We bring security to life.

報道関係各位

2022/9/29
Trellix

※当資料は、米国時間2022年9月21日に米国で発表されたプレスリリースの抄訳です。

Trellix（トレリックス）、アドバンスト リサーチ センターを設立

35 万件（推計）のオープンソースプロジェクトが サプライチェーン脆弱性のリスクにさらされていると判明

XDR（Extended Detection and Response）の未来を提供するサイバーセキュリティ企業である Trellix は、本日、グローバルな脅威インテリジェンスを推進する、Trellix アドバンスト リサーチ センター（Trellix Advanced Research Center）の設立を発表しました。世界屈指のセキュリティアナリストや研究者ら数百人で構成される当センターは、実用的なリアルタイムインテリジェンスと脅威インテリジェンスの提供を通じ、お客様が最新のサイバーセキュリティ脅威を検知、対応、修復できるよう支援します。

Trellix の最高製品責任者（CPO）であるアパルナ・ラヤサム（Aparna Rayasam）は、次のように述べています。「脅威の状況は高度化するとともに、影響を与える可能性が拡大しています。私たちは、デジタルとフィジカルの世界を誰にとってもより安全なものにするために、この仕事をしています。敵対者は戦略的に人材と技術ノウハウに投資していますが、セキュリティ業界は最も攻撃的なアクターとその手法を研究し、イノベーションを加速させる義務があります。」

当センターは、サイバーセキュリティ業界で最も包括的な行動憲章を持ち、脅威の全体像から新たな手法やトレンド、攻撃者などを最前線で研究します。世界中のセキュリティ運用チームの主要なパートナーとして、当センターは、当社の主要な XDR プラットフォームを強化するとともに、セキュリティアナリストにインテリジェンスと最先端のコンテンツを提供します。

その他の情報は、**Trellix Advanced Research Center のブログ**および **Trellix 脅威センター**でご覧いただけます。

Python Tarfile の脆弱性がソフトウェアのサプライチェーンの複雑さを浮き彫りに

また、本日の発表に合わせて、当センターでは、35 万以上のオープンソースプロジェクトに存在し、クローズドソースプロジェクトにも蔓延していると推定される脆弱性である **CVE-2007-4559** に関する調査結果を発表しました。Python を使用するあらゆるプロジェクトのデフォルトモジュールである Python tarfile モジュールに存在し、Netflix、AWS、Intel、Facebook、Google が作成したフレームワークや、機械学習、自動化、Docker コンテナ化に使用するアプリケーションで広範囲で確認されました。この脆弱性は、2～3 行の簡単なコードで生成された不正なファイルをアップロードすることで悪用される恐れがあり、攻撃者に任意のコードの実行や、ターゲットデバイスの制御を許すことになります。

Trellix の敵対者・脆弱性研究（Adversarial & Vulnerability Research）責任者であるクリスチャーン・ビーク（Christiaan Beek）は、次のように述べています。「サプライチェーンの脅威といえば、一般的には SolarWinds で起きたようなサイバー攻撃を指しますが、脆弱なコード基盤をもとにした構築物も同様に、深刻な影響を及ぼす可能性があります。この脆弱性の広がりは、業界のチュートリアルやオンラインコンテンツの不適切な使用が拡散することで、さらに加速します。開発者は、過去

の攻撃対象領域を再び導入することをきちんと防ぐために、技術スタックの全レイヤーについて学ぶことが重要です。」

Python のようなオープンソースの開発ツールは、コンピューティングとイノベーションの発展のために必要であり、既知の脆弱性に対する保護には、業界の協力が必要です。Trellix は、オープンソースプロジェクトを脆弱性から保護するために、GitHub のプルリクエストでコードをプッシュするよう取り組んでいます。開発者が自分のアプリケーションに脆弱性があるかどうかを確認するための無償ツールを、**Trellix Advanced Research Center の GitHub** で公開しています。

参考情報

- **Trellix 脅威 センター**
- **Tarfile: Exploiting the World With a 15-Year-Old Vulnerability**
- **Open-Source Intelligence to Understand the Scope of N-Day Vulnerabilities**
- **Limiting the Software Supply Chain Attack Surface**
- **Trellix GitHub**

Trellix について
Trellix は、サイバーセキュリティの未来を再定義するグローバル企業です。オープンかつネイティブな Trellix の XDR（Extended Detection and Response）プラットフォームは、現在最も高度な脅威に直面するお客様が業務の保護や回復に確信を持って対応するための支えとなります。Trellix のセキュリティ専門家は、広範なパートナーエコシステムとともに、データサイエンスと自動化によりテクノロジーイノベーションを加速させ、4 万を超える企業や政府機関のお客様の力となっています。

Trellix アドバンスト リサーチセンター（Trellix Advanced Research Center）について
Trellix Advanced Research Center では、セキュリティの専門家と研究者のエリートチームが、洞察に満ちた実用的なリアルタイムインテリジェンスを作成し、お客様の業績や業界全体を推進するために活動しています。業界で最も包括的な行動憲章に基づき、熟練した研究者が市場に先駆けてトレンドを検知し、お客様やパートナーが新たな脅威に対処できるよう支援します。
詳しくは、**https://www.trellix.com/en-us/threat-center.html**

＜本情報のお問い合わせ＞
Trellix（McAfee Enterprise）
広報担当 戸田
Tel: 070-2680-0731
hiromi.toda@trellix.com

Trellix（McAfee Enterprise）広報担当
LaCreta 担当：野澤 / 近藤
Tel: 050-4560-2425
trellixjpn@lacreta.jp