Nexans switches and AMNESIA:33 Vulnerabilities in TCP/IP Network Stacks

KD1804E0

Vulnerability background

Security researchers from Forescout have analyzed seven open source TCP / IP stacks and found a total of 33 partially critical vulnerabilities in four of them (uIP, picoTCP, FNET, Nut / Net).

The vulnerabilities known as "AMNESIA: 33" can be used, among other things, to carry out denial-of-service attacks or to read out sensitive information. At least four vulnerabilities can be used by a remote, unauthenticated attacker to execute arbitrary code on the vulnerable device. In all cases, the exploitation of the vulnerability is based on specially prepared network packets that are exchanged between the device and the attacker.

For more information see BSI document CSW-Nr. 2020-532768-10k3.

Nexans switches unaffected

Nexans is NOT exposed to the AMNESIA:33 Vulnerability in TCP/IP Network Stacks.

All types of Nexans Switches are unaffected because Nexans doesn't use TCP/IP network stacks from uIP, picoTCP, FNET or Nut/Net.

Nexans Deutschland GmbH
Advanced Networking Solutions

Issued in 18.12.2020, Mönchengladbach Germany