utimaco®

Utimaco IS GmbH • Germanusstraße 4 • 52080 Aachen

To whom it may concern

05.01.2018

Meltdown and Spectre Vulnerabilities
(CVE-2017-5754, CVE-2017-5753, and CVE-2017-5715)

The Meltdown and Spectre security flaws exploit the way that modern CPUs use out-of-order and speculative execution for better performance.

Utimaco declares that CryptoServer Hardware Security Modules (HSMs) including their firmware are not affected by these vulnerabilities.

- Meltdown only affects Intel processors, which are not used in our HSMs.
- For Spectre to work it is necessary to run code mounting an attack on the target device. Code running on a CryptoServer HSM needs to be signed by a trusted party and loaded by an administrator with specific credentials. The firmware signature is validated by the HSM. To load custom code, an administrator must also load the public part of the Alternative Module Signature Key first. Execution of random malware such as a JavaScript described in the Spectre paper is ruled out by construction.

Code running on client systems interfacing CryptoServer HSMs may be vulnerable to Meltdown and Spectre. Advisories published by processor vendors and operating systems providers should be consulted and best practices should be implemented.

The Utimaco CryptoServer LAN appliance uses an Intel processor. It is it not part of the security architecture though. Its main function is to provide the CryptoServer HSM with power, cooling, and network access.

With best regards
Utimaco IS GmbH

Thorsten Grötker
Head of R&D, HSM