WEOS-17-03: Security Advisory

CRITICAL / HIGH / **MEDIUM** / LOW 2017-10-17

Description

The WPA2 four-way handshake is vulnerable to Key Reinstallation Attacks forcing the client to use an all-zero encryption key, these vulnerabilities (VU#228519) indexed below:

- CVE-2017-13077: Reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the four-way handshake
- CVE-2017-13078: Reinstallation of the Group Temporal Key (GTK) during the four-way handshake
- CVE-2017-13079: Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11w allows reinstallation of the Integrity Group Temporal Key (IGTK)
- CVE-2017-13080: Reinstallation of the Group Temporal Key (GTK) during the group key handshake
- CVE-2017-13081: Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11w allows reinstallation of the Integrity Group Temporal Key (IGTK) during the group key handshake
- CVE-2017-13082: Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11r allows reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the fast BSS transmission (FT) handshake
- CVE-2017-13084: Reinstallation of the Station-To-Station-Link (STSL) Transient Key (STK) during the PeerKey handshake
- CVE-2017-13086: Reinstallation of the Tunneled Direct-Link Setup (TDLS) Peer Key (TPK) during the TDLS handshake
- CVE-2017-13087: Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Group Temporal Key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame
- CVE-2017-13088: Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Integrity Group Temporal Key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame

Affected products

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

The following Westermo Products are susceptible to the vulnerability:

- RT-310
- RT-320
- RT-370

Impact

An attacker can remotely exploit the following services:

- WPA Key Reinstallation
- Forced association to rouge AP
- Interception of encrypted data

Severity

*The CVSSv3 severity base score is **6.8** for **VU#228519,***

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N/E:P/RC:R

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

Mitigation

We recommend all users put in place the following:

- An HTTPS browser for end users/services. Fully secure HTTPS browser already available for the Westermo Wi-Fi network devices.
- Creating a MAC address ACL of the allowed network devices and connections.

Updates

This vulnerability is addressed and available on firmware version 6.8.2 RC1.

References

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13077

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13078

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13079

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13080

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13081

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13082

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13084

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13086

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13087

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13088

https://www.kb.cert.org/vuls/id/228519

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