Westermo-24-02: Code injection in web interface for WeOS products

CRITICAL / HIGH / **MEDIUM** / LOW Last revised: 2024-11-11

Original release date: Feb 23, 2024

Description

This Security Advisory covers the following CVEs affecting Westermo products running WeOS (versions as per section Affected versions):

1. CVE-2023-45735 (ICSA-24-023-04 3.2.3)

A requirement for the described CVEs is that the attacker must first be authenticated by using an administrator account. The vulnerability provides the capability to perform Code injection in the products web-based configuration GUI (WebGUI).

The attacker can inject malicious JavaScript code in the SNMPv3 router setting which will later be executed when a legitimate user accesses the web section where the information is displayed.

Affected versions

Westermo products running WeOS 4 versions 4.12.1 and later.

Westermo products running WeOS 5 versions to and including 5.20.1

Impact

The impact is restricted by the access level required. In general, malicious JavaScript code can manipulate data sent to and from the device. As JavaScript executes in the client's environment it can be assumed that a malicious script could access data in the client executing environment.

Severity

Base score	The CVSS severity base score for CVE-2023-45735 is 8.0.
Environmental	The CVSS severity environmental score is 5.4
Vector string	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/CR:M/IR:M/AR:M/MAV:A/MAC:L/MPR:H/MUI:R/MC:L/MI:L/MA:L

Mitigation

Workarounds

We recommend the following mitigations that do not require an update:

- 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 minimize the risk associated with the vulnerability.

Updates

- For devices running WeOS 5: Update to firmware 5.22.0 or later, available from Westermo support.

References

ICS Advisory: Westermo Lynx 206-F2G | CISA

CVE: CVE-2023-45735: Code injection in Web application

Revision History

Nov 11, 2024: Updated affected versions and added information on upgrade options

Feb 23, 2024: Initial release