zabezpiecz się przed atakiem BadUSB

dzięki pamięciom flash USB IronKey.

Bezpieczne urządzenia USB IronKey™ i DataTraveler® są zabezpieczone przed możliwością zainfekowania złośliwym oprogramowaniem BadUSB ujawnionym na konferencji Black Hat w sierpniu 2016 roku. BadUSB to pierwszy przykład złośliwego oprogramowania przenoszonego przez porty USB, które atakuje samo urządzenie, a nie dane na nim. Wiodąca pozycja marki IronKey w obszarze bezpiecznych rozwiązań, wśród których znajdziemy na przykład podpisane cyfrowo oprogramowanie sprzętowe kontrolera, gwarantuje, że jej produkty są odporne na to nowe zagrożenie.

Jak podano podczas sesji konferencji Black Hat poświęconej atakowi BadUSB, polega on na zamianie oprogramowania sprzętowego sterującego układami urządzenia USB, przekształcając je w nosiciela, który może następnie infekować inne komputery i urządzenia USB. Zmodyfikowanego oprogramowania sprzętowego kontrolera nie potrafią wykrywać programy antywirusowe i w wielu przypadkach ujawnienie tej modyfikacji może być niemożliwe.

Zgodnie z zaleceniami specjalistów najlepszą ochronę przed tą luką w zabezpieczeniach zapewnia stosowanie podpisanego kodu w aktualizacjach oprogramowania sprzętowego. Modyfikacja podpisanego oprogramowania sprzętowego powoduje brak możliwości potwierdzenia jego autentyczności przez urządzenie i przestaje ono po prostu działać. Dzięki temu infekcja przestaje się rozprzestrzeniać, ale urządzenie jest bezużyteczne. Właśnie dlatego w urządzeniach IronKey obok podpisanego oprogramowania sprzętowego zastosowano ochronę mechanizmu aktualizacji oprogramowania sprzętowego z użyciem sprzętowych kluczy zabezpieczających. Takie zabezpieczenie uniemożliwia ingerencję w podpisanym oprogramowaniu sprzętowym sprawiającą, że urządzenie staję się bezużyteczne.

DODATKOWE WAŻNE CECHY

Dodatkowe ważne zabezpieczenia dostępne dla bezpiecznych pamięci USB DataTraveler i IronKey:

- Bezpieczne, 256-bitowe sprzętowe szyfrowanie AES klasy wojskowej wszystkich danych w pamięci
- Zgodność ze standardem FIPS (Federal Information Processing Standards) 140-2 Level 3
- Centralne zarządzanie, umożliwiające zdalne wymazywanie/dezaktywowanie zgubionych lub skradzionych urządzeń
- Uwierzytelnianie wielopoziomowe
- Wbudowane reguły ochrony hasłem
- Wzmocniona, wodoszczelna obudowa z metalu, odporna na fizyczne manipulacje i uwidaczniająca próby ingerencji
- Ochrona przed wirusami/złośliwym oprogramowaniem

IRONKEY™

Wydrukowano w USA MKF-743PL

Kingston TECHNOLOGY