protiviti®
Face the Future with Confidence

IoT デバイスセキュリティの脅威

シンガポール工科デザイン大学の研究者により、無数のIoTデバイスに重大なセキュリティ脆弱性（サイバー攻撃を受ける可能性が有る弱点）が有ることが発見されました。

2020
2月28日

高まるIoTデバイスの脆弱性

このセキュリティ脆弱性は「Bluetoothに関する脆弱性」で、480以上のIoTデバイスに含まれている大手ベンダー7社のシステムオンチップ（SoC）[1]に12個発見されました（全てのケースを網羅的に調査していないため、実際はより多くの、数千のデバイスが影響を受けている可能性があります）。これらのシステムオンチップは世界で最も使われているものの1つであるため、多くの組織で使われている無数のIoTデバイスがサイバー攻撃に対して脆弱であり、デバイスのデッドロックやクラッシュ、バッファオーバーフローが引き起こされたり、特定のセキュリティ設定が回避されたりする可能性があります。

プロティビティは、自社のセキュリティラボにてこの「Bluetoothに関する脆弱性」の調査を行い、それらが深刻かつ確かな脅威であることを検証しました。以下は、影響を受ける可能性が有るデバイスの一例です。

- 医療機器
- ビル管理システム
- セキュリティシステム
- 自動車機器
- 照明機器
- スマートホーム製品
- 家電

また、研究者によって、この「Bluetoothに関する脆弱性」の証明としてエクスプロイトコード（脆弱性がどのように悪用されるかを実証したコード）を公開しました。これにより、サイバー犯罪者がこれらの脆弱性を悪用しようとする可能性が一層高まっています。企業は自社内に設置されているIoTデバイスの影響を直ちに見極めるための措置を講じ、影響を受けるIoTデバイスが発見された場合は、セキュリティパッチの適用や脆弱性が悪用されるリスクを軽減する措置を実行する必要があります。

この「Bluetoothに関する脆弱性」は、システムオンチップ内のBluetooth Low Energy（BLE）に影響します。BLEとは、スマートフォンやiPad等のユーザーデバイスおよびIoTデバイスで実装されている、無線通信（範囲：10~20メートル）です。特定された脆弱性により、デバイスのデッドロックやクラッシュによって強制再起動が引き起こされることから、デバイス上の設定や機能の仕様が変更され、攻撃者がデバイス間の機密データ通信を窃取する等、さまざまな影響が考えられます。特に医療機器が影響を受けた場合、人々の健康や安全に重大な影響を与える可能性が高くなります。

企業はどうすべきか

Bluetooth対応のIoTデバイスを利用または製造する企業は、影響を受けるシステムオンチップを特定すると共に、本研究結果を確認し、必要なアクションを行うことが求められます。推奨される対策は以下の通りです。

- IoTデバイスの棚卸しを行い、影響を受けるチップが内蔵されているデバイスの有無を確認する。
- デバイスのベンダーに連絡し、そのデバイスが脆弱性の影響を受けているか確認する。
- BLE機能を備えたデバイスの場合、必要性とビジネスへの影響度の観点から優先順位付けを行ったうえで、BLE機能を無効化できるか判断する。
- BLE機能を無効化できない場合は、デバイスベンダーに、セキュリティパッチのリリース状況およびセキュリティパッチの適用方法を確認する。

1 System On Chip：装置やシステムを動かすために必要な機能の多くを半導体チップに実装する方式

- セキュリティパッチを適用できず、かつ脆弱性の影響を受けるシステムについては、デバイスへの物理的アクセスを制限するなどの代替対策を講じて、攻撃者がBLEの範囲に侵入できないようにする。

- これらのデバイスに異常な動作や通信が発生しないかを監視し、サイバー攻撃を認識できるよう利用者への周知徹底を行う。

本研究により、特定のシステムオンチップを内蔵するIoTデバイスのセキュリティについて、迅速な確認および管理が必要であること明らかになりました。IoTデバイス分野におけるセキュリティ戦略の必要性が一段と高まっています。IoTデバイスの活用が普及し、ビジネスにおいてこれらのデバイスがより多く使用される一方、IoTデバイスのセキュリティに対する理解が十分でないことに留意することが重要です。

企業は、環境内のIoTデバイスに対する管理やメンテナンス、デバイスやデータの保護、および破棄を実行するためのIoT戦略を策定する必要があります。この戦略には、デバイスの調達から破棄までの全ライフサイクル管理を含める、主要な対策である資産管理、セキュリティ設定および更新、通信の安全性とモニタリング、インシデント発生時の復旧やデバイスの破棄を網羅しなければなりません。IoTデバイスもリスク評価対象とし、適切なリソースを割り当てることで、新たなテクノロジーが組織に与えるビジネスリスクを管理可能とすることが重要です。

プロティビティの支援内容

IoTデバイスを使用または製造する企業は、以下の質問項目への対応を検討する必要があります。

- 組織内で使用されているIoTデバイス資産の一覧はありますか。

- これらのデバイスの潜在的な脅威の特定、および異常な動作や通信の監視を行えますか。

- セキュリティの脆弱性が特定された場合、IoTデバイスの更新を行う計画およびスキルを有していますか。

- IoTデバイスが組織にもたらすセキュリティとリスクを管理する統制はありますか。

- 技術的およびビジネス復旧計画はありますか。

プロティビティは、IoTデバイスやテクノロジーにより引き起こされる技術的およびビジネスリスクを理解し管理できるよう、企業を支援します。管理基準の策定やデバイスのテスト、IoTデバイス資産ライフサイクル管理、モニタリング、復旧計画等、これらのデバイスがもたらすリスクの管理計画の立案および展開を支援します。

protiviti®