

IronKey USB フラッシュドライブから、BadUSB 保護を 入手してください

IronKey™ および DataTraveler® Secure USB デバイスは、2016 年 8 月開催の The Black Hat conference 会議で明らかにされた BadUSB マルウェアに対して脆弱ではありません。BadUSB は、デバイス内のデータを攻撃するのではなく、デバイス自体を攻撃するようにデザインされた最初の USB マルウェアです。すべてのコントローラファームウェア内でデジタル署名を用いるものも含め、IronKey のセキュリティにおけるリーダーシップにより、この新たな脅威に対してその製品は免疫を持ちます。

BadUSB に関する Black Hat セッションで明らかのように、その攻撃は USB ハードウェアの挙動を制御するファームウェアを書き換えて、USB デバイス側をホストとして動作させます。その後、他のコンピュータや USB デバイスに感染していきます。コントローラファームウェアの書き換えは今日のマルウェア対策手法によって検出することはできず、多くの場合は、検出不能のまま残ることとなるでしょう。

研究者たちが説明するように、この脆弱性に対する最善の保護策は、ファームウェア更新用のコード署名を使用することです。署名されたファームウェアが変更された場合、デバイスはファームウェアを認証することができず、動作しません。その結果、デバイスは使用不能になり、感染の拡大が防止されます。署名されたファームウェアの使用に加えて、IronKey はハードウェアベースのセキュリティキーを用いてファームウェアを更新するメカニズムを保護します。これにより署名されたファームウェアで改ざんを防止し、デバイスは使用不能になります。

その他の特徴

その他のセキュリティ機能 IronKey および DataTraveler Secure USB ドライブに利用可能。

- セキュアな軍用グレードの 256 ビット AES フルディスクハードウェアの暗号化
- FIPS (連邦情報処理規格) 140-2 レベル 3 検証済み
- 一元化管理リモートワイプ対応/紛失または盗難デバイスの無効化
- マルチファクター認証
- 内蔵パスワード保護ポリシー
- 堅牢性と防水性の高い金属製ケースは、物理的な耐性と、改ざん明示性を持ちます
- ウイルス/マルウェア保護

