WEOS-17-02: Security Advisory

CRITICAL / **HIGH** / MEDIUM / LOW 2017-10-12

Description

A security related update of the dnsmasq open source component, which provides DHCP and DNS features in WeOS, has been released to fix the following vulnerabilities:

- CVE-2017-13704: Resulted in a crash on a large DNS query
- CVE-2017-14491: DNS heap buffer overflow
- CVE-2017-14492: DHCPv6 RA heap overflow
- CVE-2017-14493: DHCPv6 - Stack buffer overflow
- CVE-2017-14494: Infoleak handling DHCPv6 forwarded requests
- CVE-2017-14495: OOM in DNS response creation
- CVE-2017-14496: Integer underflow in DNS response creation

After investigation it has been determined that only **CVE-2017-14491** is applicable to WeOS.

Affected products

Westermo products running any of the following WeOS versions are susceptible to the vulnerability:

4.8.0 to 4.21.1

Impact

An attacker can remotely exploit the following services, which would crash or even allow control of the underlying component:

- DNS, Domain Name System
- DHCP, Dynamic Host Configuration Protocol

Severity

*The CVSSv3 severity base score is **9.8** for CVE-2017-14491,*
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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 of DHCP and DNS services to upgrade all products to WeOS 4.21.2.

Alternative mitigation involves disabling use of the switch as a DHCP server and blocking of DNS requests following the instructions below:

- If the device acts as a DHCP server, remove all DHCP server configurations if present. See section *22.1.3 General DHCP Server settings* in the WeOS Management Guide
- Block DNS requests by using the following firewall rule:
  filter deny in <vlanX> dport 53 proto udp
  For each VLAN in use, replace <vlanX> with the actual VLAN ID and apply the firewall rule.
  See section *31.1.2.2 Filter Rules Packet Matching* in the WeOS Management Guide

Updates

This issue is corrected in WeOS version 4.21.2 that is available for download at http://www.westermo.com

References

https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-14491

https://security.googleblog.com/2017/10/behind-masq-yet-more-dns-and-dhcp.html

http://thekelleys.org.uk/gitweb/?p=dnsmasq.git&a=search&h=HEAD&st=commit&s=CVE-2017

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