SSH Protocol Authentication Bypass

KD1880E0

SSH Protocol Authentication Bypass Description

A vulnerability was found in libssh's server-side state machine before versions 0.7.6 and 0.8.4. A malicious client could create channels without first performing authentication, by presenting SSH2_MSG_USERAUTH_SUCCESS message in place of the SSH2_MSG_USERAUTH_REQUEST method that normally would initiate authentication, resulting in unauthorized access.

This vulnerability has the CVE ID CVE-2018-10933.

From CVE (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10933)

Nexans switches with management hardware HW5 are affected

All Nexans switches with management hardware version V5.xx which have firmware versions before V7.00aa installed are affected.

The vulnerability has been fixed by updating libssh's sever on the version V7.00aa.

We recommend an update with firmware version V7.04D or later.
Please download this firmware from our support portal at http://www.nexans-ans.de/support/.

Nexans Advanced Networking Solutions GmbH

Issued in 30.05.2023, Moenchengladbach Germany