# Nexans switches and Spectre and Meltdown Vulnerability

KD1593E0

## Spectre and Meltdown vulnerability background

Two vulnerabilities (CVE-2017-5753 and CVE-2017-5715) are commonly known as Spectre and one (CVE-2017-5754) is known as Meltdown.

Researchers found two major weaknesses in processors that could let attackers read sensitive information that should never leave the CPU, or central processing unit. In both cases, attackers could see data that the processor temporarily makes available outside of the chip.

For details please read Wikipedia articles https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability) and https://en.wikipedia.org/wiki/Spectre_(security_vulnerability).

## Nexans switches unaffected

***Nexans is NOT exposed to the Spectre and Meltdown vulnerability.***

To exploit any of these vulnerabilities, an attacker must be able to run malicious code on an affected device. Although the underlying CPU and operating system combination in our switches may be affected by these vulnerabilities, all Nexans switches are closed systems that do not allow customers to run custom code on the device, and thus are not vulnerable.

Nexans Deutschland GmbH
Advanced Networking Solutions

Issued in 08.01.2018, Mönchengladbach Germany