PRESS RELEASE

2018 年 12 月 17 日

Tenable Network Security Japan K.K

データサイエンスチーム「Tenable Research」

Zoom で会議ハイジャックが起こり得る脆弱性を発見

～スレットアクターが攻撃対象のデスクトップを支配し、マルウェアをダウンロード・実行する恐れがある欠陥～

※本リリースは 2018 年 11 月 29 日（米国時間）に米国で発表されたプレスリリースの抄訳版です。原文は下記 URL を参照ください。

https://www.tenable.com/press-releases/tenable-research-discovers-vulnerability-in-zoom-that-could-lead-to-conference

企業の様々な情報資産の脆弱性を手間なく自動で可視化、改善するソリューションを提供する『Tenable Network Security』（以下：テナブル、所在地：メリーランド州コロンビア、代表：Amit Yoran （アミット・ヨーラン））が結成したデータサイエンスチーム「Tenable Research」は、Zoom のデスクトップ会議アプリ「CVE-2018-15715」において、遠隔攻撃者または不正出席者が画面制御をハイジャックし、チャットメッセージを通じて会議出席者になりすまし、出席者を会議から追い出せる重大な脆弱性を発見したと発表しました。この欠陥は、日常業務に Zoom を利用している世界中で最大 75 万社を危険にさらすものです。

デジタルトランスフォーメーションの波が押し寄せるにつれ、リモートワークの一般化がより進み、Zoom のような会議サービスを至る所で見かけるようになりました。Zoom は新たな会議室となり、組織が機密情報を扱う会議でも利用され、クラウド上で通話の記録や保管もできるようになりました。このような脆弱性に対してのエクスプロイトは、幹部や顧客が参加する会議、今後の見通し会議といった重要な話し合いを Zoom にて行っている組織に深刻なレピュテーションリスクが生じさせます。

悪質なスレットアクターは脆弱性を以下のように利用します。

1. **画面制御ハイジャック**：遠隔出席者がスクリーン共有をする間に画面制御許可を迂回し、被害者のデスクトップを完全制御し、攻撃者によるマルウェアのダウンロード・実行機会を与える。
2. **なりすましチャットメッセージ**：会議に出席している他人に成りすまし、チャットメッセージを送る。
3. **会議から出席者を追い出す**：主催者以外の出席者が他の出席者を追い出したり締め出したりする。

【米国テナブル社 Renaud Deraison 氏（最高技術責任者・テナブルの共同創始者）のコメント】

「昨今のデジタル経済においてビジネスを行うには、組織は新しい技術やサービスを取り入れていく必要があります。しかし、新たな技術投資には新たな攻撃による危険がつきものです。今回の脆弱性は、Zoom のように一見無害に思えるサービスによってサイバー・アタックサーフェスが生じるという典型的な例です。テナブル・リサーチは、消費者や事業者が依存しつつある技術の安全性を確保するため、脆弱性の発見およびベンダーとの提携に尽力します。」

テナブルは、「脆弱性に関する情報開示方針」に概要が記載されている標準手法に従い、Zoom の脆弱性を発見しました。この脆弱性は、macOS と Windows 用の Zoom（バーション 4.1.33259.0925）と、Ubuntu 用 Zoom（バージョン 2.4.129780.0915）の両方に影響を及ぼします。Zoom 社は迅速な対応を行い、この脆弱性を修正するため、Windows 用バージョン 4.1.34814.1119 と macOS 用バージョン 4.1.34801.1116 をリリースしました。各ユーザーは、デスクトップ会議アプリが最新版になっていることを至急ご確認ください。

さらに、テナブルは各組織が脆弱性評価を実施するためのプラグインを発表しました。macOS 用プラグインの詳細はこちらを、Windows 用プラグインの詳細はこちらをクリックしてください。詳細はテナブル・リサーチ・アドバイザリーのブログ投稿をご参照ください。

【米国テナブル社プロフィール】

Tenable Network Security は、世界中の 24,000 社を超える組織に対し、総合的なセキュリティソリューションにより、将来のビジネスニーズに合わせてそのテクノロジーを変革し、企業組織の情報保護に向けた有効的な対策を提供しています。Nessus®を開発した Tenable は、脆弱性対策の技術をさらに発展させることで、あらゆる情報資産やデバイスの脆弱性を管理、保護できる世界初のセキュリティプラットフォーム「Tenable.io®」を展開。Tenable のセキュリティプラットフォームは、米国ビジネス誌 Fortune が選定する『Fortune 500』（総収入に基づいた全米上位 500 社）に選ばれている企業の 53%、世界の有力企業 2000 社の 29%に導入されています。詳細は tenable.com へ

【米国テナブル社企業概要】

商号： Tenable Network Security
代表： Amit Yoran アミット・ヨーラン
住所： 7021 Columbia、
Gateway Drive Suite 500 Columbia,
MD 21046

【テナブル社企業概要】

商号：Tenable Network Security Japan K.K.
住所：東京都千代田区丸の内 2-3-2
郵船ビルディング 1 階