WEOS-15-06: Security Advisory

CRITICAL / **HIGH** / MEDIUM / LOW 2016-01-20

Description

The WeOS firmware ships with a default self signed certificate and private key for the HTTPS web user interface. Extracting the certificate and private key from the firmware makes it possible to masquerade as a WeOS device, potentially staging a successful man-in-the-middle attack, for example to steal the user credentials otherwise protected by the SSL/TLS channel.

The possibility to change this default certificate exists as an undocumented technical preview using the command line interface, CLI. Please refer to the section *Mitigation* for more information.

This advisory is registered with ICS-CERT as CVE-2015-7923

Affected versions

Westermo products running or based on any of the following WeOS operating system versions and that support HTTPS are susceptible to this vulnerability:

- 4.2.0 and later

Impact

A successful attack allows an attacker to obtain the user credentials submitted from the web browser when authenticating to the device. Depending on authority, the credentials may allow full access to the device configuration.

Severity

ICS-CERT has given this issue a CVSS[1]v3 base score of **9.0**;
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:T/RC:C

Westermo product security incident response team PSIRT has set a CVSSv3 severity base score of **8.3**;
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:T/RC:C

Mitigation

Procedure to replace the default web certificate:

1. Devices with WeOS versions older than 4.15.2 should be upgraded to the latest release in order to get the capability to replace the default web certificate.
2. Upload a custom certificate, preferably from an established internal or external PKI. See section 7.1.8 in the WeOS Management Guide.
3. Login to the CLI (console or SSH).

[1] https://www.first.org/cvss/calculator/3.0

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

4. Issue the following commands (where <LABEL> is the label defined during step 2 as described in the WeOS Management Guide):
    a. config
    b. web
    c. certificate <LABEL>
    d. exit
    e. exit
    f. copy run start

Self signed certificates should always be avoided at all costs as they always provide a similar attack vector even without the private key of the device as the user does not know the public key before first access.

Web access either be disabled completely or allowed only from the most secure network, which reduces the exposure of this vulnerability to that network. The attacker must gain access to that network in order to stage an attack.

Updates

This vulnerability is addressed by Westermo and a fix is currently planned for release first half of 2016.