



# Westermo-25-05: CVE-2025-29906 - Improper argument handling

Severity: **HIGH**

2025-06-30

Original release date: Mar 26, 2026

## Description

WeOS utilizes several different third-party components that provide vital services to Westermo products. The component providing the capability for system management introduced a potential exploitable vulnerability in WeOS, due to improper argument handling.

## Affected versions

WeOS 5: Affects all versions of WeOS 5 up to and including 5.23.0.

*WeOS 4 is not affected.*

## Impact

A potential adversary could gain access to WeOS configuration interface, utilizing the console port on Westermo device running specified WeOS versions.

## Severity

<i>Base score</i>	The CVSS severity base score is 8.6
<i>Environmental</i>	The CVSS environmental score is 7.4
<i>Vector string</i>	<a href="#">#CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/MAV:P</a>

## Mitigation

Westermo recommends upgrading to the latest WeOS 5 version available. The threat can be reduced by physical enclosing the device and by that prevent the access to the console port.

## Updates

**WeOS 5** - With the release of WeOS 5 version 5.24.0 the vulnerability has been removed.

Additionally, Westermo have released the following versions of WeOS 5 to support customers that are not able to upgrade to the latest version of WeOS:

- 5.21.2
- 5.22.2
- 5.23.1
- 5.20.2
- 5.19.2
- 5.18.1
- 5.16.1



- 5.15.2
- 5.14.4
- 5.13.1
- 5.12.2

## References

[WeOS - Westermo Operating System ▷ Westermo https://www.westermo.com/solutions/weos](https://www.westermo.com/solutions/weos)

[CWE-233: Improper Handling of Parameters](#)

[NVD - CVE-2025-29906](#)

## Revision History

Mar 26, 2025: Initial release

Jun 30, 2025: Additional software versions released. Added reference to CVE.