Nexans switches and NAME:WRECK vulnerabilities in DHCP/DNS implementation of TCP/IP Network Stacks

KD1813E0

Vulnerability background

Security researchers from JSOF and Forescout Research Labs have found nine vulnerabilities in the DHCP and DNS implementations of the TCP / IP stacks of four operating systems, which are mainly used in real-time communications.

Four systems are affected by these vulnerabilities, to different degrees:
- FreeBSD
- IPNet
- NetX
- Nucleus Net

The exact extent to which the individual stacks were affected can be found in the Forescout report:
[FOS2021] Advisory NAME:WRECK DNS Vulnerabilities
https://www.forescout.com/company/resources/namewreck-breaking-and-fixing-dns-implementations/

For more information see BSI document CSW-Nr. 2021-207948-10k2.

Nexans switches unaffected
Nexans is NOT exposed to the NAME:WRECK vulnerability.

All types of Nexans Switches are unaffected because Nexans doesn't use any of the above listed OS systems.

Nexans Deutschland GmbH
Advanced Networking Solutions

Issued in 19.07.2021, Mönchengladbach Germany