KeyWe 社製スマートロックに関するアドバイザリー

脆弱性の概要

KeyWe 社製スマートロックは、複数の設計上の欠陥のために (潜在的に悪意のある) 不正なアクターが正規のユーザからのトラフィックを傍受して解読ができてしまいます。次に、このトラフィックを使用して、所有者に代わってロックの開閉、サービス拒否、ロックのサイレンシングなどのアクションを実行することができます。

正規のアプリケーションとスマートロック間の通信メッセージは、Bluetooth Low Energy を使用して転送されます。送信前に、AES-128-ECB を使用してランダムな 2B (2 バイト) プレフィックス (初期化ベクターの代わりとして機能) を使用して暗号化されるため、第三者が正規のユーザから発信されたコマンドを簡単に盗聴したり改ざんしたりすることはできません。ただし、キー生成プロセスは重大な欠陥の影響を受けます。

KeyWe が現在使用しているメッセージングチャネルのセキュリティは、次の 2 つの要因に依存しています。

●鍵交換を開始するために使用される共通鍵
●アプリ／スマートロック (ドア) キーの計算プロセス

F-Secure は、これらの制約の両方を克服できることを証明しています。まず、共通キーはグローバルに利用可能なデバイスアドレスに基づいて作成されるため、ネゴシエーションの最初の段階を簡単に解読できます。次に、モバイルアプリケーションからキー生成プロセスを取得できます。

アプリケーションは難読化と root 検出を利用して、デバイスを標的とする脅威からユーザをプロテクトすることに注意してください。ただし、ソリューション全体は、その数や品質に関係なくそのようなプロテクションを克服することができる (またはする) 意志のある攻撃者が標的にすることができます。

通信

スマートロックを使用する前に、デバイスを登録する必要があります。登録プロセスは 3 つのフェーズから成り立っています。

フェーズ 1: 登録が必要かどうかを確認するためのロックモードの設定
フェーズ 2: デバイスのパスワードの登録 (以下、EKEY)
フェーズ 3: EKEY 値の検証 (認証と承認)

デバイスが認証／承認ステップを正常に通過すると、スマートロックの開閉などの追加の操作が許可されます。前述の各フェーズは、いくつかの追加ステップで構成されています。

最初に、デバイスの Bluetooth アドレスに基づく共通キーが計算されます。双方は、計算されたキー (以下、comm) を使用して、次に示すように、任意の 12B (12 バイト) 値を暗号化してから、相手側に送信します。

app num
app --[comm(12B value)]-> door
door num
app <-[comm(12B value)]-- door

番号が交換されると、双方は自身と相手のキーを計算します：

door_key = make_door_key(app_num, door_num)

app_key	= make_app_key(app_num, door_num)

このハンドシェイクと呼ばれる通信は次のとおりです。

app <-[	door(Hello)]-- door
app --[	app(Welcome)]-> door
app <-[	door(START)]-- door

ハンドシェイクが終了すると、EKEY 検証コマンドを含む追加のメッセージが続きます。

影響

ドア／キーの生成はカスタムアルゴリズムに基づいていますが、前述のように取得し、比較的低コストでリバースエンジニアリングが可能です。したがって、悪意のある攻撃者が約 15 メートルの有効範囲内にある限り、上記の説明と同様にトラフィックを傍受および解読できます。

通信傍受も比較的低コストで実行できます。例えば、BLE 通信を可能にする nRF51822 チップは 5 ドル以下で購入できます。

EKEY 値が取得されると、攻撃者は正規のユーザができるあらゆるアクションを実行できます。これは、元のアプリケーションがデバイスに登録されている限り可能です。さらに、EKEY 値はオンラインレンダリングで保存されるため、そのような攻撃を克服するには、モバイルデバイスを変更するだけでは不十分です。

デバイスをオンラインで登録／使用しない (つまり、機械的なロックとしてのみ使用する) という稀なシナリオでは、悪意のある攻撃者は追加の対話なしでスマートロックを乗っ取り、操作できます。機械的な部品はロック機構を操作するサーボ機構に依存しているため、これも完全な侵害を招きます。

対策

執筆時点では、この問題への対策はありません。唯一の方法は、エンドユーザにとっては不便ですが、スマートロックから可能な限り離れたモバイルデバイスをペアリングし、物理的なキー／タッチパッドのみを使用することです。