https://www.theinquirer.net/inquirer/news/3019326/roca-rsa-encryption-key-flaw-puts-millions-of-devices-at-risk

ROCA: RSA encryption key flaw puts 'millions' of devices at risk

Vulnerability targets hardware created by Infineon Technologies

ROCA: RSA encryption key flaw puts 'millions' of devices at risk

- Nicholas Fearn
- 17 October 2017

0 Comments

SECURITY RESEARCHERS have uncovered a new vulnerability in a generation of RSA encryption keys used by software libraries in cryptographic smart cards, security tokens and PC chipsets.

The vulnerability has been identified by researchers working at the Centre for Research on Cryptography and Security at Masaryk University, Czech Republic; Enigma Bridge Ltd, Cambridge, UK; and Ca' Foscari University of Venice, Italy.

Specifically targeting hardware created by German semiconductor manufacturer Infineon Technologies, the vulnerability enables a practical factorisation attack.

This results in cyber criminals computing the private part of an RSA key and affects chips manufactured from 2012 onwards, which are now commonplace in the industry.

According to the researchers, hackers are able to target a plethora of commonly used key lengths - including the industry standard 1024 and 2048 bits.

Related: Vendors start to patch KRACK WPA2 flaw

The ROCA vulnerability, CVE-2017-15361, is closely related to the Trusted Platform Module (TPM). It applies cryptographic protection to computer systems and services.

Discovered in a cryptographic library applied in Infineon TPM products, the attack results in threat actors quickly targeting public keys to create private variants quickly.

The research team has come up several offline and online detection tools that allow users to access their keys safely and are recommending that affected parties contact their vendors.

Major vendors like Microsoft, Google, HP, Lenovo and Fujitsu have since released software updates and guidelines for mitigation, and more details will be revealed at the upcoming ACM CCS Conference.

RSA keys created on flawed products are weak and full of bugs. And if companies fail to find a solution, areas such as disk encryption, software signing and account security could all be left in jeopardy.

The time complexity and cost for the selected key lengths vary greatly, with the researchers estimating as follow:

- 512 bit RSA keys - 2 CPU hours (the cost of $0.06);
- 1024 bit RSA keys - 97 CPU days (the cost of $40-$80);
- 2048 bit RSA keys - 140.8 CPU years, (the cost of $20,000 - $40,000).

Writing in a blog post, the researchers said: "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.

"The actual impact of the vulnerability depends on the usage scenario, availability of the public keys and the lengths of keys used.

"We found and analyzed vulnerable keys in various domains including electronic citizen documents, authentication tokens, trusted boot devices, software package signing, TLS/HTTPS keys and PGP.

"The currently confirmed number of vulnerable keys found is about 760,000, but possibly up to two to three magnitudes more are vulnerable. The details will be presented in two weeks at the ACM CCS conference." µ