Utimaco IS GmbH • Germanusstraße 4 • 52080 Aachen

To whom it may concern

17.10.2017

ROCA: Vulnerable RSA generation (CVE-2017-15361)

Utimaco has been made aware of the vulnerability CVE-2017-15361 aka. ROCA (The Return of Coppersmith's Attack), affecting the RSA library in Infineon chips. Details about this vulnerability can be found on https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15361 and https://crocs.fi.muni.cz/public/papers/rsa_ccs17 .

Utimaco declares that CryptoServer Hardware Security Modules (HSM) including their firmware and tools are not affected by this vulnerability:

- None of Utimaco's HSMs embeds any of the affected Infineon chips nor any copy or derivative of Infineon's RSA library.
- Smartcards supplied by Utimaco and used for user authentication do not embed any of the affected Infineon chips.
- RSA keys generated by Utimaco HSMs have been tested as "safe" by the ROCA Vulnerability Test Suite available on https://keychest.net/roca , demonstrating that the RSA key generation implemented in Utimaco's HSMs and tools is not affected by the attack behind CVE-2017-15361.

With best regards
Utimaco IS GmbH

Dieter Bong
Product Manager HSM