WEOS-15-08: Security Advisory

CRITICAL / **HIGH** / MEDIUM / LOW 2017-08-14

Description

Multiple vulnerabilities have been fixed in version 1.7.7.0 (some already in 1.7.5.0) of our MRD product family.

The four vulnerabilities were reported by Qualys Security through ICS-CERT as:

- Hardcoded SSH keys
- Hardcoded HTTPS keys and certificate
- CSRF, Cross Site Request Forgery

Please read the Impact section for more information about the individual vulnerabilities.

Affected versions

The following Westermo products and firmware versions are affected:

Hardcoded SSH keys

- MRD-305-DIN, MRD-315, MRD-355, MRD-455 firmware versions lower than 1.7.5.0

Hardcoded HTTPS keys and certificate

- MRD-305-DIN, MRD-315, MRD-355, MRD-455 firmware versions lower than 1.7.5.0

Cross Site Request Forgery

- MRD-305-DIN, MRD-315, MRD-355, MRD-455 firmware versions lower than 1.7.7.0

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

Impact

Hardcoded keys (SSH and HTTPS) allow an attacker to use them to both impersonate an affected device and decrypt traffic protected by these keys. Both cases may lead to the disclosure of admin credentials which ultimately grants the attacker authenticated access to the device with administrative privileges.

The Cross Site Request Forgery vulnerability may lead to unauthorized manipulation of the device if an authenticated user is accessing an infected web site concurrently to the device web management interface (in the same browser but a different tab). The attacker will be able to invoke any command with the same privileges as the authenticated user.

Severity

Westermo CVSS[1] v3 severity base scores are:

- 7.5 – Hardcoded SSH keys (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)
- 7.5 – Hardcoded HTTPS keys and certificate (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)
- 8.8 – Cross Site Request Forgery (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

Mitigation

We recommend all users that expose SSH and HTTPS user interfaces to the network to update to the latest version available, which currently are the ones listed in the Updates section.

Mitigations that do not require update:

- Users that do not use SSH or HTTPS should disable those services. Please consult the management guide more information.

Updates

Updates fixing all issues are available for download:

- MRD-305-DIN, firmware version 1.7.7.0
- MRD-315, firmware version 1.7.7.0
- MRD-355, firmware version 1.7.7.0
- MRD-455, firmware version 1.7.7.0

[1] For more information on CVSS scores, see: https://www.first.org/cvss/user-guide

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

References

The issues in this advisory were reported by security researcher Mandar Jadhav at Qualys Vulnerability Signature/Research Team, research@qualys.com

ICS-CERT advisory, ICSA-17-236-01 Westermo Westermo MRD-305-DIN, MRD-315, MRD-355, and MRD-455

CVE-2017-12703

CVE-2017-12709

CVE-2017-5816

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