PRESS RELEASE

2019 年 5 月 27 日

Tenable Network Security Japan K.K

データサイエンスチーム「Tenable Research」

Slack のダウンロードハイジャック脆弱性を発見

～企業の情報流出や情報改竄の危険性につながるサイバーリスクの恐れ～

※本リリースは、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-discovered-a-download-hijack-vulnerability-in-slack

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、ビジネスチャットサービス「Slack」の Windows 用デスクトップアプリケーションの脆弱性を発見したことを発表しました。攻撃者にこの脆弱性を悪用されると、ユーザーが Slack 内でドキュメントをダウンロードした際に、ファイルの格納先を変更することで、情報を不正に入手・改竄される可能性があります

※今回の脆弱性はバージョン 3.3.7 において発見されました

Slack は多くの企業が従業員間の連絡を密にするための重要なツールとなっています。攻撃者は、巧妙に作ったハイパーリンクを Slack のメッセージを通して送信することで、ドキュメントのダウンロード先を、攻撃者の所有するサーバーへと変更することができます。この脆弱性を悪用して、攻撃者は Slack の中でダウンロードしたドキュメントを不正に入手するだけでなく、ファイルに悪質なコードを埋め込むなど、被害者のデバイスを危険にさらすような操作もできてしまいます。

【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】

「デジタル経済の到来と労働力が世界中に分散したことによって、シームレスなつながりを求める新しい技術が市場において発展してきました。しかし、この新たな技術には脆弱性が伴う可能性があり、攻撃の対象が拡大し続けていることを、組織は認識する必要があります。テナブル・リサーチは、Slack などのベンダーと共同して、顧客と組織の安全を守るために、脆弱性に関する最新情報を引き続き公開していきます。」

Slack はこの脆弱性に対応したバージョン 3.4.0 をリリースしました。ユーザーは、Windows 用 Slack がこの最新バージョンに更新されているか至急ご確認ください。

【米国テナブル社プロフィール】

Tenable Network Security は、世界中の 27,000 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、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を展開。Tenable のセキュリティプラットフォームは、大規模行政機関ならびに、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)に選ばれている組織の 50%以上、世界の有力組織 2000 社の 25%以上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 1-6-5
丸の内北口ビルディング 9 階