Westermo-24-04: CVE-2023-40544 – Exchange of sensitive information in clear text

Severity: **MEDIUM** 2024-05-06

Description

In HTTP Auth, credentials and session id are sent as plain text and can potentially be captured by anyone capable of intercepting traffic on the network.

This is a limitation of the HTTP protocol, Westermo encourage that the HTTP access to the WebGUI is disabled.

Affected versions

Westermo products running WeOS version 4.33.2 and older, and Westermo products running WeOS version 5.20.1 and older

Impact

If an attacker intercepts login credentials and session id, they can use this information to change the configuration of the attacked device.

Severity

Base score	The CVSS severity base score is 5.7
Environmental	-
Vector string	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

Mitigation

We recommend all users to disable WebGUI HTTP access and instead enable HTTPS access to WebGUI. Additionally, we recommend the following mitigations that do not require an update:

- Disable access to WebGUI on outward facing interfaces.
- Limit administration account access to trusted parties.
- Use best practices for passwords related to administration accounts.

References

ICS Advisory: Westermo Lynx 206-F2G | CISA

CWE - CWE-319: Cleartext Transmission of Sensitive Information (4.14) (mitre.org)

Credits

Westermo thanks Aarón Flecha Menéndez, Iván Alonso Álvarez and Víctor Bello Cuevasand and Aviv Malka, for identifying and reporting these vulnerabilities.

Revision History

May 06, 2024: Initial release