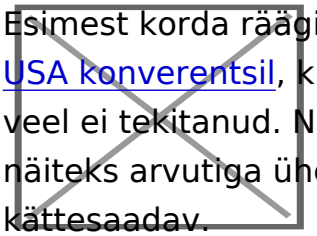
Paha USB: turvaauk nimega "BadUSB" laseb kurikaeltel arvutit juhtida

12 aastat tagasi - 04.10.2014 Autor: AM



Esimest korda räägiti kurjast BadUSB turvaaugust augustis toimunud Blackhat USA konverentsil, kuid suurt kõmu Karsten Nohl´i ning Jakob Lell´i ettekanne siis veel ei tekitanud. Nüüd aga on turvaauk, mis laseb pahategijal USB-pulga muuta näiteks arvutiga ühendatud juhitavaks klaviatuuriks, kõigile soovijatele Githubist kättesaadav.

Turvaauk seisneb selles, et häkitakse pealtnäha süütu USB-seadme - mälupulga mikrokontrolleri tarkvarasse ja muudetakse selle kaudu pulk näiteks võrgukaardiks või klaviatuuriks või mõneks muuks võimekamaks lisaseadmeks, mis suudab arvutit käsklustega juhtida.

Githubis avalikustatud Caudill´i ja Wilson'i koodi abil (kaks teadlast, kes lasid koodi nö laia maailma) saab muuta USB-mälupulga näiteks USB-klaviatuuriks. Kui tavaline klaviatuur edastab sellel tipitud käske, siis häkitud mikrokontrollerisse võib sisse panna klahvikombinatsioonide jada, mis käivitavad arvutis soovitud tegevused.

Efektiivset tõrjet turvaaugu vastu pole - peale selle, et tuleks vältida tundmatute USB-pulkade oma arvuti taha ühendamist. Samuti võib kahtlane USB pulk paljastada end siis, kui üritab arvutisse midagi kahjulikku sokutada - siis annab sellest juba viirusetõrje märku. Muidu aga ei pruugi mingit kahtlast tegevust märgatagi, sest viirusetõrje kontrollib vaid USB pulgal olevaid faile ja need võivad olla nakatamata.

Viirusetõrjefirmad soovitavad kuni BadUSB vastu efektiivse kaitse väljatulemiseni mitte võtta messidel ja konverentsidel pakutavaid tasuta USB-mälupulkasid ja mitte kasutada võõrastelt saadud mälupulki.

Selleks, et BadUSB-d tõkestada, tuleb üle vaadata USB-standardid ja see võib võtta väga kaua aega.

Kuidas BadUSB-ga nakatamine käib, seda saab näha allolevast esitlusest.

Ülalolev foto: Stuart Miles / Freedigitalphotos.net

- Uudised
- Turvalisus