PRESS RELEASE

2019 年 4 月 22 日

Tenable Network Security Japan K.K

データサイエンスチーム「Tenable Research」
Verizon ルーターの脆弱性を発見
～数百万人にのぼるユーザーにサイバーリスクの恐れ～

※本リリースは 2019 年 4 月 9 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/new-vulnerabilities-in-verizon-routers-expose-millions-of-consumers-according-to

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、Verizon Fios Quantum Gateway ルーターに複数の脆弱性を発見したことを発表しました。攻撃者は、この脆弱性を悪用することで、ルーターのネットワークを完全に支配し、接続されているデバイスの可視性をコントロールすることができてしまいます。Verizon のルーターはアメリカの家庭で広く使用されており、接続されている数百万台のデバイスが危険にさらされています。

スマートホームの普及によって、こういった家庭用に使われている一般的なルーターがサイバー攻撃の最大の標的となっています。Tenable Research が直近で検出した脆弱性（CVE-2019-3914, CVE-2019-3915 及び CVE-2019-3916）は、ホームセキュリティーシステムのような、ルーターに接続されたスマートデバイスも攻撃シナリオ数種につながる対象となり、遠隔操作でセキュリティ機能を欠落させてしまう恐れがあります。攻撃者はデバイスの安全設定を改ざんし、ファイアウォール規則を変更、またはペアレンタル・コントロールを解除することができてしまいます。また、インターネット上のトラフィックを嗅ぎ付け、攻撃対象のオンラインアカウントを危険にさらし、銀行口座の詳細を盗み、そしてパスワードを読み取ることも可能です。

【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】

「ルーターは各スマートホームにとって中心的なハブとなっています。利用者をインターネットの上のあらゆる場所につなぎ、家庭の安全を守り、遠隔操作でドアの開錠もできます。しかしルーターは、現代の家庭のセキュリティ機能の深部への実質的な入り口ともなっており、出ていくものだけでなく、入ってくるものもコントロールしている非常に重要な役割を担っています。」

Verizon は、ファイアウォールをバージョン 02.02.00.13 にアップデートすることで、今回の脆弱性に対応することができると発表しました。また、利用者は所有するデバイスがこのバージョンに更新されているかを早急に確認し、疑問点は同社に問い合わせるよう呼び掛けています。

【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 2-3-2
郵船ビルディング 9 階