

# The encryption many major companies rely on has a serious flaw

RSA keys generated by Infineon chips are vulnerable to hackers.




Mallory Locklear, [@mallorylocklear](#)

10.16.17 in [Security](#)

<https://www.engadget.com/2017/10/16/encryption-companies-rely-on-has-serious-flaw/>

1 Comments

886 Shares

AdChoices 

Sponsored Links by Taboola

6 Jobs That Will Be Gone in 10 Years [BleuBloom.com](#)

18 Best Looking Cars to Buy in 2017 [Carophile](#)

Want to speak a new language in just 15 hours? This app makes it possible! [Babbel](#)

AdChoices 

Bloomberg via Getty Images

Researchers at Masaryk University in the Czech Republic uncovered a major security vulnerability in [RSA keys](#) generated by [Infineon Technologies](#)-produced chips. These chips are used in products manufactured by Acer, ASUS, Fujitsu, HP, Lenovo, LG, Samsung, Toshiba and Chromebook vendors, reports [Bleeping Computer](#) and the RSA keys generated by [Infineon's chips](#) are used in government-issued identity

documents, during software signing, in authentication tokens, with message protection like PGP, in programmable smartcards and during secure browsing.

The researchers say that key lengths of 1024 and 2048 bits are able to be figured out with little effort using the public portion of the key. "A remote attacker can compute an RSA private key from the value of a public key. The private key can be misused for impersonation of a legitimate owner, decryption of sensitive messages, forgery of signatures (such as for software releases) and other related attacks," they said in a [report](#). "The vulnerability does NOT depend on a weak or a faulty random number generator - all RSA keys generated by a vulnerable chip are impacted. The attack was practically verified for several randomly selected 1024-bit RSA keys and for several selected 2048-bit keys." And the affected RSA library has been generating weak keys since 2012. "The currently confirmed number of vulnerable keys found is about 760,000 but possibly up to two to three magnitudes more are vulnerable," said the researchers. As [Ars Technica](#) reports, a number of the vulnerable keys included those used in Estonian government-issued documents like e-residency cards.

The vulnerability was discovered and reported to Infineon in February and as per the agreed upon delay before public disclosure, the researchers will be releasing their full report on November 2nd at the ACM Conference on Computer and Communications Security. The delay is to ensure that people have time to change affected keys before the details of how the vulnerability works are released. It has also allowed vendors like Microsoft, Google, HP, Lenovo and Fujitsu to release [software updates](#) to mitigate the impact of the flaw.

The researchers have released a [blog post](#) about the vulnerability, which includes tools for testing whether existing RSA keys are secure or vulnerable. It also provides advice on what to do if you find your RSA key is compromised.

Via: [Ars Technica](#), [Bleeping Computer](#)

Source: CRoCS

In this

article: asus, gear, google, hack, hp, Infineon, internet, lenovo, lg, microsoft  
, personal computing, personalcomputing, rsa, samsung, security