WESTERMO-18-04: Security Advisory

CRITICAL / HIGH / MEDIUM / LOW / INFORMATIONAL 2018-05-29

Vulnerabilities in BusyBox

CVE

- **CVE-2016-2147**
- **CVE-2016-2148**

Description

After investigating the multi-call binary BusyBox, it has been determined that WeOS are affected by the following CVEs:

CVE-2016-2148: Heap-based buffer overflow in the DHCP client (udhcpc) in BusyBox before 1.25.0 allows remote attackers to have unspecified impact via vectors involving OPTION_6RD parsing.

CVE-2016-2147: Integer overflow in the DHCP client (udhcpc) in BusyBox before 1.25.0 allows remote attackers to cause a denial of service (DoS, crash) via a malformed RFC1035-encoded domain name, which triggers an out-of-bounds heap write.

Affected versions

WeOS 4.8.0 to 4.23.0.

Impact

An attacker can remotely exploit the following service:

- DHCP client

Triggering the two different vulnerabilities causes a buffer overflow, in two different functions, that can either crash the DHCP client service (DoS) or cause an unspecified impact.

Severity

The CVSSv3 severity base score for the CVE:s are:

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

CVE-2016-2148: **9.8**
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
CVE-2016-2147: **7.5**
https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Mitigation

- Do not use the DHCP client feature in unsecure environments. Instead, assign static addresses to the clients.
- Upgrade to the latest version of WeOS when a fix is available.

Updates

Pending

References

https://nvd.nist.gov/vuln/detail/CVE-2016-2147

https://nvd.nist.gov/vuln/detail/CVE-2016-2148

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