functionality Abuse

CORS 要求がヌルのオリジン「Origin: null」から発生するのを許容すると、システム セキュリティが侵害され、アプリケーションが情報窃盗に対して脆弱になることがあります。今回のリリースには、サーバー応答内の Access-Control-Allow-Origin CORS ヘッダーに「null」値があると検出するチェックが含まれています。

Insecure Deployment: HTTP Request Smuggling[3]

HTTP Request Smuggling 脆弱性は、フロントエンド サーバーやバックエンド サーバーで非準拠の HTTP ヘッダーの解析結果に矛盾があると発生します。提供した要求についてサーバーごとに長さの解釈が異なっていると、攻撃者は、バックエンド TCP/TLS ソケットをポイズニングして次の要求の先頭に任意のデータを追加したり、フロントエンド サーバーで認識されることなしにバックエンド サーバーへ別の要求をスマグリングしたりすることができます。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。

Header Manipulation[4]

既存の Header Manipulation チェックが今回のリリースで機能強化され、復帰 (「CR」) 攻撃と改行 (「LF」) 攻撃が既存の CRLF 攻撃に追加されています。

コンプライアンス レポート

DISA STIG 4.10

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 4.10 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 4.10

DISA STIG 4.10 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。

[3]Insecure Deployment: HTTP Request Smuggling チェックには WebInspect v19.2.0 以降が必要です。
[4] Header Manipulation の機能強化には WebInspect v19.2.0 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 4.10 と 2019 CWE Top 25

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 4.10 と 2019 CWE Top 25 の両方をサポートする Fortify Software Security Center 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 12 月 13 日