Press Release

2020 年 3 月 2 日

報道関係者各位

FOSSID AB
テクマトリックス株式会社
（東証一部 /証券コード：3762）

まったく新しい OSS セキュリティ脆弱性検出ツール「VulnSnippet Finder」の販売を開始

～セキュリティ脆弱性の原因となるコードスニペットを検出～

テクマトリックス株式会社（本社：東京都港区、代表取締役社長：由利孝、以下「テクマトリックス」）と、FOSSID AB（本社：スウェーデン ストックホルム、最高経営責任者：Oskar Swirtum、以下「FOSSID 社」、読み方：フォスアイディー）は FOSSID 社が開発した、OSS（オープンソースソフトウェア）のセキュリティ脆弱性検出ツール「VulnSnippet Finder」（読み方：ヴァルン スニペット ファインダー）について、日本国内での販売を開始することを共同で発表します。

現在のソフトウェア開発において、OSS（オープンソースソフトウェア）は不可欠な存在となりましたが、その一方で日々新しいセキュリティ脆弱性が報告されています。セキュリティ脆弱性を放置した場合、情報漏洩や Web サイト改ざんなど、企業に大きな打撃を与えるリスクが高まることが懸念されます。このようなリスクに対応するため、多くの企業では OSS のセキュリティ脆弱性対策の一環として、その利用を厳密に管理する取り組みを行っています。FOSSID 社も、OSS ライセンス&セキュリティ管理ツール「FOSSID」を提供し、企業における OSS の管理を支援してきました。

一般的な OSS 管理ツールのセキュリティ脆弱性検出の仕組みは、ソースコードに含まれるオープンソースコンポーネントを識別し、公開リポジトリ（最も一般的には「National Vulnerability Database（NVD）」）のセキュリティ脆弱性リストとコンポーネント単位で照会するものです。しかし、多くの場合、セキュリティ脆弱性に関連しているのはコンポーネント内の一部のファイルであり、さらにその中のたった数行のコードが原因であるため、コンポーネント単位で照会する従来の OSS 管理ツールではユーザーが使用していない部分のセキュリティ脆弱性についてもレポートがなされ、ユーザーは手動による仕分け作業に多くの時間を割かざるを得ない状況でした。

このたび販売を開始する「VulnSnippet Finder」は、コード行（スニペット）単位で FOSSID ナレッジベースと照合し、オープンソースコンポーネントや自社開発のソースコードに挿入されたオープンソースの一致個所を検索してセキュリティ脆弱性の原因になりうるコード行（スニペット）を検出します。これにより、企業はソフトウェアの中にある OSS のセキュリティ脆弱性を引き起こすコードスニペットを検出できるため、より正確に、迅速に OSS のセキュリティ脆弱性情報を確認することができます。

テクマトリックスと FOSSID 社は、以前より販売している OSS ライセンス&セキュリティ管理ツール「FOSSID」を「VulnSnippet Finder」と組み合わせた、より強固な OSS 管理ソリューションの販売、マーケティング、ユーザーサポートなどの活動を推進してまいります。

そして、FOSSID 社は今後も「FOSSID」と「VulnSnippet Finder」の機能拡張を重ね、企業の OSS 活用を支援してまいります。

最後に、FOSSID 社の最高経営責任者 Oskar Swirtum は、日本における「VulnSnippet Finder」のリリースに、次のようにコメントしています。「オープンソースソフトウェア（OSS）はエンジニアによるコードの統合やサプライチェーンからのコード納入によって社内に入ってきます。多くの場合、OSS セキュリティ脆弱性は OSS プロジェクト内の数行だけに依存します。FOSSID の VulnSnippet Finder（VSF）は OSS コンポーネントを脆弱にする特定の行を検知します。さらに、FOSSID の VSF は、特定バージョンの OSS コンポーネントが有するセキュリティ脆弱性をすべて提示するのではなく、該当するコード内に存在するセキュリティ脆弱性のみを提示します。この FOSSID の VSF の「OSS のセキュリティ脆弱性をコードレベルで検出する」機能は、おそらく、業界で初めての試みであり、OSS を利用している企業やプロジェクトのセキュリティ対策の一助になることを期待しております。」

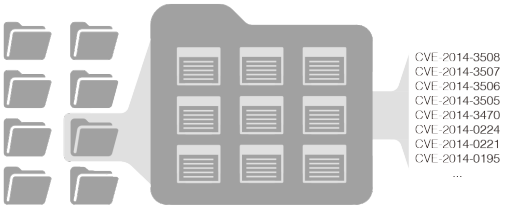
【VulnSnippet Finder の特長】

- **オープンソースをコード行（スニペット）単位で FOSSID ナレッジベースと照合**
  オープンソースをコンポーネント単位で公開リポジトリと照会する従来のセキュリティスキャナーと異なり、VulnSnippet Finder では、オープンソースをコード行（スニペット）単位で FOSSID ナレッジベースと照合し、オープンソースコンポーネントやソースコード内の一致個所を検索してセキュリティ脆弱性の原因になりうるコード行（スニペット）を検出します。そのため、従来のセキュリティスキャナーに比べて、より正確に、迅速に OSS のセキュリティ脆弱性情報を確認することができます。

  - **従来のセキュリティスキャナーとの違い**

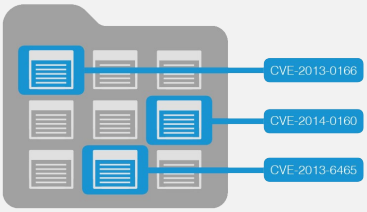
従来のセキュリティスキャナー

- コンポーネント／バージョンに基づいてセキュリティ脆弱性を想定
- 識別されたコンポーネントのバージョンが正しいことが前提。この前提が常に正しいわけではないため、誤ったセキュリティ脆弱性セットが報告される可能性がある
- コンポーネント全体が使用されていると仮定。実際には、オープンソースコンポーネントの一部（ファイルまたはスニペット）のみが使用される場合もある
- 既知の脆弱なコンポーネントに一致するすべてのファイルを警告（誤検出）



VulnSnippet Finder

- セキュリティ脆弱性の原因になる実際のコード行（スニペット）を検出
- 一致するオープンソースとして誤ったコンポーネントまたはバージョンを選択するなどのよくある人的エラーを排除
- 自社コードに挿入されたオープンソースも検出
- 誤検出を削減
- 派生物およびフォークの既知のセキュリティ脆弱性を検出



- **豊富なセキュリティ脆弱性データを含む FOSSID ナレッジベースと照合**
  National Vulnerability Database（NVD）に加えて、Bugzilla などのレポジトリもセキュリティ脆弱性情報のデータベースとして採用しています。

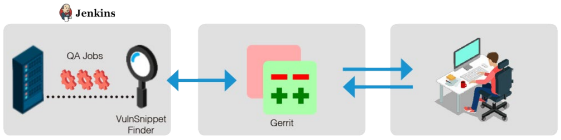
- **継続的インテグレーションに最適**
  特許取得済みの FOSSID スキャンエンジンおよびオープンソースナレッジベースへのアドオンであり、FOSSID のコマンドラインインターフェースから利用できます。コマンドひとつで脆弱なスニペットと照合し、該当コードをセキュリティ脆弱性の情報とともに JSON 形式でレポートされます。

例 1：ナイトリービルド時のスキャン

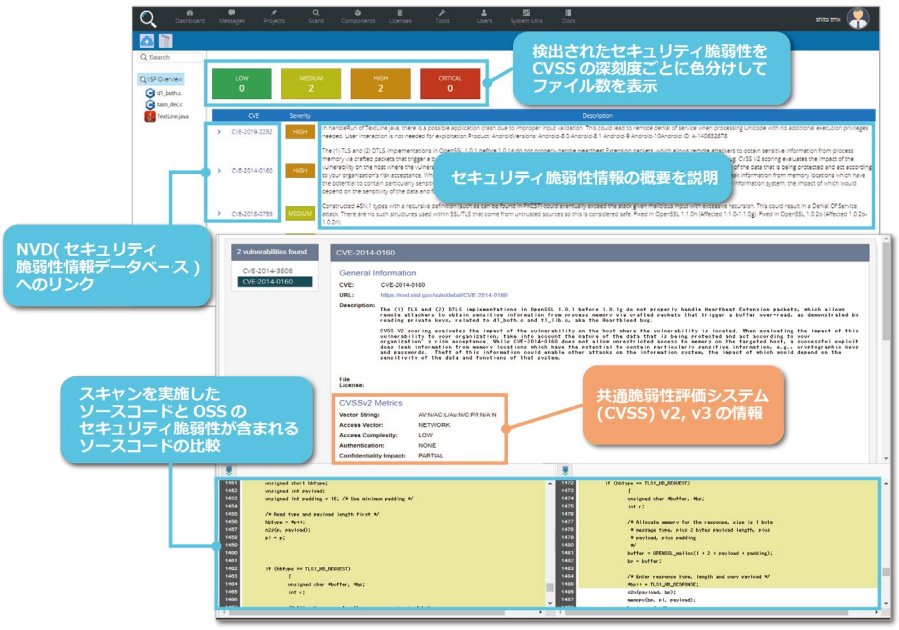
特定のブランチと FOSSID のナレッジベースに登録されたセキュリティ脆弱性のあるコードを比較し、セキュリティ脆弱性のあるコードが入り込んでいないかを夜間に検証

例 2：コミットアップロード時のスキャン

コミットされたコードと FOSSID のナレッジベースにある登録されたセキュリティ脆弱性のある
コードを比較し、セキュリティ脆弱性のあるコードが入り込んでいないかをマージする前に検証



- **FOSSID の GUI 上からスキャンが可能**
  FOSSID の GUI 上から、対象のソースファイルをドラッグ＆ドロップするだけで、スキャンを実行できます。これにより、開発者は OSS を製品に組み込む前の段階から、セキュリティ脆弱性を引き起こすコードスニペットの有無を確認することができます。（※VulnSnippet Finder と FOSSID のライセンスが必要です。）



【VulnSnippet Finder の販売について】

- VulnSnippet Finder は FOSSID 社が販売する OSS ライセンス&セキュリティ管理ツール「FOSSID」のオプション機能として販売します。ご希望のお客様には、「VulnSnippet Finder」単体でも販売可能です（VulnSnippet Finder のみの購入の場合、コマンドラインのみの提供です）。
- 販売開始日：2020 年 3 月 2 日
- 出荷開始日：2020 年 3 月 2 日

■FOSSID AB について

FOSSID AB は、オープンソース開発プラクティス、ライセンス コンプライアンスおよび特許保護の分野で豊富な経験を持つ、フリーおよびオープンソースソフトウェア（FOSS）、そしてライセンス管理に携わった起業家からなるチームであり、2001 年から活動しています。10 年以上にわたって多くの既存の FOSS 管理ツールを取り扱ってきた経験から、オープンソースの指数関数的な増大に対し既存ツールの限界を感じ、サービス品質とパフォーマンスを念頭に独自のナレッジベースの構築と検索アルゴリズムを開発、FOSSID をリリースし、2016 年に FOSSID AB を設立しました。
詳細は Web サイト： www.fossid.com/ をご参照ください。

■テクマトリックス株式会社について

テクマトリックス（東証一部：3762）は、クラウドコンピューティング時代に技術革新をもたらす情報基盤技術のインテグレーションを提供する「情報基盤事業」と、ソフトウェア開発のベストプラクティスを駆使してアプリケーション開発を行なう「アプリケーション・サービス事業」を展開しております。ソフトウェアエンジニアリング分野では、20 年にわたり、ソフトウェア品質向上をサポートする製品を海外より輸入し、日本国内に提供するためのローカライゼーション、コンサルティング、技術サポート、教育などさまざまな付加価値を付けてご提供しています。
詳細は Web サイト：www.techmatrix.co.jp/ をご参照ください。

＜本件に関するお問い合わせ先＞
テクマトリックス株式会社
ソフトウェアエンジニアリング事業部　FOSSID 担当
E-mail：fossid-info@techmatrix.co.jp
TEL：03-4405-7853