Nexans Switches unaffected by Heartbleed Vulnerability

KD1206E0

Heartbleed vulnerability background

Heartbleed is a security bug in the open-source **OpenSSL cryptography library**, widely used to implement the Internet's Transport Layer Security (TLS) protocol. This vulnerability results from a missing bounds check in the handling of the Transport Layer Security (TLS) heartbeat extension, the heartbeat being why the vulnerability got its name.
A fixed version of OpenSSL was released on April 7, 2014, at the same time as Heartbleed was publicly disclosed. At that time, some 17 percent (around half a million) of the Internet's secure web servers certified by trusted authorities were believed to be vulnerable to the attack, allowing theft of the servers' private keys and users' session cookies and passwords. The Electronic Frontier Foundation, Ars Technica, and Bruce Schneier all deemed the Heartbleed bug "catastrophic". Forbes cybersecurity columnist Joseph Steinberg wrote, "Some might argue that [Heartbleed] is the worst vulnerability found (at least in terms of its potential impact) since commercial traffic began to flow on the Internet."

From Wikipedia (http://en.wikipedia.org/wiki/Heartbleed)

Nexans switches unaffected

Nexans is NOT exposed to the OpenSSL Heartbleed vulnerability.

Unlike hardware and software vendors who have integrated OpenSSL into their core product and service offerings, Nexans is unaffected because Nexans uses a proprietary SSL stack to process SSL and TLS network traffic. Currently Nexans switches use SSL/TLS for HTTPS communication only.

Nexans Deutschland GmbH
Advanced Networking Solutions

Issued in 17.04.2014, Mönchengladbach Germany

Nexans Deutschland GmbH • Advanced Networking Solutions
Bonnenbroicher Straße 2-14 • 41238 Monchengladbach • Tel: +49 (0) 2166 27-2220 Fax: +49 (0) 2166 27-2499
E-Mail: sales.ans@nexans.com • **www.nexans.de/ans**