報道関係各位

2018 年 5 月 9 日

Tenable Network Security Japan K.K

データサイエンスチーム「Tenable Research」 FBI と国土安全保障省による前例のない警告に続き、重要インフラの脆弱性を発見 シュナイダーエレクトリック社のシステム脆弱性により、 IT とオペレーショナル・テクノロジー（OT）システムが無制限攻撃を受ける可能性を示唆

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、製造業、オイル・ガス、水、自動化、風力、太陽熱発電設備に多用されるシュナイダーエレクトリック社のアプリケーション 2 つに、リモートコード実行による重大な脆弱性を発見し、サイバー犯罪者がその脆弱性を利用した場合、基幹システムが完全に制御されてしまう恐れがあることを発表しました。

攻撃者が欠陥システムを利用してネットワーク内を自在に動き回り、ヒューマン・マシン・インターフェース（HMI）クライアントおよびその他のシステムを攻撃することが可能になり、最悪の場合、攻撃者が脆弱性を利用して工場の稼働を混乱させ、機能不全に陥らせるといった可能性もあります。

※本リリースは 2018 年 5 月 2 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/following-unprecedented-fbi-and-department-of-homeland-security-warning-tenable

今回発見した脆弱性は、米国の重要インフラに対するロシア国家主導の攻撃に対し、合同警告（warning）を国土安全保障省とFBIが発表したわずか数週間後に発見されました。合同警告で強調されたように、OTシステムは世界中のサイバー犯罪における高価値ターゲットとなっているため、人的安全性、継続的な生産性、アップタイム、効率性が大きな懸念事項となっています。同時に、重要インフラのデジタル化に対して、サイバーセキュリティ対策の展開は遅れをとっているため、サイバーセキュリティ・リスクが常に存在し、これが非常に大きなサイバー・エクスポージャー・ギャップとなっていることを正しく理解し行動できていないという深刻な不能状態に陥っています。

Tenable Research が発見した脆弱性は、HMI や監視制御データ取得（SCADA）システム、および OT とインターネットや社内イントラネットを接続する組込式計測ソリューション開発のために使用される自動ツール「InduSoft Web Studio」や、スケーラブル HMI クライアントである「InTouch Machine Edition」に影響を及ぼします。このソフトウェアは製造業、オイル・ガス及び自動車などの重工業数社の間で一般に普及しており、産業分野で分散型遠隔モニタリングの導入が進むにつれ、OT と IT は一点集中化しつつあります。OT がより多く接続されて境界がなくなるにつれ、これらの重大安全システムのサイバー攻撃に対する脆弱性はますます高まっていきます。

リモートアクセスする署名のない攻撃者は、この脆弱性を利用して脆弱システムに任意コードを実行し、「InduSoft Web Studio」や「InTouch Machine Edition」のサーバーマシンを最大の危機に晒す恐れがあります。攻撃者が欠陥マシンを利用して被害者ネットワーク内を自在に動き回り、さらなる攻撃を実行する恐れもあります。

Tenable Research は責任を持って脆弱性を公表するため、ベンダーと共に取り組んでおり、シュナイダーエレクトリック社は、影響を受けた両システム用のパッチを公開しました。OT 市場で影響を受けたソフトウェアの広範な普及状況とマーケットシェアを考慮した早急な対応、およびユーザーレスポンスが求められています。

【米国テナブル社 Dave Cole 氏（最高プロダクト責任者（CPO））のコメント】

「デジタルトランスフォーメーションによって重要インフラへのアクセスが可能となり、隔離システムが外部ネットワークと接続されました。このシュナイダーエレクトリック社の脆弱性の問題は、我々の生活圏にパワーを供給する基幹システムに深刻な被害を与えたいサイバー犯罪者に、アクセスの機会を与える恐れがあるという意味で特筆すべき事象です。Tenable Research はクラウド、IT、IoT、OT など、現代のコンピュータ環境において、業界の総合的なサイバー・エクスポージャー全般を評価・分析・低減することを目的としています。この拡大する問題の解決には、業界全体の結束が必要です。シュナイダーエレクトリック社がこの重大な問題の修正パッチを早急に公開したことを喜ばしく思います。」

※脆弱性に関する追加情報は、Tenable Research Advisory の下記ブログ記事を参照ください。

https://jp.tenable.com/blog/tenable-research-advisory-critical-schneider-electric-indusoft-web-studio-and-intouch-machine

【米国テナブル社プロフィール】

Tenable Network Security は、総合的なセキュリティの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。Tenable はセキュリティの脆弱部分を解消し、脅威に優先順位を付け、エクスポージャーと損失を削減します。世界中に 100 万人以上のユーザーと 2 万社を超える法人顧客をもつ Tenable は、裏付けのあるセキュリティ・イノベーションによって企業から信頼を得ています。

【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