Nexans switches and Interpeak TCP/IP Network Stack Vulnerability

KD1725E0

Vulnerability background

Security researchers from Armis have identified critical vulnerabilities in the network stack Interpeak IPNet TCP/IP. The network stack is used in real-time operating systems (i.a. for embedded systems in routers, modems, printers, medical devices) and also memory programmable controllers of many manufacturers. The vulnerabilities can be exploited over the network regardless of the vendor-specific application programs.

For more information see BSI document CSW-Nr. 2019-243492-10k3 or get a detailed documentation from Armis: https://www.armis.com/resources/iot-security-blog/urgent-11-update/

Nexans switches unaffected

Nexans is NOT exposed to the Interpeak IPNet TCP/IP Network Stack Vulnerabilities.

All types of Nexans Switches are unaffected because Nexans doesn't use the Interpeak IPNet TCP/IP network stack.

Nexans Deutschland GmbH
Advanced Networking Solutions

Issued in 16.10.2019, Mönchengladbach Germany