Nexans switches and 11 Zero Day Vulnerabilities in VxWorks

KD1717E0

Vulnerability background

As of July 2019, a paper published by Armis exposed 11 critical vulnerabilities including remote code execution, denial of service, information leaks, and logical flaws impacting more than 2 billion devices which use the VxWorks RTOS. The findings are significant since this system is in use by quite a few mission-critical products.

For more information please read Wikipedia article
https://en.wikipedia.org/wiki/VxWorks#TCP_vulnerability

or get a detailed documentation from Armis:
https://go.armis.com/urgent11

Nexans switches unaffected

Nexans is NOT exposed to the 11 zero day vulnerabilities in VxWorks.

All types of Nexans Switches are unaffected because Nexans doesn’t use the VxWorks operation system.

Nexans Deutschland GmbH
Advanced Networking Solutions

Issued in 21.08.2019, Mönchengladbach Germany