WESTERMO-18-05: Security Advisory

CRITICAL / HIGH / MEDIUM / LOW / INFORMATIONAL 2018-11-26

LibSSH - Authentication Bypass Vulnerability

CVE

- **CVE-2018-10933**

Description

After investigation of the authentication bypass vulnerability in libSSH it has been determined that all xRD products with older firmware versions are affected by the following CVEs:

CVE-2018-10933: libssh versions 0.6 and above have an authentication bypass vulnerability in the server code. By presenting the server an SSH2_MSG_USERAUTH_SUCCESS message in place of the SSH2_MSG_USERAUTH_REQUEST message which the server would expect to initiate authentication, the attacker could successfully authenticate without any credentials.

Affected versions

- All xRD-products running firmware version 1.7.8.5 and older.

- MRD-355/455 1.7.8.5 and older
- MRD-305/405 1.7.8.5 and older
- MRD-315 1.7.8.5 and older
- BRD-355 1.7.6.16 and older
- ADSL-350 1.7.6.16 and older (discontinued)
- MRD-350 1.5.7.0 and older (discontinued)
- MRD-310/330 1.5.7.0 and older (discontinued)

Impact

An attacker can gain unauthorized access, without credentials, to a router. Enabling unauthorized actions to be performed.

Westermo Teleindustri AB
SE-640 40 Stora Sundby, Sweden
Tel. +46 (0)16 42 80 00 I Fax. +46 (0)16 42 80 01
info@westermo.com I www.westermo.com

Corp ID No: 556361-2604
VAT: SE556361260401

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, resulting in unauthorized access.

There is a vulnerability within the server code which can enable a client to bypass the authentication process and set the internal state machine maintained by the library to authenticated, enabling the (otherwise prohibited) creation of channels.

Severity

The CVSSv3 severity base score for the CVE is:
CVE-2018-10933: **9.1**
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2018-10933&vector=AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Mitigation

Firmware version 1.7.9.0 (for all models) and later have an updated LibSSH package (0.7.7) in use, where the vulnerability has been fixed.

To mitigate this vulnerability, update xRD firmware to version 1.7.9.0 or later. The latest firmware can be downloaded from www.westermo.com/support/product-support.

Firmware of discontinued products will not be updated, following guidelines in Westermo life cycle policy. If a firmware upgrade is not possible, we recommend that the SSH port is blocked in the firewall, all attempts to connect over SSH will be blocked.

Updates

BRD-355 waiting for an updated firmware.

References

CVE-2018-10933 – https://nvd.nist.gov/vuln/detail/CVE-2018-10933

Westermo Teleindustri AB
SE-640 40 Stora Sundby, Sweden
Tel. +46 (0)16 42 80 00 I Fax. +46 (0)16 42 80 01
info@westermo.com I www.westermo.com

Corp ID No: 556361-2604
VAT: SE556361260401