Nexans switches and Apache webserver "httpd" vulnerability

KD1820E0

Vulnerability background

On October 4th, 2021, Apache released an "important" security update for Apache "httpd", which closes CVE-2021-41773 (see [APA2021a], [NVD2021]). The impact of the vulnerability was described as "Path Traversal & Information Disclosure" (see [APA2021a]). Various media reported on the matter including a proof-of-concept (PoC).
On October 6th, 2021, the security company Rapid7 published a blog entry which explains that the vulnerability can also be used to execute operating system commands by unauthenticated attackers (see [RAP2021]).
The standard configuration of the "httpd" in combination with the activated module "mod_cgi" is vulnerable to the attack. The "mod_cgi" module is delivered with the "httpd" as standard and has long served as the standard interface between "httpd" and scripting languages such as Perl or Python in the past. It is likely that the module is activated on some of the vulnerable instances.

For more information see BSI document CSW-Nr. 2021-260764-11k2

Nexans switches unaffected

Nexans is NOT exposed to the Apache webserver "httpd" vulnerability.

All types of Nexans Switches are unaffected because Nexans doesn't use the stated webserver.

Nexans Deutschland GmbH
Advanced Networking Solutions

Issued in 08.11.2021, Mönchengladbach Germany