報道関係者各位

エフセキュア、KeyWe 社製スマートロックの脆弱性について警告

～ 増加する IoT デバイスにおいて、「スマート」と「セキュア」の両立は困難 ～

2019 年 12 月 12 日
エフセキュア株式会社

先進的サイバー・セキュリティ・テクノロジーのプロバイダである F-Secure (本社: フィンランド・ヘルシンキ、CEO: Samu Konttinen、日本法人: 東京都港区、以下、エフセキュア) は、攻撃者が簡単にピッキングできるスマートロックの設計上の脆弱性を、同社のセキュリティコンサルティング部門である F-Secure Consulting が発見したと発表しました。ファームウェアの更新ができない IoT デバイスがその脆弱性を完全に修正できない場合、そうしたデバイスがインターネットに接続される際に、デバイスメーカーやユーザに対して大きな問題をもたらすこととなります。

KeyWe 社が市場で展開している KeyWe Smart Lock は、主に個人の住宅で使用されるリモート制御のエントリデバイスであり、ユーザはスマートフォンのアプリでドアの開閉ができます。F-Secure Consulting は、通信プロトコルの設計における脆弱性により、物理デバイスとモバイルアプリの間で交換されるロックを制御する秘密のパスワードが傍受されてしまうことを発見しました。

今回の脆弱性発見に関わったエフセキュアのサイバーセキュリティコンサルタントである Krzysztof Marciniak (クリストフ・マーシニアック) は述べています。
「スマートロックにはいくつかの保護メカニズムがありますが、設計上の不備により、これらのメカニズムをバイパスして、ロックとアプリとの間で交換されるメッセージを攻撃者が簡単に傍受でき、比較的単純と言える攻撃に対して脆弱な状態となります。しかし、これを防御する方法はないのです。そのため、スマートロックで保護された住居に簡単に侵入することができてしまいます。何度も、簡単にです。攻撃者にとって必要なのは、わずかなノウハウ、家電量販店でたった 10 ドルで購入できるトラフィックをキャプチャするためのデバイス、そして誰がこのスマートロックを使用しているかを見つけるためのほんの少しの時間です。」

多くの IoT デバイスが市場に出回っているなか、これはメーカーとユーザが直面しているセキュリティ上の問題の一つに過ぎません。最近のリサーチでは、2025 年までに推定 1,250 億台のデバイスがインターネットに接続されるだろうと考えられています。[*1] IoT デバイスの普及に伴い、より多くのセキュリティ上の懸念が浮上してきます。

[*1] https://www.techradar.com/news/rise-of-the-internet-of-things-iot

スマートロックには通常、権限を持たない第三者が秘密のパスワードなどのシステム上の重要な情報にアクセスすることを防ぐためのデータ暗号化など、いくつかの便利なセキュリティ機能が搭載されています。しかし、F-Secure

Consulting は、この KeyWe 社製スマートロックのセキュリティ対策を回避できてしまう、比較的簡単な方法を発見しました。そして、デバイスがファームウェアの更新を受信できないため、見つかった脆弱性を修正することはできません。スマートロックのユーザはロックそのものを交換するか、侵入されるリスクに耐えるかを選択しなければなりません。

Marciniak は、セキュリティは正しく実装された場合にのみ機能すると指摘しています。これは、全ての IoT デバイスメーカーが理解する必要がある、重要かつ微妙な点です。
「全てのデバイスや企業に共通して保護を提供する『フリーサイズ』のセキュリティサービスなどありません。ユーザ、使用環境、潜在的脅威モデルなど様々な要素を考慮して導入する必要があります。これを実行するのは簡単ではありませんが、IoT デバイスメーカーがファームウェアの更新ができない製品を出荷する場合、設計段階からセキュリティについて意識する必要があります。」

Marciniak はまた、元々オフラインデバイスだったものをオンラインバージョンに置き換える前に、インターネット接続におけるセキュリティの懸念に広く消費者に認識してもらうことと、デバイスメーカーが設計の一環として製品のセキュリティ評価を実施することを強く勧めています。

今回発見した KeyWe 社製スマートロックの具体的な脆弱性にはユーザが実行できる対策がなく、また、攻撃者が簡単にその脆弱性を利用できてしまうため、エフセキュアでは重要な技術的詳細の発表を差し控えることとしました。ただし、詳細情報を含むアドバイザリーとブログ投稿は F-Secure Labs ページに掲載しています。また、デバイスメーカー向けの追加のサポートとサービスは、F-Secure Consulting ページよりご覧いただけます。F-Secure Consulting は 4 大陸 11 ヶ国に拠点を構え、銀行、金融サービス、航空、海運、小売、保険、その他セキュリティがクリティカルとなる分野において、高度なサイバーセキュリティコンサルティングサービスを提供しています。

KeyWe 社製スマートロックに関するアドバイザリー
https://labs.f-secure.com/advisories/keywe-smart-lock-unauthorized-access-traffic-interception（英語）
http://jp.press.f-secure.com/2019/12/12/keywe-smartlock-jp/（日本語）
F-Secure Labs:
https://labs.f-secure.com/
F-Secure Consulting:
https://www.f-secure.com/en/consulting

エフセキュアについて

エフセキュアほど現実世界のサイバー脅威についての知見を持つ企業は市場に存在しません。数百名にのぼる業界で最も優れたセキュリティコンサルタント、何百万台ものデバイスに搭載された数多くの受賞歴を誇るソフトウェア、進化し続ける革新的な人工知能、そして「検知と対応」。これらの橋渡しをするのがエフセキュアです。当社は、大手銀行機関、航空会社、そして世界中の多くのエンタープライズから、「世界で最も強力な脅威に打ち勝つ」という私たちのコミットメントに対する信頼を勝ち取っています。グローバルなトップクラスのチャネルパートナー、200 社以上のサービスプロバイダーにより構成されるネットワークと共にエンタープライズクラスのサイバーセキュリティを提供すること、それがエフセキュアの使命です。
エフセキュアは本社をフィンランド・ヘルシンキに、日本法人であるエフセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。詳細は https://www.f-secure.com/en/welcome（英語）および https://www.f-secure.com/ja_JP/（日本語）をご覧ください。また、Twitter @FSECUREBLOG でも情報の配信をおこなっています。

※以下、メディア関係者限定の特記情報です。個人の SNS 等での情報公開はご遠慮ください。

【本件に関する報道関係者からのお問合せ先】

エフセキュア株式会社
PR マネージャ:　秦　和哉
TEL：03-4578-7745（直通）　　japan-pr@f-secure.com