Westermo-25-08: Sensitive Information in logging

Severity: **HIGH** 2025-06-30

Description

Westermo have identified an issue where a threat actor potential could gain unauthorized access to sensitive information.

Affected versions

WeOS 5: Affects all versions of WeOS 5 version from 5.24.0

WeOS 4 is not affected.

Impact

Due to verbose logging, sensitive information like credentials is written to a log file that can be read by users authorized to read syslog files. A potential adversary could gain access to sensitive information through system logging information.

Severity

Base score	The CVSS severity base score is 8.5
Environmental	The CVSS environmental score is 8.1
Vector string	#CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/MAV:A

Mitigation

Westermo recommend the following actions to mitigate the vulnerability:

- Limit administration account access to trusted parties. Regularly review and update the list of trusted parties to ensure only current and necessary personnel have access
- Store audit records on an independent syslog server. Ensure the syslog server is hardened and regularly updated to protect against vulnerabilities. Implement access controls and encryption for the stored audit records to prevent unauthorized access
- Enable TLS for remote logs. Use strong cipher suites and enforce the use of TLS 1.2 or higher to ensure secure communication.

Updates

Currently no update is available.

References

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

CWE - CWE-532: Insertion of Sensitive Information into Log File (4.17)

Revision History

Jun 30, 2025: Initial release