keyon

CVE-2017-15361 V1.0b

End of January 2017 a vulnerability was discovered that affects RSA keys generated by an Infineon library, which is widely used in smart cards and Trusted Platform Module Chips (TPM). The vulnerability was disclosed to the public on October 16th 2017 and might need your attention.

Management summary

- RSA private keys with commonly used key lengths (e.g. 2048 Bit RSA) generated in an affected device can be efficiently calculated from their corresponding public keys (RSA factorization). In other words, such RSA keys can no longer be considered as secure;
- It has been practically shown that RSA 1024 and 2048 bit private keys can be factorized from a vulnerable public key within days or even less;
- Such vulnerable public keys are widely used and exposed to the public as part of certificates. They can be easily detected as such;
- Non-RSA keys, like DH and EC DH based keys, are not affected by this vulnerability;
- Organizations using hardware based RSA keys should analyze the keys used in their environment.

keyon AG
Schlüsselstrasse 6
8645 Jona
Switzerland

Tel +41 55 220 64 00
Fax +41 55 220 64 01

www.Keyon.ch
info@Keyon.ch

keyon

About this summary

The vulnerability, as referenced under CVE-2017-15361, is well documented on the internet. Details about the factorization method will be released at the ACM CCS conference in Dallas, USA (Oct 30th 2017). The respective sources on the internet are highlighted below. The goal of this document is to summarize the most important facts and to put them into a real-world context.

CVE-2017-15361 at a glance

An attacker is able to compute the RSA private key from the corresponding RSA public key, if the key-pair has been generated using a specific software library which has been adopted in Trusted Platform Modules, cryptographic smart cards, security tokens, and other secure hardware chips manufactured by Infineon Technologies AG. The attack is feasible for RSA keys with commonly used key lengths, including 1024 and 2048 bits, and affects chips manufactured as early as 2012. It can be performed within days or hours at a cost of approximately USD 40-80 for an individual 1024 Bit RSA key and about USD 20k-40k for an individual 2048 Bit RSA key. Since public keys are exposed to the public by design, an attacker can easily get possession of specific public keys in order to perform targeted attacks.

Affected security controls and use-cases

The following security controls and use-cases are affected (not conclusive list)

- TPM related use-cases: BitLocker, 802.1X for certificate based wireless and wired access control, certificate based access to VPN and Direct Access, virtual smart cards used for Windows Logon, personal authentication or digital signatures;
- Smart card related use-cases: Smart cards used for Windows logon, personal authentication, or digital signatures.

How to proceed?

Organizations using hardware based RSA keys should analyze the keys used in their environment. Online and offline testing applications are available to check the vulnerability of the RSA keys. In addition, major vendors already released software updates and guidelines for a mitigation.

Keyon can provide support in the bulk analysis of certificates used in your organization and plan and support your mitigation activities. Please contact info@keyon.ch to plan your next steps.

Sources

- https://nvd.nist.gov/vuln/detail/CVE-2017-15361
- https://crocs.fi.muni.cz/public/papers/rsa_ccs17
- https://www.infineon.com/cms/en/product/promopages/tpm-update/?redirId=59160