Westermo-24-15: Potential vulnerability in WeOS affecting link layer discovery protocol

Severity: **MEDIUM** 2024-11-18

Description

WeOS utilizes several different third-party components that provide vital services to Westermo products. To provide Link-Layer notifications to adjacent network devices, WeOS utilize LLDP (Link Layer Discovery Protocol), an industry standard protocol designed to supplant proprietary Link-Layer protocols. The component providing LLDP introduced potential vulnerability in certain WeOS versions.

Affected versions

CVE-2023-41910

Affects all versions of WeOS 4 to and including version 4.33.2

Affects all versions of WeOS 5 to and including version 5.18.0

Impact

By crafting a CDP PDU packet with specific CDP_TLV_ADDRESSES TLVs, a malicious actor on an adjacent network force the lldpd daemon to perform an out-of-bounds read on heap memory.

Severity

Base score	The CVSS severity base score is 9.8
Environmental	The CVSS Environmental score has been calculated to 6.1
Vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/AR:L/MAV:A/MAC:H/MI:L/MA:L

Mitigation

We recommend updating to the latest version of WeOS 5 or WeOS 4 to resolve the vulnerabilities mentioned in this advisory.

Updates

WeOS 5 – With the release of WeOS 5 version 5.19.0 the vulnerability has been removed.

WeOS 4 – With the release of WeOS 4 version 4.34.0 the vulnerability has been removed.

WeOS version 4.34.0 and WeOS 5.19.0 are available for download at Westermo Network Technologies support site.

References

WeOS - Westermo Operating System ▷ Westermo https://www.westermo.com/solutions/weos

CVE-2023-41910 : lldpd: https://nvd.nist.gov/vuln/detail/CVE-2023-41910

Revision History

Nov 18, 2024: Initial release