Westermo-26-03: WeOS Management - Web Session Timeout Disabled by Using Multiple Tabs

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

Description

A vulnerability in WeOS 5 web session handling may prevent inactive users from being logged out when the default timeout expires. To be vulnerable, an authenticated user must leave at least two browser tabs open with the same active session.

Exploitation requires an adversary to reuse a web session left unattended in multiple browser tabs, granting access to a session that normally would have expired.

Affected products

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

Impact

An adversary may gain access to a web session that normally would have expired, left unattended by a previously authenticated user, either through access to the same browser or potentially by extracting a session cookie expected to be expired.

Severity

CVSS	WeOS 5
Base score	6.6
Vector string	CVSS:3.1/AV:P/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

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 help mitigate the vulnerability:

- Actively log out of the web management session
- Keep active web management sessions limited to one browser tab

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-613 - Insufficient Session Expiration: https://cwe.mitre.org/data/definitions/613

Revision History

- 2026-05-26: Initial release