Westermo-25-12: Improper Limitation of Pathname in Configuration Export

Severity: **MEDIUM** Publication date: 2025-11-03

Description

Westermo have identified an issue in WeOS 5 where the configuration export functionality exposes the device underlying filesystem through path traversal. This issue can lead to unintended exposure of sensitive information.

For this vulnerability to be exploitable the adversary must be authenticated as an administrator.

Affected versions

OS	Vulnerable versions	Fixed in version
WeOS 5	From 5.25.0 to and including 5.25.4	5.26.0
WeOS 4	(Not affected)	-

Impact

An adversary authenticated as an administrator will be able to export arbitrary files from the vulnerable device filesystem, potentially uncovering sensitive information.

Severity

Base score	The CVSS severity base score is 6.0
Environmental	-
Vector string	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

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 5.26.0

Workarounds

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

- Minimize network exposure of the management interface
- Limit administration account access to trusted parties
- Use best practices for administration account passwords

Recommendations

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

- Update the login credentials for previously vulnerable devices

References

- WeOS - Westermo Operating System: https://www.westermo.com/solutions/weos
- WeOS User Guide: https://docs.westermo.com/weos/weos-5/
- CWE - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Revision History

- 2025-11-03: Initial release