https://www.scmagazine.com/roca-proof-of-concept-attacks-threaten-rsa-encrypted-devices-as-far-back-as-2012/article/700886/

October 17, 2017

ROCA vulnerability threatens RSA encrypted devices on heels of KRACK scare

ROCA proof of concept attacks threaten RSA encrypted devices as far back as 2012.

Less than a day after the KRACK vulnerability scare affecting all Wi-Fi devices using the WPA2 protocol security pros once again have their hands full to update patches for the ROCA vulnerability which could allow an attacker to circumvent RSA encryption.

The vulnerability (CVE-2017-15361) infects vulnerable keys found in about 760,000 products from major vendors including Microsoft, Google, HP, Lenovo, and Fujitsu who have already released software updates and guidelines for a mitigation and is caused by cryptographic chips produced by Infineon Technologies AG, according to an advisory detailing the attack.

ROCA stands for Return of Coppersmith's Attack and was developed by Researchers at the Centre for Research on Cryptography and Security using an old technique to exploit a vulnerability in NIST FIPS 140-2 and CC EAL 5+ certified devices and has been present since at least 2012.

The exploit allows an attacker to carry out a practical factorization attack to compute the private part of an RSA key for commonly used key lengths for $76 to decrypt 1024 bits in a matter of hours and about $40,000 for the 2048-bit version in a matter of days.

“A remote attacker can compute an RSA private key from the value of a public key,” researchers said in the advisory. “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 impact of the vulnerability varies depending on the venders' implementation of the encryption however a large number of Google Chromebook and Windows devices created by Fujitsu, HP and Lenovo are amongst those affected. The vulnerability also impacted Estonia ID cards which were recently shown to be vulnerable to a proof of concept attack.

"The authors have made it clear that this flaw is embedded into the hardware and firmware of many devices widely used across the globe,” Synopsys Security Consultant Jesse Victors said. “This makes it difficult to completely patch, but there are some mitigating controls.”

Victors added that RSA turned 40 years old this year and we still seem to struggle with using and implementing it correctly however RSA is one of our best public key encryption schemes, so it isn't going away any time soon.

The revelation is similar to the problem Sony's PlayStation software download system suffered in 2010, and exactly what happened to the Taiwan National ID registry in 2013, Thales e-Security Chief Technology Officer Jon Geater said.

“While the effects of this latest flaw are concerning, it's interesting to note that this is far from the first time it's happened,” he said. “Generating high quality signing keys from high quality entropy and key generation processes is absolutely fundamental, especially in large scale systems where lots of public keys are available to sample.”

Geater added that crypto is harder than it looks and that it's important to employ experts and use quality specialist equipment to generate, store and use your keys. Furthermore, encryption is only secure if implemented correctly.

“In this case, where private keys can be derived from public keys, the implementation was flawed,” Bitglass Chief Technology Officer Anurag Kahol said. “For organizations and governments that choose to encrypt data, key management – storing keys securely, rotating master keys and aliases to that master key – can be invaluable in protecting data.”

Infineon Technologies AG has been notified and is reportedly working on a fix for the vulnerable chips.