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 3

2022 年 9 月 30 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) や 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 1,244 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 (英語版、バージョン 2022.3.0)、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。

Fortify Secure Coding Rulepacks [Fortify Static Code Analyzer]

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 1,024 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。

ASP.NET Core の更新 (サポートされているバージョン: 6.0)[1]

Model-View-Controller (MVC) パターンでは、ビューは *.cshtml* ファイルであり、Razor マークアップに埋め込まれた C# プログラミング言語を使用します。Razor マークアップは、HTML マークアップと連携して、クライアントに送信される Web ページを生成するコードです。ビューは、アプリケーションのデータ表示とユーザー操作を処理します。Fortify Static Code Analyzer バージョン 22.2.0 以降を使用すると、ルールでビュー内の問題の検出がサポートされるようになりました。
サポートには、次の脆弱性カテゴリが含まれます。

- ASP.NET MVC Bad Practices: Form Without AntiForgery Token
- Cross-Site Scripting: Inter-Component Communication (Cloud)
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Open Redirect
- Privacy Violation
- System Information Leak

Entity Framework Core (サポートされているバージョン: 6.0)

Entity Framework (EF) Core は、.NET アプリケーション用のオープンソース データ アクセス技術です。EF Core を使用すると、開発者は .NET オブジェクトをデータベース スキーマにマッピングし、標準 API と LINQ クエリを介してデータベース操作を呼び出すことができます。サポートには、次の脆弱性カテゴリが含まれます。

- Access Control: Database
- ASP.NET Bad Practices: Leftover Debug Code
- Connection String Parameter Pollution
- Insecure Transport: Database
- Password Management: Hardcoded Password
- Setting Manipulation
- SQL injection
- System Information Leak: Overly Broad SQL Logging

[1] Fortify Static Code Analyzer バージョン 22.2.0 以降が必要です。

GitHub Actions

GitHub Actions は、ビルド、テスト、デプロイの各パイプラインの自動化を可能にする継続的インテグレーションおよび継続的デリバリー (CI/CD) プラットフォームです。最近表面化している脆弱性では、さまざまなシステムにわたってコマンド インジェクションの攻撃ベクトルが発生しています。このリリースには、次のカテゴリで発生する、このコマンド インジェクションの脆弱性に関連する一般的なインスタンスの検出が含まれています。

- Command Injection: GitHub Actions

React (サポートされているバージョン: 18.2)[2]

React (ReactJS) は、コンポーネントベースのユーザー インターフェイスを構築するためのオープンソースの JavaScript ライブラリです。このリリースで新たにサポートが追加された脆弱性カテゴリはありませんが、正確性を向上し誤検知を減らすために React の適用範囲がリファクタリングされました。

React Native (サポートされているバージョン: 0.70)[2]

React Native は、JavaScript および JSX でマルチプラットフォームのユーザー インターフェイスを開発するためのオープンソースの UI フレームワークです。React Native を使用すると、開発者は、ターゲット プラットフォームのネイティブ レンダリング API によってレンダリングされるモバイル アプリケーションを記述して、洗練された一貫したユーザー エクスペリエンスを生み出すことができます。React でサポートされている脆弱性カテゴリに加えて、React Native では次の脆弱性カテゴリが追加されています。

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

React Native Async Storage (サポートされているバージョン: 1.17)[2]

Async Storage は、コミュニティ *react-native-async-storage プロジェクト*に基づいた、React Native 用の暗号化されていない非同期のキー値ストレージ ライブラリです。Async Storage は、iOS および Android プラットフォーム固有のネイティブ ストレージ メカニズムの上に抽象化を提供します。サポートにより、Async Storage を介したデータフローと、既存の JavaScript およびプラットフォーム/ライブラリ固有の脆弱性カテゴリのレポートが可能になります。

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、さまざまなソース コードと構成ファイルでシークレットを見つけるという概念です。Fortify Static Code Analyzer は、シークレット スキャンをすべてのファイル タイプに適用します。これにより、コード言語に関係なく、特定のシークレットを見つけることができます。次のシークレットへのサポートが追加され、次のカテゴリで報告されます: *Password Management: Hardcoded Password* または *Credential Management: Hardcoded API Credentials*:

- HTTP Basic 認証トークン
- JWT (JSON Web Tokens)
- NPM (Node Package Manager) アクセス トークン
- Postman API キー
- PyPI API トークン

---

[2] Fortify Static Code Analyzer バージョン 22.2.0 以降が必要です。

Java および Go 用 gRPC の初期サポート (サポートされているバージョン: 1.49.0)

Google Remote Procedure Call (gRPC) は、最新のマルチ環境およびマルチ言語に対応した、オープンソースの高性能 RPC フレームワークです。gRPC により、サービスで負荷分散、トレース、および認証がサポートされます。従来の JSON-over-HTTP とは異なり、gRPC は HTTP2 に基づいており、通常はメッセージにバイナリ プロトコル バッファー (protobuf) 形式を使用します。gRPC プロジェクトの場合、ユーザーは Fortify Static Code Analyzer の変換フェーズ中に .proto ファイル定義から生成されたコードを含める必要があります。

追加された Go gRPC v1.49.0 のサポートでは、次の脆弱性カテゴリがカバーされます。

- Header Manipulation
- Privacy Violation
- System Information Leak: External

追加された Java gRPC v1.49.0 のサポートでは、次の脆弱性カテゴリがカバーされます。

- Denial of Service
- gRPC Metadata Manipulation
- Insecure Transport
- Insecure Transport: gRPC Server Credentials
- Insecure Transport: gRPC Channel Credentials
- Privacy Violation
- Resource Injection
- System Information Leak: External

Flask の初期サポート (サポートされているバージョン: 2.2.x)

Flask は Python で書かれた Web フレームワークです。当初は *Werkzeug* および *Jinja* ライブラリのラッパーでしたが、Flask は最も人気のある Python Web アプリケーション フレームワークの 1 つになりました。Python に対する Google Cloud Functions サポートを補完するために、このリリースには Flask Response オブジェクトのみのサポートが含まれています。
サポートには、次の脆弱性カテゴリが含まれます。

- Cookie Security: Cookie not Sent Over SSL
- Cookie Security: HTTPOnly not Set
- Cookie Security: Missing SameSite Attribute
- Cookie Security: Overly Broad Domain
- Cookie Security: Overly Broad Path
- Cookie Security: Overly Permissive SameSite Attribute
- Cookie Security: Persistent Cookie
- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- Header Manipulation
- Header Manipulation: Cookies
- HTML5: Misconfigured Content Security Policy
- HTML5: Overly Permissive Content Security Policy
- HTML5: Overly Permissive CORS Policy
- HTML5: Unenforced Content Security Policy
- Open Redirect

- Privacy Violation
- System Information Leak: External

Google Cloud Functions (サポートされているバージョン: 403.0.0)

Google Cloud Functions は、クラウド サービスを構築して接続するためのサーバーレス実行環境です。API 呼び出し、データベース トランザクション、Cloud Storage へのファイルのアップロード、Pub/Sub トピックの受信メッセージなど、事前定義されたイベントに応答してコードを実行できます。
Cloud Functions には、次の 2 つの製品バージョンがあります。オリジナル バージョンである Cloud Functions (第 1 世代) と、*Cloud Run* および *Eventarc* 上に構築された新しいバージョンである、機能セットが強化された Cloud Functions (第 2 世代) です。このリリースには、Python での Google Cloud Functions のサポートと、Java での Google Cloud Functions の更新されたサポートが含まれています。

Python でサポートされている脆弱性カテゴリには、Flask API でサポートされているカテゴリ以外に、次のものがあります。

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

Python Google Cloud Functions の場合、ユーザーは JSON または YAML クラウド ビルド ファイルを含める必要があります。または、ユーザーはスキャン時に次のプロパティを設定できます。

- *com.fortify.sca.rules.GCPFunctionName* を関数名に設定する必要があります。
- *com.fortify.sca.rules.GCPHttpTrigger* は、トリガー タイプが HTTP の場合は true に設定し、他のトリガー タイプの場合は false に設定する必要があります。

第 2 世代の更新されたルール サポートにより、Java Google Cloud Functions は CloudEvents リクエストから発生した危険な入力のソースを識別します。

Apollo Server の初期サポート (サポートされているバージョン: 3.6.8)

Apollo Server は、GraphQL API を構築するために JavaScript アプリケーションで使用されるオープンソースの GraphQL サーバーです。このリリースでは、Apollo Server 用 GraphQL サーバーの初期サポートが追加されています。これには、Apollo Server で開発された GraphQL API の次の脆弱性カテゴリの検出が含まれます。

- Cross-Site Scripting: Persistent
- Cross-Site Scripting: Poor Validation
- Cross-Site Scripting: Reflected
- GraphQL Bad Practices: Introspection Enabled
- Privacy Violation
- System Information Leak: External

Infrastructure as Code (IaC)

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。サポートされている技術には、GCP、OpenAPI 仕様、および MuleSoft への展開用の 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。

Google Cloud Platform (GCP) 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、オープンソース IaC ツールです。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、GCP インフラストラクチャの構成と管理をサポートします。このリリースでは、GCP Terraform 構成の次の脆弱性カテゴリがカバーされています。

- GCP Terraform Misconfiguration: Cloud SQL Database Publicly Accessible
- GCP Terraform Misconfiguration: Cloud Storage Bucket Uniform Access Disabled
- GCP Terraform Misconfiguration: Compute Engine IP Forwarding Enabled
- GCP Terraform Misconfiguration: Compute Engine Serial Console Enabled
- GCP Terraform Misconfiguration: Compute Engine Shielded VM Option Disabled
- GCP Terraform Misconfiguration: GKE Cluster Node Auto-Repair Disabled
- GCP Terraform Misconfiguration: GKE Cluster Publicly Accessible
- GCP Terraform Misconfiguration: Overly Permissive Role
- GCP Terraform Misconfiguration: Permissive Firewall

OpenAPI 仕様

OpenAPI 仕様では、プログラミング言語に依存しない標準の HTTP API の記述が定義されています。OpenAPI 仕様に準拠する OpenAPI ドキュメントは、JSON または YAML 形式で表すことができます。この標準は、実装やドキュメントにアクセスせずに、またはネットワーク検査を通じて、サービスの機能を定義します。このリリースでは、OpenAPI 構成の次の脆弱性カテゴリがカバーされています。

- OpenAPI Misconfiguration: Credential Leakage
- OpenAPI Misconfiguration: Empty Global Security Requirement
- OpenAPI Misconfiguration: Empty Operation Security Requirement
- OpenAPI Misconfiguration: Insecure Transport
- OpenAPI Misconfiguration: Missing Error Handling
- OpenAPI Misconfiguration: Missing Global Security Requirement
- OpenAPI Misconfiguration: Missing Operation Security Requirement
- OpenAPI Misconfiguration: Missing Security Schemes
- OpenAPI Misconfiguration: Optional Global Security Requirement
- OpenAPI Misconfiguration: Optional Operation Security Requirement
- OpenAPI Misconfiguration: Weak Authentication

Mule

Mule Runtime は、MuleSoft が提供するエンタープライズ サービス バスおよび統合フレームワークで、単に Mule と呼ばれることもよくあります。Mule を使用すると、Web Services、HTTP、Java Database Connectivity (JDBC) などの既存のシステムの統合が可能になります。Mule は、エンタープライズ ネットワーク内でまたはインターネットを介してアプリケーション間のトランジット システムとして機能することにより、異なるアプリケーションが相互に通信できるようにします。このリリースでは、Mule 構成の次の脆弱性カテゴリがカバーされています。

- Mule Misconfiguration: Hardcoded Password
- Mule Misconfiguration: Insecure Database Transport
- Mule Misconfiguration: Insecure Transport
- Mule Misconfiguration: Server Identity Verification Disabled

2022 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。6 月にリリースされた 2022 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。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 2022 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、誤検知の数を減らし、一貫性を確保するためにリファクタリングを行い、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。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。

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

2021.4 リリースで行われたように、Fortify Static Code Analyzer の最新の 4 つのメジャー リリースを引き続きサポートします。したがって、これは、19.x より前のバージョンの Fortify Static Code Analyzer をサポートする Rulepack の最後のリリースになります。次のリリースでは、19.x より前のバージョンの Fortify Static Code Analyzer は最新の Rulepack をロードしません。これには、Rulepack をダウングレードするか、Fortify 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の必要があります。今後のリリースでは、Fortify 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。

Infrastructure as Code (IaC) の脆弱性カテゴリの名前変更

IaC に関連する構成ミスや好ましくない挙動を検出するためのサポートが継続的に更新されているため、セキュリティ コンテンツの次のリリースでは、脆弱性カテゴリのサブセットでカテゴリ名が変更されます (2022 Update 4)。脆弱性カテゴリ名が変更された場合、以前のスキャンを新しいスキャンとマージしたときのスキャン結果では、カテゴリが追加または削除されます。

脆弱性カテゴリに対する Fortify Priority Order メタデータのリファクタリング

アプリケーション セキュリティ ドメインが成熟するにつれて、脆弱性カテゴリが機密性、整合性、および可用性に与える影響についての集合的な知識と理解も進化しています。セキュリティ コンテンツの次のリリースには、脆弱性カテゴリのサブセットの脆弱性メタデータ フィールド「精度」と「影響」への変更が含められます (2022 Update 4)。脆弱性メタデータ フィールドが変更されると、今後のスキャン結果で、さまざまなフィルター セット フォルダー (重要、高、中、低など) に問題が表示される可能性があります。最初の更新では、上位の Fortify Priority Order (FPO) フォルダーから下位の FPO フォルダーへの移動でいくつかの問題が発生します。この変更が既存のフィルター セットとテンプレートに与える影響について、お客様の側でご準備いただく必要があります。

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。

- *Cross-Site Request Forgery* - 4.5.2 以降のバージョンの .NET Framework を使用する .NET アプリケーションでの誤検知の排除
- *JavaScript Hijacking* - 問題 (以下のセクションを参照)

- *Key Management* - JavaScript スキャン全体での誤検知の削減
- *Key Management* - 主に SAPUI5 プロジェクトに影響する誤検知の削減
- *Key Management* - 多数の誤検知生成の比較に基づく問題と排除
- *Password Management: Hardcoded/Empty/Null Password* - C# 条件ステートメントの誤検知の防止
- *Password Management* - NPM、Yarn、および Bower ファイルからの誤検知の削減
- *Privacy Violation: Autocomplete* - 新しいパスワードを設定する際の誤検知の削減
- *Setting Manipulation* - 環境変数をクリアする際の誤検知の削減
- *Weak Cryptographic Signature* - java.security パッケージでの誤検知の防止
- *XML Entity Expansion Injection* - JAXP トランスフォーマーを使用する Java プログラムでの誤検知の削減

JavaScript Hijacking の削除

次のカテゴリは、最新の ECMAScript では関連性がなくなったため、削除されました。

- JavaScript Hijacking
- JavaScript Hijacking: Constructor Poisoning
- JavaScript Hijacking: Vulnerable Framework

その結果、上記のカテゴリのすべての問題がスキャン結果から削除されます。

カテゴリの変更

誤検知の削除に加えて、カテゴリを統合する必要があった場所や、誤ってラベル付けされた場所をいくつか特定しました。脆弱性カテゴリ名が変更された場合、以前のスキャンを新しいスキャンとマージしたときのスキャン結果では、カテゴリが追加または削除されます。

- *Insecure SSL: Android Hostname Verification Disabled* が次のように報告されるようになりました: *Insecure SSL: Server Identity Verification Disabled*
- Dockerfiles で、*Password Management: Hardcoded Password* の問題が次のように報告されるようになりました: *Password Management: Password in Configuration Files*
- .NET では、データベース接続文字列を設定するときの *Setting Manipulation* の一部のインスタンスが次のように報告されるようになりました: *Connection String Parameter Pollution*

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: Unpatched Application

dotCMS は、コンテンツ、イメージ、アセットを 1 か所で作成および再利用できるコンテンツ管理システムです。ContentResource API は、CVE-2022-26352 で特定されたリモート コード実行 (RCE) の脆弱性の影響を受けやすくなっています。コンテンツを保存するために使用されるファイル名は、マルチパート リクエストで提供されたユーザー入力から構築され、dotCMS によってサニタイズされません。

これにより、攻撃者がシステムに任意のファイルをアップロードできるようになり、結果として RCE が発生します。このリリースには、影響を受ける dotCMS バージョンを実行するターゲット 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。

Insecure Deployment: Unpatched Application

Apache APISIX は、負荷分散、動的アップストリームなどのトラフィック管理機能を提供するオープンソース API ゲートウェイです。この API ゲートウェイは、CVE-2022-24112 で特定された RCE の脆弱性の影響を受けやすくなっています。攻撃者は、バッチリクエスト プラグインを介して Apache APISIX の IP 制限をバイパスできます。APISIX がデフォルトの管理キーを使用し、管理 API が有効になっており、カスタム管理ポートが割り当てられていない場合、攻撃者はバッチリクエスト プラグインを介して管理 API を呼び出すことができ、結果として RCE が発生します。このリリースには、影響を受ける Apache APISIX バージョンを実行するターゲット 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: JNDI Reference Injection[3]

Java Naming and Directory Interface (JNDI) は、クライアントがデータとオブジェクトを名前で検出および検索できるようにする Java API です。これらのオブジェクトは、Remote Method Invocation (RMI)、Common Object Request Broker Architecture (CORBA)、Lightweight Directory Access Protocol (LDAP)、または Domain Name Service (DNS) などのさまざまなネーミング サービスまたはディレクトリ サービスを介して格納および取得できます。攻撃者が JNDI ルックアップ操作の引数に対する制御を取得した場合、攻撃者は制御下にあるネーミング サービスまたはディレクトリ サービスへのルックアップをポイントし、オブジェクトのインスタンス化にリモート ファクトリを使用する JNDI 参照を返す可能性があります。この攻撃により、ルックアップ操作を実行するターゲット サーバーで任意のリモート 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、対象の 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。

Dynamic Code Evaluation: Unsafe Deserialization[3]

Oracle Fusion Middleware バージョン 12.2.1.3.0 および 12.2.1.4.0 の ADF Faces コンポーネントで、事前認証の安全でない Java デシリアライズの脆弱性が、CVE-2022-21445 によって識別されました。これは、Business Intelligence、Enterprise Manager、Identity Management、SOA Suite、WebCenter Portal、Application Testing Suite、Transportation Management など、ADF Faces コンポーネントに依存するすべてのアプリケーションに影響を与えます。この問題により、攻撃者はサーバー上で任意のコードを実行し、アプリケーション ロジックを悪用し、Denial of Service (DoS) 攻撃を仕掛けることができます。このリリースには、対象の 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。

コンプライアンス レポート

2022 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。6 月にリリースされた 2022 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。

---

[3] WebInspect 21.2.0.117 以降のパッチで利用可能な OAST 機能が必要です。

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

2022 CWE Top 25

2022 CWE Top 25 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、誤検知の数を減らし、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。

Dynamic Code Evaluation: Unsafe Deserialization[4]

ID 11504 で識別されるチェックは、OAST 機能をサポートするペイロードを使用するように変更されました。このチェックの改善により、誤検知が減少し、結果の効率と精度が向上します。

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。

2022 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 2022 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。

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。

[4] WebInspect 21.2.0.117 パッチ以降で利用可能な OAST 機能が必要です。

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

2022 年 9 月 30 日