http://www.ceskatelevize.cz/ct24/veda/2276110-vedci-z-brna-nasli-slabinu-ktera-ohrozuje-cipy-po-celem-svete

Vědci z Brna našli slabinu, která ohrožuje čipy po celém světě

17. 10. 2017

Několik let existovala v čipech Infinein závažná díra, která mohla narušit bezpečnost řady zařízení – například elektronických dokladů v Estonsku. Nyní se podařilo vážné bezpečnostní riziko spojené s čipy německého výrobce odhalit brněnským vědcům.

Zvětšit obrázek Zmenšit obrázek Zvětšit obrázek na celou obrazovku

Estonská identifikační karta s čipem

Zdroj: Wikimedia Commons Autor: Uninen, CC BY-SA 2.0

Sdílet obsah

Facebook

Google+

Twitter

Vytisknout

Odkaz

Dronům průlet zakázán. Bojuje proti nim bazuka, hacker nebo orel

Problém se týká způsobu, jak se generovaly kryptografické klíče pro široké spektrum zabezpečených zařízení. „Z veřejné části klíče bylo možné získat jeho tajnou hodnotu," uvedl pro ČT24 Petr Švenda z Masarykovy univerzity.

Vědci už výrobce o problému informovali na začátku roku, firma našla řešení. Nyní, s dohodnutým časovým odstupem, výzkumníci z fakulty informatiky o svém zjištění informují veřejnost. S tématem se chystají na přelomu října a listopadu na konferenci do Dallasu ve Spojených státech.

Čipy z Infineonu se používají v mnoha různých zařízeních, třeba v elektronických dokladech v Estonsku, což je pionýrská země v oblasti digitální komunikace. Výzkumníci podle Švendy nemají informace o tom, že by slabinu objevil také někdo jiný a stihl ji zneužít. Provedení takového útoku by také bylo zřejmě dosti náročné na počítačový výkon. „Pokud by si případný útočník na prolomení klíče najal hardware z cloudu Amazonu, přišlo by ho v nejhorším případě odhalení 1024bitového klíče na 76 dolarů, u 2048bitového by se částka vyšplhala na asi 40 tisíc dolarů," uvádí server Lupa.

Odkaz

Co všechno se dá hacknout? Od kardiostimulátoru až po jadernou elektrárnu

Přesto jde prý o poměrně závažné zjištění. „Díra v zabezpečení“ existovala přibližně pět let a potenciálně se dotkla velkého množství různých zařízení. Brněnští výzkumníci vytvořili a dali veřejnosti k dispozici nástroj, jehož prostřednictvím mohou lidé zjistit, zda rizikový čip mají také oni. „V českých elektronických dokladech se ale používají jiné,“ zdůraznil Švenda.

Společnost Infineon podle agentury Reuters už na problém reagovala a vyřešila jej, patřičné kroky podnikly také estonské úřady nebo společnosti Microsoft, Google, HP, Lenovo či Fujitsu.