Westermo-25-01: HTTP Application Session Hijacking

Severity: **MEDIUM** 2025-03-26

Description

Westermo have identified an issue where a threat actor potential could gain unauthorized access to a device. The entropy for the session ID's used during web sessions are not strong enough and thereby rendering WeOS potentially vulnerable to application session hijacking. A threat actor could hijack the insufficiently protected HTTP session token to gain unauthorized access to a device. A threat actor could obtain HTTP session tokens if the tokens are sent unencrypted over the network or if the site is vulnerable to cross-site scripting (XSS).

Affected versions

WeOS 4: Affects all versions of WeOS 4 up to and including 4.34.0

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

Impact

Potentially a threat actor could gain unauthorized access to a device with a potential loss of integrity as impact.

Severity

Base score	The CVSS severity base score is 7.5
Environmental	The CVSS Environmental score has been calculated to 6.5
Vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/MAV:A

Mitigation

For WeOS 5 Westermo recommends an upgrade to the latest WeOS 5 version available.

If an upgrade is not possible, we recommend the following actions to mitigate the listed vulnerabilities:

- Limit web access from external interfaces, by e.g. disable administrative access to WebGUI on outward facing interfaces
- Limit administration account access to trusted parties.
- Use best practices for passwords related to administration accounts.
- Additionally, completely disable the WebGUI to eliminate the risk associated with the vulnerability and thereby disable the web service capability.

Updates

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

WeOS 4 - Currently no update is available

WeOS 5.24.0 are available for download at Westermo Network Technologies support site.

References

WeOS - Westermo Operating System ▷ Westermo https://www.westermo.com/solutions/weos

CWE-384: Session Fixation

Revision History

Mar 26, 2025: Initial release