PRESS RELEASE

2019 年 1 月 22 日

Tenable Network Security Japan K.K

データサイエンスチーム「Tenable Research」

大手ビルセキュリティシステムに複数のゼロデイ脆弱性を発見

～偽造バッジを作成して施錠システムをハッキングされる可能性～

※本リリースは 2019 年 1 月 14 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/multiple-zero-day-vulnerabilities-discovered-by-tenable-research-in-building-access

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、IDenticard が開発した PremiSys™のアクセスコントロール・システムに複数のゼロデイ脆弱性を発見したことを発表しました。最も深刻な脆弱性を悪用すれば、攻撃者は自由にバッジシステム・データベースにアクセスが可能になり、偽造バッジを作成して施錠システムを操作することで、ビル内に侵入することができてしまいます。IDenticard は世界中に数万社以上の顧客を持っており、その中にはフォーチュン 500 企業、K-12 教育機関、大学、医療施設、および政府機関も含まれます。

現代の企業は、ワークステーション、社内サーバーからビル警備システムやスマート機器に至るまで、従来および最新のアセットから構成される非常に複雑なデジタル・インフラを構築しています。インフラが複雑化されていくこの状況において、企業のセキュリティ・チームは、ダイナミックな企業環境下で安全なネットワークを構築することがさらに困難になっています。PremiSys™のゼロデイ脆弱性はその顕著な例であり、新技術の大量導入により物理的安全性とデジタル上の安全性の間の線引きが曖昧になってきています。テナブル・リサーチがこの脆弱性を発見したのは、監視カメラソフトウェア Peekaboo のゼロデイ脆弱性を発見してからわずか数カ月後のことでした。

PremiSys™の技術は、ドア・アクセスの権限付与を操作できる他、設備を施錠したり、内臓カメラで録画した動画データを確認することができます。攻撃者が最も深刻な脆弱性をエクスプロイトした場合、PremiSys Windows Communication Foundation (WCF) サービスのエンドポイントを経由し、バッジシステム・データベース全体への管理者アクセスが可能となります。攻撃者はこの管理者権限を利用して、システムデータベースのあらゆるコンテンツのダウンロード、書き換え、ユーザー削除など、様々なアクションを実行できてしまいます。

【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】

「デジタル時代が到来したことで、IoT の導入も相まって、サイバー世界と現実世界は一体化しつつあります。組織のセキュリティ範囲は、もはやファイア・ウォールやサブネット、または物理的範囲にとどまらず、境界が無くなっています。このため、セキュリティ・チームは、自身の情報資産におけるサイバー・エクスポージャーを完全に可視化することが非常に重要です。残念ながら、IoT という新世界における製造業者の多くは、パッチが適用されていないソフトのリスクを完全には理解していないことから、消費者や企業はサイバー攻撃の脆弱性に晒されています。今回の例では、アクセス管理に PremiSys™を導入している組織は膨大なリスクにさらされています。今回の例に限らず、セキュリティ業界は、エンベデッド・システムとその後の保守に関する幅広い議論を行う必要があります。デジタル・インフラはますます複雑化しており、その管理方法もまた同様です。我々は、セキュリティ・パッチを迅速かつ完全自動化された方法で確実に供給してくれるベンダーを必要としています。テナブル・リサーチは消費者と組織の安全を等しく確実に守るため、協調開示に賛同するベンダーと連携しています。業界の連携は、消費者のエクスポージャーリスクを管理・測定・軽減する上で非常に重要です。」

テナブル・リサーチは、脆弱性の開示方針に記載されている標準手法に基づき、IDenticard のバージョン 3.1.190 における脆弱性（CVE-2019-3906, CVE-2019-3907, CVE-2019-3908, CVE-2019-3909）を開示しました。IDenticard は、問題の解決に取り組んでいるものの、現在もパッチは公開されていません（2019 年 1 月 17 日時点）。被害リスクを軽減するには、ユーザーは自社ネットワークを切り放し、PremiSys™のようなシステムを内外の脅威からできるだけ隔離するといった対策を確実に実行する必要があります。

【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、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 1 階