Westermo-25-11: Improper Restriction of Communication Channel During Bootup

Severity: **HIGH** Publication date: 2025-10-16

Description

Westermo have identified an issue in WeOS 5 where a reboot can cause the device to temporarily expose ports to the network before the device firewall rules have been applied. This issue can lead to having communication channels established that otherwise should be blocked by the firewall. The duration of unintended exposure is limited to the bootup time of the device.

For this vulnerability to be exploitable an adversary must be able to time the attack with the device bootup duration. If the adversary can trigger multiple device reboots, the total duration of exposure will be extended.

Affected versions

Westermo products running any of the following WeOS versions are affected:

OS	Vulnerable versions	Fixed in version
WeOS 5	From 5.9.0 to and including 5.25.2	5.25.4
WeOS 4	(Not affected)	-

Impact

An adversary could exploit the temporarily exposed ports to establish a communication channel that would otherwise be blocked by the firewall rules. The communication channel could potentially be established from both inside and outside the network depending on the adversary attack vector.

Severity

Base score	The CVSS severity base score is 7.4
Environmental	-
Vector string	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:L

Mitigation

Updates

Westermo recommends upgrading to the latest WeOS version available at the Westermo Network Technologies support site. The vulnerability has been removed with the following release:

- WeOS 5.25.4

Workarounds

If an upgrade is not possible, the following actions can be performed to mitigate the vulnerability:

- Limit network access to where the vulnerable device resides

Recommendations

After performing any of the mitigations the following steps are recommended:

- Monitor network devices for reboots
- Monitor network traffic for potential malicious traffic during device bootups

References

- WeOS - Westermo Operating System: https://www.westermo.com/solutions/weos
- CWE-923: Improper Restriction of Communication Channel to Intended Endpoints

Revision History

- 2025-10-16: Initial release