Nexans switches and FREAK vulnerability

KD1271E0

FREAK vulnerability background

FREAK ("Factoring RSA Export Keys") is a security exploit of a cryptographic weakness in the SSL/TLS protocols introduced decades earlier for compliance with U.S. cryptography export regulations. These involved limiting exportable software to use only public key pairs with RSA moduli of 512 bits or less (so-called RSA_EXPORT keys), with the intention of allowing them to be broken easily by the NSA, but not by other organizations with lesser computing resources.

The flaw was found by researchers from IMDEA, INRIA and Microsoft Research. The FREAK attack has the CVE identifier CVE-2015-0204.
From Wikipedia (http://en.wikipedia.org/wiki/FREAK)

Nexans switches unaffected

Nexans is NOT exposed to the FREAK vulnerability.

All Nexans switches are unaffected because Nexans doesn't use weak "RSA_EXPORT" keys. 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**