Nexans switches and POODLE vulnerability

KD1244E0

POODLE vulnerability background

The POODLE attack (which stands for "Padding Oracle On Downgraded Legacy Encryption") is a man-in-the-middle exploit which takes advantage of a clients' fallback to SSL 3.0. If attackers successfully exploit this vulnerability, on average, they only need to make 256 SSL 3.0 requests to reveal one byte of encrypted messages. Bodo Möller, Thai Duong and Krzysztof Kotowicz from the Google Security Team discovered this vulnerability; they disclosed it in September 2014. Tal Klein and Ivan Ristic do not consider the POODLE attack as serious as the Heartbleed and Shellshock attacks.

To mitigate POODLE attack, one way is to completely disable SSL 3.0 on the client side and the server side.

This vulnerability has the CVE ID CVE-2014-3566.

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

Nexans switches with management hardware HW3 are affected

All Nexans switches with management hardware version 3.xx which have firmware versions before V4.03cd installed are affected.

The vulnerability has been fixed by disabling the SSLv3 protocol for the integrated HTTPS server. From firmware version V4.03cd a HTTPS connection is possible via TLSv1 only.

For customers who have enabled HTTPS on their Nexans switches we recommend an update with firmware version V4.03cd or later.
Please download this firmware from our support portal at http://www.nexans-ans.de/support/.

Nexans Deutschland GmbH
Advanced Networking Solutions

Issued in 22.10.2014, Moenchengladbach 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**