https://www.novinky.cz/internet-a-pc/bezpecnost/452103-cesti-vedci-nasli-slabinu-pri-generovani-kryptografickych-klicu.html

Čeští vědci našli slabinu při generování kryptografických klíčů

Brněnským vědcům se podařilo odhalit vážné bezpečnostní riziko spojené s čipy německého výrobce Infineon Technologies. Jde o způsob, jak se generovaly kryptografické klíče pro široké spektrum zabezpečených zařízení. Díra v zabezpečení přitom existovala bez povšimnutí několik let.

Petr Švenda, bezpečnostní výzkumník z Masarykovy univerzity.
FOTO: Masarykova univerzita/Profimedia.cz

úterý 17. října 2017, 10:46 - Brno

Čipy od společnosti Infineon se používají v mnoha různých zařízeních, třeba v elektronických dokladech v Estonsku, což je pionýrská země v oblasti digitální komunikace. Možnosti zneužití čerstvě objevené trhliny jsou tak poměrně široké.

„Z veřejné části klíče bylo možné získat jeho tajnou hodnotu," uvedl Petr Švenda, bezpečnostní výzkumník z Masarykovy univerzity.

S těmito daty by mohli počítačoví piráti například zkopírovat právě zmiňované elektronické doklady v Estonsku a ukrást tak lidem jejich identitu. Výzkumníci podle Švendy nicméně nemají informace o tom, že by slabinu objevil také někdo jiný a stihl ji zneužít.

Hrozba pominula

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.

Je zřejmé, že jde o poměrně závažné zjištění. Díra v zabezpečení totiž existovala několik let a potenciálně se dotkla velkého množství různých zařízení. Brněnští výzkumníci vytvořili a dali veřejnosti k dispozici nástroj (v angličtině k dispozici zde), 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 autority nebo společnost Microsoft.