Westermo-26-04: WeOS ICMP - Denial-of-Service via Echo Reply (CVE-2025-47268)

Impact: **LOW** Publication date: 2026-05-26

Description

Westermo products running WeOS utilize several third-party components that provide vital services. In WeOS 5, the component responsible for ICMP contains a vulnerability that may allow a crafted ICMP Echo Reply message to cause a denial of service in the ICMP service.

Exploitation requires the adversary to send ICMP packets to the vulnerable device while it is processing ICMP Echo Replies.

Affected products

OS	Vulnerable versions	Fixed in version
WeOS 5	>=5.24.0, <5.29.0	5.29.0
WeOS 4	(Not affected)	-

Impact

An adversary able to send ICMP packets to a vulnerable WeOS 5 device may use crafted ICMP Echo Reply messages to disrupt the ICMP service or cause incorrect ICMP timestamp calculations. The underlying operating system and hardware are not expected to be affected, which lower the exploitation impact.

Severity

CVSS	WeOS 5	NVD
Base score	6.5	6.5
Vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U /C:N/I:L/A:L	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U /C:N/I:L/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 5.29.0

Workarounds

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

- Temporarily disable ping alarms on vulnerable devices.
- Discard unexpected ICMP Echo Replies at network boundaries.

Recommendations

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

- Remove unused accounts.
- Restrict Operator, Engineer, and Administrator accounts to trusted users only.
- Limit Administrator account access to a small number of trusted users.
- Change the login credentials on previously vulnerable devices.
- Follow password best practices.
- Minimize exposure of the management interface.
- Limit physical access to the device console port.

Contact

Westermo strongly encourages anyone experiencing a product security issue to contact the Westermo PSIRT. Details are available under Report a vulnerability ▷ Westermo.

References

- Westermo Operating System - WeOS: https://www.westermo.com/solutions/weos
- WeOS 5 - User Guide: https://docs.westermo.com/weos/weos-5/
- CWE-190 - Integer Overflow or Wraparound: https://cwe.mitre.org/data/definitions/190.html
- NIST NVD - CVE-2025-47268: https://nvd.nist.gov/vuln/detail/CVE-2025-47268

Revision History

- 2026-05-26: Initial release