Fortify ソフトウェア セキュリティ コンテンツ

2021 年更新版 3
2021 年 9 月 24 日

CyberRes 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、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、CyberRes 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 1,051 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。

Fortify Software Security Research (SSR) は、Fortify Secure Coding Rulepacks (英語、バージョン 2021.3.0)、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。

CyberRes Fortify Secure Coding Rulepacks [Static Code Analyzer]

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 831 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。

Golang 標準ライブラリの更新 (バージョン: 1.16)

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、標準ライブラリ名前空間であり、次の新しいカテゴリのサポートが追加されました。

- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute
- Go Bad Practices: Leftover Debug Code
- Insecure Randomness: Hardcoded Seed
- Insecure Randomness: User-Controlled Seed
- Insecure Transport: Cipher Suite Downgrade
- Insecure Transport: Weak SSL Protocol
- Often Misused: Privilege Management
- Weak Cryptographic Signature

Android 11 の更新 (API レベル: 30)

Android プラットフォームは、モバイル デバイス向けに設計されたオープンソースのソフトウェア スタックです。Android の主要なコンポーネントは、アプリケーション開発者に Android の機能を提供する Java API フレームワークです。このリリースでは、Android の Java API フレームワークを活用した、Java または Kotlin で記述された Android ネイティブ アプリケーションの脆弱性検出機能が拡張されています。Android アプリケーションのモデリングと API 適用範囲の更新により、結果のさらなる改善を期待できます。このリリースでは、危険な Android の権限に対するガイダンスを提供する、以下の新しい権限管理の脆弱性のカテゴリも含まれています。

- Privilege Management: Android Activity Recognition
- Privilege Management: Android Calendar
- Privilege Management: Android Call Log
- Privilege Management: Android Camera
- Privilege Management: Android Contacts
- Privilege Management: Android Microphone
- Privilege Management: Android Sensors

iOS 標準ライブラリの更新 (バージョン: iOS 14)

このリリースでは、Swift と Objective-C の両方で、iOS 14 のライブラリ API のサポートが更新されています。更新の対象となるのは、以下のフレームワークです。

- UIKit
- UserNotification
- SwiftUI
- MessageUI

Insecure IPC、Link Injection、Path Manipulation、Privacy Violation、Shoulder Surfing、および System Information Leak のカテゴリで改善が行われていることを確認できます。

Micro Focus Visual COBOL の更新 (バージョン: 7.0)

Micro Focus Visual COBOL バージョン 7 のサポートを拡張し、以下の 2 つの脆弱性カテゴリのサポートを追加しました。

- Integer Overflow
- Race Condition: File System Access

SAPUI5/OpenUI5 のサポート [1] (バージョン: 1.93)

SAPUI5 は、SAP が開発したクライアントサイド JavaScript フレームワークで、オープンソースの OpenUI5 とコア コントロール ライブラリのセットを共有しています。このリリースでは、以下のカテゴリの脆弱性を特定するための初期サポートを提供します。

- Cross-Site Scripting: DOM
- Cross-Site Scripting: SAPUI5 Control
- Cross-Site Scripting: Self
- Privacy Violation
- SAPUI5 Misconfiguration: Unsanitized Editor
- System Information Leak: External

JSON のサポート [2]

JavaScript Object Notation (JSON) は、軽量なデータ交換フォーマットです。このリリースでは、以下のカテゴリーの JSON における脆弱性の特定に対するサポートが改善されています。

- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password

[1] Static Code Analyzer v21.2.0 以降を使用したときに期待できる結果を改善しました。

[2] Static Code Analyzer v21.1.0 と次のフラグが必要です: '-Dcom.fortify.sca.use.json-analyzer=true'

- Password Management: Password in Comment[3]

Kotlin 標準ライブラリの更新 (バージョン: 1.4.30)

Kotlin は、Java との相互運用性を備えた、汎用の、静的に型指定された言語です。このリリースでは、Java Virtual Machine (JVM) をターゲットとした Kotlin 1.4 で導入された新しい標準ライブラリ API のサポートが更新されています。

ECMAScript 2021 (バージョン: ECMA-262)

ECMAScript 2021 で導入された新しい API のサポート。ECMAScript は、ECMAScript 言語仕様で定義された汎用プログラミング言語で、すべての最新 Web ブラウザに組み込まれていることで知られています。しかしながら、Web サーバーやモバイル アプリケーションなど、従来型のアプリケーションを構築するために使用されることが多くなっています。最新の ECMAScript 規格をターゲットにしたアプリケーションをスキャンするときに、データフローが改善されることが期待されます。

2021 Common Weakness Enumeration (CWE™) Top 25

2019 年に、SANS Top 25 に代わる Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) が導入されました。7 月にリリースされた 2021 CWE Top 25 はヒュ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した。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、CyberRes Fortify Taxonomy と 2021 CWE Top 25 との相関関係が追加されています。

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。

18.x より前のバージョンの Static Code Analyzer のサポート廃止

2020.4 リリースと同様に、Static Code Analyzer の過去 4 つのメジャー リリースのサポートを継続しています。したがって、これは、18.x より前のバージョンの Static Code Analyzer をサポートするルールパックの最後のリリースになります。次のリリースでは、18.x より前のバージョンの Static Code Analyzer は最新のルールパックをロードしません。このため、ルールパックをダウングレードするか、Static Code Analyzer のバージョンをアップグレードするかのいずれかが必要です。
今後のリリースでは、Static Code Analyzer の最新の 4 つのメジャー リリースを継

続してサポートします。

[3] Static Code Analyzer v21.2.0 以降が必要です。Static Code Analyzer v21.2.0 以降では、フラグは必要ありません。

Java J2EE の改善:

Privacy Violation および *System Information Leak* カテゴリにおける javax.servlet API のサポートを改善しました。 ***Android Bound Services:***

Android を継続的にサポートするために、このリリースでは Android Bound Services を対象範囲に含めています。Android Bound Service のメソッド パラメーターに起因する新たなデータフローの問題が想定されます。これにより、バウンド サービス内でメソッドが呼び出されたときに、データフローのサブトレースが重複する可能性があります。

Node.js の Weak Cryptographic Hash:

Node.js アプリケーションにおける脆弱な暗号ハッシュの使用を特定します。

OWASP ASVS 4.0 マッピングにレベルのサポートを追加

OWASP Application Security Verification Standard (ASVS) のアプリケーション セキュリティ検証レベル (L1、L2、L3) に違反している問題が報告されている場合、その問題を照会したいというお客様の要望に応えて、最新のセキュリティ コンテンツでは、マッピング名にこれらのレベルが追加されています。*OWASP ASVS 4.0* のグループ内で、関連する *L1*、*L2*、および *L3* キーワードの検索に加えて、AuditWorkbench や Software Security Center (SSC) で使用する関連フィルター セットとフィルター テンプレートの設計を行えるようになりました。

誤検知の改善:

このリリースでも引き続き、誤検知の除去に取り組みました。他の改善点に加えて、次の領域で誤検知がさらに減ったことを確認できます。

- jQuery における *Cross-Site Scripting* の誤検知
- *Privacy Violation: Shoulder Surfing* (JsonIgnore 属性を使用した.NET アプリケーションにおける)
- 数しか制御できない *Path Manipulation* の問題で、Fortify Priority Order を下げる場合の一貫性が強化されました
- パスワードが列挙の一部である場合に、Swift でパスワードを識別することはなくなりました
- .NET における *XML 検証の欠落*
- Java プロジェクトにおける *Null に対するチェックの欠落*

CyberRes 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

Insecure Deployment: HTTP Request Smuggling

HTTP2 Over Clear Text Smuggling (h2c Smuggling) は、従来の HTTP Request Smuggling に代わるもので、プロキシ サーバーなどの h2c に対応していないフロントエンドを悪用して、バックエンド システムへのトンネルを作ります。攻撃者はこのトンネルを利用して、フロントエンド サーバーに検知されることなく、バックエンド サーバーに追加のリクエストを密かに送信することができます。これにより、攻撃者はフロントエンドの認証制御を回避し、バックエンド システムの制限されたリソースにアクセスすることができます。このリリースには、h2c Smuggling 攻撃に使用される可能性のある設定を検出するチェック機能が含まれています。

Access Control: 認証チェックの欠落

GraphQL イントロスペクションでは、サーバーへの問い合わせにより、基礎となるスキーマに関する情報を得ることができます。イントロスペクションでは、クエリ、タイプ、フィールドなどの要素の詳細がわかります。GraphQL イントロスペクションは通常、デフォルトで有効になっています。適切な権限を持たない攻撃者は、この情報を SQL Injection やバッチ攻撃などの

攻撃に悪用することができます。このリリースには、イントロスペクションが有効になっている GraphQL エンドポイントを検出するためのチェックが含まれています。

NoSQL Injection: MongoDB

NoSQL スクリプト インジェクションの脆弱性により、攻撃者はデータベースに悪意のあるクエリを挿入することができます。
MongoDB は NoSQL データベースの 1 つで、そのドキュメントには、アプリケーションが JavaScript の操作を実行できると記載されています。NoSQL Injection は、認証されていない攻撃者がデータを抽出したり、JavaScript のコードを実行したりできるため、非常に危険です。これにより、リモート コードの実行、機密性の侵害、アプリケーション データの完全性、Denial of Service (DoS) 攻撃などが発生する可能性があります。このリリースには、MongoDB で NoSQL スクリプト インジェクションを検出するためのチェックが含まれています。

Dynamic Code Evaluation: Unsafe Deserialization

ForgeRock AM サーバー 7.0 以前、および OpenAM サーバー 14.6.4 以前には、認証前の安全でない Java 逆シリアル化の脆弱性が CVE-2021-35464 により確認されています。この脆弱性により、攻撃者は jato.pageSession パラメーターに悪意のあるシリアル化されたオブジェクトを細工して、そのオブジェクトを単一のリクエストでエンドポイント "/ccversion/Version" に送信することができます。この脆弱性は、アプリケーションで安全でないサードパーティ製の Java ライブラリが使用されているために存在します。この問題により、通常、攻撃者はサーバー上で任意のコードを実行したり、アプリケーション ロジックを悪用したり、Denial of Service (DoS) 攻撃を行ったりすることができます。このリリースには、ターゲットの Web サーバー上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。

Cross-Site Scripting: DOM[4]

Cross-Site Scripting は、動的に生成された Web ページで、ログイン情報などのユーザーの入力内容が適切に検証されずに表示されるときに発生します。これにより、攻撃者は生成されたページに悪意のあるスクリプトを埋め込み、そのサイトを閲覧したユーザーのマシン上でスクリプトを実行できます。Document Object Model (DOM) に基づく XSS の場合、悪意のあるコンテンツは、DOM 操作の一部として実行されます。成功した場合、DOM Cross-Site Scripting の脆弱性は、クッキーの操作や盗用、有効なユーザーによるものと誤認されるリクエストの作成、機密情報の漏洩、エンド ユーザーのシステム上での悪意のあるコードの実行などに悪用される可能性があります。このリリースには、クライアント側の URI フラグメントで DOM XSS を検出する新しいチェック機能が含まれています。

Web Server Misconfiguration: Insecure Mapping Directives

Web サーバー上で PHP を実行するように Nginx を構成すると、.php で終わるすべての URI をバックエンドの PHP インタープリタ (FastCGI など) に渡さなければならないことがあります。この安全でない PHP の設定をした Nginx は、要求されたフル パスが実際の既存のファイルにつながっていない場合、URL パス内のフォルダを実行対象のファイルとみなします。この誤った構成

[4] WI v21.2.0 以降が必要です。

により、攻撃者は、Web サーバーにアップロードされてアクセスできるならば、画像ファイルなどの任意のタイプのファイルで任意の PHP コードを実行することができます。このリリースには、ターゲットの Web サーバー上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。

Integer Overflow

Nginx の 0.5.6 以降、1.13.2 までのバージョンには、CVE-2017-7529 で確認された Integer Overflow の脆弱性があります。この問題は、Nginx のレンジ フィルター モジュールに存在し、攻撃者が特別に細工したリクエストを送信することで、機密の可能性がある情報を取得することができます。このリリースには、ターゲットの Web サーバー上で CVE-2017-7529 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

2021 Common Weakness Enumeration (CWE™) Top 25

2019 年に、SANS Top 25 に代わる Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) が導入されました。7 月にリリースされた 2021 CWE Top 25 はヒュ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。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。この SecureBase の更新には、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が含まれています。

ポリシーの更新

CWE Top 25 2021

CWE Top 25 2021 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。

LDAP Injection

このリリースでは、LDAP Injection チェックに改良を加え、誤検出を減らし、検査結果の精度を向上させました。

CyberRes 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。

2021 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 2021 CWE Top 25 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。

CyberRes 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、CyberRes Fortify Support Portal で見つかる場合があります。

Contact Fortify 技術サポート

CyberRes Fortify
http://softwaresupport.softwaregrp.com/
+1 (844) 260-7219

SSR へのお問い合わせ

Alexander M. Hoole
Software Security Research シニア マネージャー
CyberRes Fortify hoole@microfocus.com
+1 (650) 258-5916

Peter Blay
Software Security Research マネージャー
CyberRes Fortify
peter.blay@microfocus.com