CERT-EU Security Advisory 2017-023

RSA Key Generation Prone to Factorization Attack

November 7, 2017 — v1.1

History:

- *17/10/2017 — v1.0 – Initial publication*
- *07/11/2017 — v1.1 – More efficient ways of attack reported*

Summary

A vulnerability (CVE-2017-15361) [4] in the procedure of RSA key generation used by a software library allows a practical factorization attack. As a result it is possible to compute the private part of an RSA key based only on its public part. The vulnerable library is used in cryptographic smartcards, security tokens, and other secure hardware chips manufactured by Infineon Technologies AG. An attack is feasible for commonly used key lengths – including 1024 and 2048 bits – and it affects chips manufactured as early as 2012 [1].

Technical Details

The faulty software is the Infineon-developed RSA library version 1.02.013, more specifically the algorithm it implements for RSA primes generation. Only RSA encryption keys are affected, when they were generated on a smartcard or other embedded device using the mentioned software.

For performance reasons the Infineon library constructs the key pairs underlying prime numbers in a way that the secret key can be deducted from the public key through factorization.

An RSA key with 2048 bits should require – when generated properly – several quadrillion years to be factorized with a general-purpose computer. Factorizing a 2048-bit RSA key generated with the faulty Infineon library, by contrast, takes a maximum of 100 years, and on average only half that. Keys with 1024 bits take a maximum of only three months. The factorization can be dramatically accelerated by spreading the load onto multiple computers. While costs and times vary for each vulnerable key, the worst case for a **2048-bit** one would require no more than **17 days and $40,300** using a 1,000-instance machine on Amazon Web Service and **$76 and 45 minutes** to factorize an affected **1024-bit key**. On average, it would require half the cost and time to factorize the affected keys [1, 2].

The researchers who discovered the issue are providing also tools [1] to quickly verify if a key is vulnerable. Those tools can be used also, by potential attackers, to asses if the key is exploitable.

The flaw is the subject of a research paper titled *The Return of Coppersmith's Attack(ROCA): Practical Factorization of Widely Used RSA Moduli*, which will be presented on the 2nd of November 2017 at the ACM Conference on Computer and Communications Security, Dallas, USA. In order to provide time for keys change, the paper describing the factorization method will not be published until the above mentioned conference [2].

A significantly more efficient way of performing the attack was recently announced [9], which could improve the attack in some cases more than **10x**. It can be further improved by using specialized hardware. In the meantime the Estonian authorities reevaluated the threat and decided to update the 760 000 ID cards certificates affected by the vulnerability [10, 11].

Products Affected

Infineon products can be affected under a specific combination of conditions:

- The acceleration algorithm was used for the key generation.
- Cryptographic keys have to be generated on a card or token, which uses this algorithm.

Products that can be affected are typically the TPM (Trusted Platform Modules), e.g. used in professional notebooks, and smartcards for signature applications with self-generated keys. The chip hardware (symmetric and asymmetric co-processors) is not affected [6].

Examples of affected technologies include BitLocker with TPM 1.2, YubiKey 4 PGP key generation, and the Cached User Data encryption feature in Chrome OS, Electronic IDs [2, 5].

The vulnerability is also present in at least some NIST FIPS 140-2 and CC EAL 5+ certified devices since at least the year 2012 [1].

Recommendations

Verify with the vendors or with the provided tools [3] if the technologies or keys in use in your organization are affected. The researchers are providing offline [7], online [3, 8], or email S-MIME/PGP key testers.

Vulnerable key pairs and devices should be replaced with secure ones. Major vendors including Microsoft, Google, HP, Lenovo, Fujitsu already released the software updates and guidelines for a mitigation [1].

References

[1] https://crocs.fi.muni.cz/public/papers/rsa_ccs17

[2] https://arstechnica.com/information-technology/2017/10/crypto-failure-cripples-millions-of-high-security-keys-750k-estonian-ids/

[3] https://keychest.net/roca

[4] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15361

[5] https://nvd.nist.gov/vuln/detail/CVE-2017-15361

[6] https://www.infineon.com/cms/en/product/promopages/rsa-update/?redirId=59206

[7] https://github.com/crocs-muni/roca

[8] https://keytester.cryptosense.com

[9] https://blog.cr.yp.to/20171105-infineon.html

[10] https://arstechnica.com/information-technology/2017/11/flaw-crippling-millions-of-crypto-keys-is-worse-than-first-disclosed/

[11] https://medium.com/e-residency-blog/estonia-is-enhancing-the-security-of-its-digital-identities-361b9a3c9c52