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 2

2022 年 6 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 (SCA) および Fortify WebInspect 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、Fortify ソフトウェア セキュリティ コンテンツは、30 の言語における 1,220 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 2022.2.0)、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。

Fortify Secure Coding Rulepacks [SCA]

このリリースにより、Fortify Secure Coding Rulepacks は 30 のプログラミング言語で脆弱性に関する 1,000 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 についての改善点 (サポートされているバージョン: 6.0)

.NET は一般的なプログラミング プラットフォームであり、これによりプログラマーは、標準化された API セットを使用して C# や VB.NET などの言語でコードを記述できます。このリリースでは、データフローの改善のため、適用範囲が最新バージョンの .NET に拡大されたほか、次のカテゴリについて API 適用範囲が拡張されています。

- Access Control: Database
- Path Manipulation
- Privacy Violation
- Server-Side Request Forgery
- SQL Injection
- System Information Leak: External
- Weak Cryptographic Hash: Insecure PBE Iteration Count
- Weak Encryption: Insecure Mode of Operation

ASP.NET Core についての改善点 (サポートされているバージョン: 6.0)

ASP.NET Core は、.NET との使用を目的とした主要な Web フレームワークです。このフレームワークは、MVC Web アプリケーションや Web API など、さまざまな種類のアプリケーションを作成する機能を備えています。このリリースでは、適用範囲が最新バージョンの ASP.NET Core (最小限の API を含む) まで拡大され、サポートされるカテゴリが次の範囲まで拡張されています。

- .NET Attribute Misuse: Authorization Bypass
- ASP.NET Bad Practices: Compression Over Encrypted WebSocket Connection
- ASP.NET Middleware Out of Order: Default Cookie Configuration
- ASP.NET Middleware Out of Order: Insecure Transport
- ASP.NET Middleware Out of Order: Insufficient Logging
- ASP.NET Misconfiguration: Insecure Transport
- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute

Weak Cryptographic Implementation

Psychic Signatures (CVE-2022-21449) は、楕円曲線デジタル署名アルゴリズム (ECDSA) の Java 実装における脆弱性です。この脆弱性により、攻撃者は、すべてゼロのデジタル署名を有効なものとして受け入れるようアプリケーションに強制することができます。脆弱性を含む Java のバージョンは、15、16、17、および 18 です。脆弱なバージョンの Java が使用されていると、攻撃者が特定の種類の SSL 証明書、署名された JSON Web トークン、さらには WebAuthn 認証メッセージを偽造する可能性があります。このリリースでは、Java での Weak Cryptographic Implementation を報告するためのサポートが追加されています。

Jakarta EE のサポート (サポートされているバージョン: 9.0.0)

Jakarta EE は、クラウド ネイティブな Java アプリケーションの開発に使用されるオープンソース フレームワークの形式で、ベンダーに依存しない、オープンで包括的な仕様セットを提供します。これは以前、Java EE (または J2EE) と呼ばれており、最もよく知られているサーバーサイド Java のフレームワークの 1 つでした。このリリースでは、52 の脆弱性カテゴリにまたがる既存の Java EE 適用範囲に改善が加えられています。

シークレット スキャンについての改善点

シークレット スキャンは、ソース コードと構成ファイルのシークレットを検索および検出するための手法です。パスワードや API トークンを含む構成ファイルは、誤ってソース コード リポジトリに漏洩することがあります。このリリースには、一般的なパスワード ハッシュ形式のサポートが含まれています。適用範囲には、製品の構成ファイル内にある、一般的なパスワード ハッシュ形式とシークレットの識別が含まれます。これには、OpenVPN、Windows リモート デスクトップ、netrc、IntelliJ IDEA、DBeaver、FileZilla、Heroku、DigitalOcean doctl が含まれます。
強化された適用範囲は、次のカテゴリに提供されます。

- Key Management: Empty Encryption Key
- Key Management: Hardcoded Encryption Key
- Key Management: Null Encryption Key
- Password Management: Hardcoded Password
- Password Management: Password in Configuration File
- Password Management: Weak Cryptography

Express JS についての改善点 (サポートされているバージョン: 4.x)[1]

Express は、Node.js を使用して Web アプリケーションを構築するためのフレームワークです。ルーティング、エラー処理、テンプレート化、ミドルウェア管理、および HTTP 関連ユーティリティの機能を提供します。

[1] SCA バージョン 22.1.1 が必要です

このリリースでは、次のカテゴリに関する Express 4.x のサポートが改善されています。

- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Permissive SameSite Attribute
- Insecure Transport
- Path Manipulation
- Privacy Violation
- Process Control
- Setting Manipulation
- System Information Leak: External

JavaScript Handlebars (サポートされているバージョン: 4.7.7)

Handlebars は、再利用可能な Web テンプレートを作成するために設計された JavaScript ライブラリです。これらのテンプレートは、HTML、テキスト、および式を組み合わせたものです。式は HTML コードに直接埋め込まれ、コードによって挿入されるコンテンツのプレースホルダーとして機能するため、ドキュメントを簡単に再利用できます。
このリリースでは、Handlebars 4.7.7 のサポートが追加され、データフローの適用範囲が改善され、次のカテゴリについて API 適用範囲が拡張されました。

- Cross-Site Scripting: Handlebars Helper
- Handlebars Misconfiguration: Escaping Disabled
- Handlebars Misconfiguration: Prototypes Allowed
- Log Forging
- Log Forging (debug)
- Privacy Violation
- System Information Leak
- Template Injection

JavaScript Mustache (サポートされているバージョン: 4.2.0)

Mustache は、動的テンプレートを作成する基盤としてテンプレートとビューを提供する、オープンソースのロジックレス テンプレート システムです。テンプレートにはプレゼンテーションの形式とコードが含まれており、ビューにはテンプレートに含めるデータが含まれています。
このリリースでは、テンプレート インジェクションの脆弱性を特定するための Mustache 4.2.0 のサポートが追加されています。

GraphQL.js (サポートされているバージョン: 16.5.0)

GraphQL.js は GraphQL の JavaScript リファレンス実装であり、JavaScript アプリケーションで広く使用されています。このリリースでは、GraphQL API の次の脆弱性カテゴリを検出するための、初期 GraphQL サーバーのサポートが追加されています。

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- GraphQL Bad Practices: Introspection Enabled
- GraphQL Bad Practices: GraphiQL Enabled

- Privacy Violation
- System Information Leak: External

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

Python-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、GraphQL API の次の脆弱性カテゴリを検出するため、GraphQL サーバーのサポートが 2022.1.0 から改善されています。

- Cross-Site Scripting: Inter-Component Communication
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Privacy Violation
- System Information Leak: External

コードとしてのクラウド インフラストラクチャ

Infrastructure as Code (IaC) は、さまざまな手動プロセスを実行するのではなく、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。このリリースでは、IaC に対する拡張サポートが追加されています。サポートされるテクノロジーには、Azure と AWS に展開するための Ansible 構成や、Azure と GCP に展開するための Terraform 構成が含まれます。これらのサービスの構成に関連する共通の問題は、開発者に報告されるようになりました。

Terraform 構成:
Terraform は、クラウド インフラストラクチャを構築、変更、およびバージョン管理するための、コード ツールとしてのオープンソース インフラストラクチャです。これは、HashiCorp 構成言語 (HCL) と呼ばれる独自の宣言型言語を使用します。クラウド インフラストラクチャは、構成ファイルに体系化されて、目的の状態を記述します。

Terraform プロバイダーは、***Microsoft Azure*** インフラストラクチャーの構成と管理をサポートします。このリリースでは、Microsoft Azure サービスの Terraform 構成について次のカテゴリを報告します。

- Azure Terraform Misconfiguration: Insecure App Service Transport
- Azure Terraform Misconfiguration: Insecure CDN Endpoint Transport
- Azure Terraform Misconfiguration: Insecure Function App Transport
- Azure Terraform Misconfiguration: Insecure Logic App Transport
- Azure Terraform Misconfiguration: Insecure MariaDB Transport
- Azure Terraform Misconfiguration: Insecure MySQL Transport
- Azure Terraform Misconfiguration: Insecure Network Monitor Transport
- Azure Terraform Misconfiguration: Insecure PostgresSQL Transport
- Azure Terraform Misconfiguration: Insecure Redis Cache Transport
- Azure Terraform Misconfiguration: Insecure Spring Cloud Redis Transport
- Azure Terraform Misconfiguration: Insecure Spring Cloud Transport
- Azure Terraform Misconfiguration: Insecure Storage Account Transport

Terraform プロバイダーは、***Google Cloud Platform (GCP)*** インフラストラクチャーの構成と管理をサポートします。このリリースでは、Google Cloud Platform の Terraform 構成について次のカテゴリを報告します。

- GCP Terraform Bad Practice: Overly Permissive Service Account
- GCP Terraform Misconfiguration: BigQuery Dataset Publicly Accessible
- GCP Terraform Misconfiguration: Cloud DNS DNSSEC Disabled
- GCP Terraform Misconfiguration: Cloud KMS CryptoKey Publicly Accessible
- GCP Terraform Misconfiguration: Cloud SQL Backup Disabled
- GCP Terraform Misconfiguration: Cloud Storage Bucket Publicly Accessible
- GCP Terraform Misconfiguration: Compute Engine Access Control
- GCP Terraform Misconfiguration: Compute Engine Default Service Account
- GCP Terraform Misconfiguration: Compute Engine Project-Wide SSH
- GCP Terraform Misconfiguration: Google Project Network Access Control
- GCP Terraform Misconfiguration: Insecure Cloud SQL Transport
- GCP Terraform Misconfiguration: Insecure Load Balancer Transport
- GCP Terraform Misconfiguration: Insufficient Cloud Storage Bucket Logging
- GCP Terraform Misconfiguration: Insufficient GKE Cluster Logging
- GCP Terraform Misconfiguration: Insufficient GKE Cluster Monitoring
- GCP Terraform Misconfiguration: Insufficient VPC Flow Logging
- GCP Terraform Misconfiguration: GKE Cluster Administrative Interface Access Control
- GCP Terraform Misconfiguration: GKE Cluster Certificate-Based Authentication
- GCP Terraform Misconfiguration: GKE Cluster Legacy Authorization
- GCP Terraform Misconfiguration: GKE Cluster HTTP Basic Authentication
- GCP Terraform Misconfiguration: GKE Container-Optimized OS Not In Use
- GCP Terraform Misconfiguration: GKE Node Auto-Upgrade Disabled
- GCP Terraform Misconfiguration: Weak Cryptographic Cloud DNS Signature
- GCP Terraform Misconfiguration: Weak GKE Cluster Network Management
- GCP Terraform Misconfiguration: Weak Key Management

Ansible 構成:

Ansible は、構成管理、アプリケーション展開、クラウド プロビジョニング、およびノード オーケストレーションをさまざまな環境に提供するオープンソースの自動化ツールです。

Ansible には、***Amazon Web Services (AWS)*** の構成と管理をサポートするモジュールが含まれています。このリリースでは、AWS Ansible 構成について次のカテゴリを報告します。

- AWS Ansible Misconfiguration: Amazon RDS Publicly Accessible
- AWS Ansible Misconfiguration: Insecure CloudFront Distribution Transport
- AWS Ansible Misconfiguration: Insufficient CloudTrail Logging

Ansible には、***Microsoft Azure*** クラウド コンピューティング サービスの構成と管理をサポートするモジュールも含まれています。 このリリースでは、Microsoft Azure の Ansible 構成について次のカテゴリを報告します。

- Azure Ansible Misconfiguration: Overly Permissive Azure SQL Database Firewall

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。

Log4j (サポートされているバージョン: 2.17)

Log4j のサポートには、新しいカテゴリ *Denial of Service: Stack Exhaustion* の検出が含まれるようになりました。

Oslo.config (サポートされているバージョン: 8.8.0)

Python の oslo.config の初期サポートには、新しいカテゴリ *Privacy Violation: Unobfuscated Logging* の検出が含まれるようになりました。

Objective-C エラーの修正とパフォーマンスの向上

2022R1 ルールパックを使用して、Objective-C ファイルを含むプロジェクトをスキャンすると、次の問題が発生する可能性があります。

- スキャン フェーズで、「[error] Unexpected exception during dataflow analysis...」という形式のエラー メッセージが SCA 出力またはログ ファイルに表示される
- データフロー分析でのスキャン時間が異常に長くかかり、データフロー喪失の問題が起こる可能性がある

これらの問題に対処できるようお客様をサポートするため、Objective-C ホットフィックス ルールパックが提供されています。同じ修正は、この正規版の R2 リリースにも組み込まれています。ホットフィックス ルールパックをすでにご利用のお客様は、R2 リリースのルールパックに更新する際にそれを削除する必要があります。

誤検知の改善:

このリリースでは、誤検知を排除する取り組みが引き続き行われています。他の改善点に加え、次の分野で誤検知の排除が進んでいます。

- *SQL Injection: iBatis Data Map* - リテラルの「$」文字が検出された場合の誤検知を防止
- *Password Management: Password in Configuration File* - 値が可変プレースホルダーの場合の誤検知を防止
- *ASP.NET MVC Bad Practices: Model With Required Non-Nullable Property* - [BindRequired] 属性を使用しているときに発生する C# ASP.NET アプリケーションでの誤検知を防止
- *Often Misused: Authentication* - Java アプリケーションでの誤検知を削減
- *XSS: Content Sniffing* - Java Spring アプリケーションでの誤検知を削減
- *Privacy Violation* - .NET アプリケーションでの誤検知を削減
- *SOQL Injection* および *SOSL Injection* - セマンティック アナライザーで検出された問題は、Fortify Priority Order を「低」として報告

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

OGNL Expression Injection: Double Evaluation

CVE-2022-26134 で特定された重大な脆弱性である OGNL Expression Injection は、Atlassian Confluence Server および Data Center に影響を与えます。この脆弱性により、認証を受けていない攻撃者が、脆弱なアプリケーションで任意のコードを実行する可能性があります。影響を受ける Confluence Server および Data Center は、1.3.0 から 7.4.16、7.13.0 から 7.13.6、7.14.0 から 7.14.2、7.15.0 から 7.15.1、7.16.0 から 7.16.3、7.17.0 から 7.17.3、および 7.18.0 です。このリリースには、影響を受けた Confluence サーバーと Data Center サーバー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。

Dynamic Code Evaluation: Code Injection

Pivotal の Spring Framework には CVE-2022-22965 で特定されたリモート コード実行 (RCE) に対する脆弱性があることが判明しました。リモートの攻撃者による、特別に細工されたリクエスト パラメーターの提供が可能になり、任意の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、影響を受けた Spring Framework バージョンの Web 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。

Insecure Deployment: OpenSSL

SSL/TLS 接続をサポートするために広く使用されている有名な暗号ライブラリである OpenSSL は、CVE-2022-0778 で特定されたサービス拒否 (DoS) の脆弱性に対して脆弱であることが判明しています。これにより、無効で明示的な楕円曲線パラメーターを持つ証明書を作成し、影響を受けたシステムで無限ループ DoS をトリガーすることが可能になります。このリリースには、対象の Web サーバー上で CVE-2022-0778 の脆弱性を検出するためのチェックが含まれています。このチェックは、影響を受けたシステムに DoS 状態を引き起こし、サービスを利用できなくなる可能性があるため、「標準」ポリシーにはこのチェックは含まれていません。「すべてのチェック」ポリシーを使用するか、チェックを含めるように既存のポリシーをカスタマイズするか、カスタム ポリシーを作成してこのチェックを実行します。

その他の正誤情報

このリリースでは、誤検出の数を減らし、お客様の側で問題をより深く調査いただけるようにするため、継続的に力を注いできました。以下の分野に関連して報告された内容にも、問題の変化を実感いただけるはずです。

Password Management: Weak Password Policy

このリリースには、パスワード ポリシー チェックに関する軽微な改善点 (入力タイプがテキスト ボックスの場合、パスワードとユーザー名のフィールドで精度が向上) が含まれています。

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。

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

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

2022 年 6 月 24 日