Software Security Research のリリースに関するお知らせ

Fortify ソフトウェア セキュリティ コンテンツ

2022 年更新版 1

2022 年 3 月 25 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 (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、CyberRes Fortify ソフトウェア セキュリティ コンテンツは、29 の言語における 1,166 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 2022.1.0)、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。

CyberRes Fortify Secure Coding Rulepacks [SCA]

このリリースにより、Fortify Secure Coding Rulepacks は 29 のプログラミング言語で脆弱性に関する 946 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。

Log4j の更新 (サポートされているバージョン: 2.17)

Log4j は Java で人気のあるロギング フレームワークですが、このフレームワーク内で脆弱性が発見されたため、ここ数か月にわたって精査されています。このリリースでは、ソース コードのどの部分が Log4Shell の脆弱性の影響を受けやすいかを正確に特定するためのサポートが強化されており、次のカテゴリでそれらの部分をフラグ付けしています: *Dynamic Code Evaluation: JNDI Reference Injection*
また、アップグレードされた Log4j サポートでは、次の名前空間について Log4j の最新バージョンをカバーします。

- org.apache.logging.log4j

このサポートにより、次の脆弱性カテゴリの適用範囲も強化されます。

- Code Correctness: Stack Exhaustion
- Dynamic Code Evaluation: JNDI Reference Injection
- Log Forging
- Log Forging (debug)
- Privacy Violation
- System Information Leak

Azure Functions (Python、サポートされているバージョン: 3.10.x)

Azure Functions は、API 呼び出し、データベース トランザクションなどの事前定義されたイベントに応答してコードを実行したり、他の Azure サービスのメッセージ キューを管理したりできる、サーバーレス クラウド コンピューティング ソリューションです。このリリースでは、Azure Functions のサポートを拡張して、Python の HTTP トリガー関数をカバーしました。HTTP トリガーは、HTTP リクエストを使用して関数を呼び出すのに役立ち、サーバーレス API を構築して Webhook に応答するために使用できます。
このサポートには、次のカテゴリのカバレッジが含まれます。

- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Header Manipulation
- Header Manipulation: Cookies
- Privacy Violation
- System Information Leak: External

GraphQL のサポート: Python Graphene (サポートされているバージョン: 3.0.0)

このリリースには、Python Graphene に対する最初の GraphQL サーバーのサポートが含まれています。GraphQL は、Facebook によって開発されたオープンソース プロジェクトであり、厳密に型指定されたクエリ言語と API 用のサーバー側ランタイム エンジンを備えています。GraphQL は 2015 年以来のオープン スタンダードであり、現在では 24 を超えるプログラミング言語でサポートされています。Graphene は、Python アプリケーションで人気のある GraphQL サーバー フレームワークです。このリリースでは、Graphene で開発された GraphQL API の脆弱性を検出するために、次の 2 つのカテゴリが追加されています。

- GraphQL Bad Practices: Introspection Enabled
- GraphQL Bad Practices: GraphiQL Enabled

Kotlin の更新 (サポートされているバージョン: 1.5)

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 1.5 で導入された標準ライブラリ API のサポートが更新されています。

Sequelize (サポートされているバージョン: 6.17)

Sequelize は、Node.js アプリケーション内の多くの一般的な SQL ダイアレクトでの作業を簡素化するように設計された、Promise ベースのオブジェクト関係マッピング (ORM) ツールです。このサポートには、次のカテゴリのカバレッジが含まれます。

- Access Control: Database
- Password Management: Empty Password
- Password Management: Hardcoded Password
- Password Management: Null Password
- SQL Injection

HTML 内の安全でない参照ファイル

Web ページ内のサードパーティ サイトへのすべての参照は、安全な接続を介して行う必要があります。そのため、このリリースには、HTML ファイル内の次の新しいカテゴリのサポートが含まれています。

- Dynamic Code Evaluation: Insecure Transport
- Insecure Transport: External Link

共有パスワード データベースの検出

パスワード データベースは、パスワードを安全に保存するために作成されたファイルまたはファイルのセットです。パスワード データベースは通常、マスター パスワードまたはマスター キーを使用して暗号化されます。ただし、開発ライフサイクルを通じてアプリケーション内でパスワードの使用を維持するためには使用しないでください。このリリースでは、そのようなデータベースの存在について、次のように報告します: *Password Management: Shared Password Database*. サポートされているパスワード データベースは次のとおりです。

- KeePass
- 1Password
- Password Safe
- MacOS Keychain
- Gnome Keyring
- KDE KWallet

Cloud Infrastructure as Code

このリリースには、Cloud Infrastructure as Code (IaC) の拡張サポートが含まれています。Infrastructure as Code は、手動プロセスではなく、コードを介してコンピューター リソースを管理およびプロビジョニングするプロセスです。サポートされている技術は、AWS、AWS CloudFormation、Azure ARM、Kubernetes K8S、Azure Kubernetes Service などです。これらのサービスの設定に関連する一般的な問題が、開発者に報告されるようになりました。

サポートされる追加のカテゴリは次のとおりです。

- Ansible Bad Practices: CloudWatch Log Group Retention Unspecified
- Ansible Bad Practices: Unrestricted AWS Lambda Principal
- Ansible Bad Practices: User-Bound AWS IAM Policy
- Ansible Misconfiguration: Azure Monitor Missing Administrative Events
- Insecure Storage: Missing EC2 AMI Encryption
- Insecure Storage: Missing EFS Encryption
- Insecure Storage: Missing Kinesis Stream Encryption
- Insecure Transport: Azure App Service
- Insecure Transport: Azure Storage
- Kubernetes Bad Practices: Automated iptables Management Disabled
- Kubernetes Bad Practices: Kernel Defaults Overridden
- Kubernetes Bad Practices: Kubelet Streaming Connection Timeout Disabled
- Kubernetes Bad Practices: Missing NodeRestriction Admission Controller
- Kubernetes Bad Practices: Missing PodSecurityPolicy Admission Controller
- Kubernetes Bad Practices: Missing Security Context
- Kubernetes Bad Practices: Missing SecurityContextDeny Admission Controller
- Kubernetes Bad Practices: Missing ServiceAccount Admission Controller
- Kubernetes Bad Practices: Service Account Token Automounted
- Kubernetes Bad Practices: Shared Service Account Credentials
- Kubernetes Misconfiguration: Insecure etcd Client Transport
- Kubernetes Misconfiguration: Insecure etcd Peer Transport
- Kubernetes Misconfiguration: Missing Kubelet Certificate Authentication
- Kubernetes Misconfiguration: Missing Service Account Token Authentication
- Kubernetes Misconfiguration: Weak SSL Certificate for Kubelet

外部暗号化キーとバンドル

暗号化キーは、ソース コードとは別のファイルに保存できますが、バージョン管理システムに保持されます。また、暗号化キーは、証明書や暗号化キーなどの暗号化オブジェクトを格納するファイルである、Cryptographic バンドルに格納できます。このリリースでは、このようなファイルの存在を次のように報告します: *Key Management: Hardcoded Encryption Key*。サポートされている Cryptographic バンドルとキー ファイルは次のとおりです。

- Public-Key Cryptography Standards #12 KeyStore
- Java KeyStore、Oracle の KeyStore 形式
- Ruby On Rails マスター キー
- PuTTY プライベート キー
- Microsoft BitLocker 復号化キー

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。

Insecure Transport: Weak SSL Protocol

Secure Sockets Layer (SSL) と Transport Layer Security (TLS) は、ネットワークを介してデータを保護するメカニズムを提供します。このリリースでは、次のサポートを更新しました: *Insecure Transport: Weak SSL Protocol*。このリリース以降、SSL のすべてのバージョンの使用にフラグを付けるだけでなく、TLS バージョン 1.0 または 1.1 の使用にもフラグを付けます。

Insecure Transport: Weak SSL Cipher

暗号スイートは、Secure Sockets Layer (SSL) または Transport Layer Security (TLS) で使用される暗号化アルゴリズムを指定します。以前に Fortify WebInspect によって報告された、*Insecure Transport: Weak SSL Cipher* の結果は、Fortify Static Code Analyzer (SCA) によっても報告されるようになりました。

Weak Cryptographic Signature

デジタル署名は、デジタル メッセージの信頼性と整合性を判断するために使用される手法です。Digital Signature Algorithm (DSA) は廃止され、使用されなくなりました。このリリースには、DSA が Java、Ruby、および PHP で使用されている場合に、*Weak Cryptographic Signature* にフラグを付けるサポートが含まれています。

マイナー ノードの強化

'net'、'http'、'https'、および 'os' を含む Node.js パッケージのサポートが強化されました。*Cross-Site Scripting*、*Server-Side Request Forgery*、および *System Information Leak* の各カテゴリでより正確な結果を期待できます。

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、次の領域で誤検知の更なる削減を期待できます。

- Credential Management: Hardcoded API Credentials: GitHub アクセス トークンを識別する場合
- Cross-Site Scripting: Content Sniffing: Java アプリケーションの場合
- "Portability Flaw: Locale Dependent Comparison" の断続的な誤検知
- "OGNL Expression Injection: Double Evaluation" の断続的な誤検知
- Password Management: Hardcoded Password: example.com などのサンプル ドメイン内で設定された
- SQL Injection: iBatis データ マップ

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。

脆弱性サポート Dangerous File Inclusion: Local

Grafana は、監視と可観測性のためのオープンソース プラットフォームです。Grafana の一部のバージョンは、CVE-2021-43798 で識別されるように、ディレクトリ トラバーサルに対して脆弱です。この脆弱性により、ローカル ファイルへのアクセスが可能になります。攻撃者がサーバー上のファイルの内容を取得する可能性があり、それによって、機密データの開示や、独占所有権のあるビジネス ロジックのリカバリが発生することがあります。このリリースには、Grafana 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。

ポリシーの更新 Aggressive Log4Shell[1]

新しい Aggressive Log4Shell ポリシーが、サポートされているポリシーの SecureBase リストに追加されました。Log4j を使用する Web アプリケーションの包括的なセキュリティ評価のために、既存のポリシーより正確で積極的かつ明白なスキャンを実行できます。これには、脆弱なバージョンの Apache Log4j ライブラリでの *JNDI Reference Injection* が含まれます。

その他の正誤情報

このリリースでは、誤検知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、引き続きリソースを投資しています。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。

Log4Shell[1]

このリリースでは、Log4Shell チェックが強化されており、新しい Aggressive Log4Shell ポリシーのサポートが追加されています。これにより、脆弱なバージョンの Apache Log4j ライブラリで *JNDI Reference Injection* をより正確にスキャンできます。

CSRF の更新

このリリースでは、偽陰性を減らし、結果の精度を向上させるために、CSRF チェックが強化されています。

---

[1] *Log4Shell* チェックと *Aggressive Log4Shell* ポリシーには、WebInspect 21.2.0.117 パッチ以降が必要です。

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。

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

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