Westermo-26-05: WeOS File Import - Improper Preservation of Permissions (CVE-2026-35385)

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

Description

Westermo products running WeOS rely on several third-party components that provide essential services. In WeOS 5, a vulnerability in the file transfer component enabling the secure copy protocol can cause transferred files to retain their original permissions.

This vulnerability can only be exploited by an authenticated Engineer or Administrator, and its impact is lowered because WeOS CLI or Web UI cannot execute the transferred files.

Affected products

OS	Vulnerable versions	Fixed in version
WeOS 5	>=5.25.0, <5.29.0	5.29.0
WeOS 4	(Not affected)	-

Impact

An authenticated Engineer or Administrator can transfer files to a vulnerable WeOS 5 device while preserving their original permissions, including SUID and GUID bits. However, because transferred files cannot be executed through the WeOS CLI or Web UI, successful exploitation also requires shell access via an Administrator account, which limits the practical impact.

Severity

CVSS	WeOS 5	NVD
Base score	7.0	8.1
Vector string	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/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 be performed to mitigate the vulnerability:

- Transfer files only from trusted sources.
- Only allow SSH on internal interfaces.
- Disable SSH external-access if it has been activated.
  (Disabled by default; see WeOS CLI: configure > management > ssh > external-access)

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-281: Improper Preservation of Permissions
  https://cwe.mitre.org/data/definitions/281
- NIST NVD - CVE-2026-35385:
  https://nvd.nist.gov/vuln/detail/CVE-2026-35385

Revision History

- 2026-05-26: Initial release