Westermo-24-01: Vulnerabilities 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-2023-40143
2. CVE-2023-42765
3. CVE-2023-45222
4. CVE-2023-45227

A common requirement for all four CVEs is that to successfully be able to inject a payload to the vulnerable field(s), the attacker must first be authenticated by using an administrator account on the products web-based configuration GUI (WebGUI).

1. **CVE-2023-40143**: An attacker with access to the web application that has the vulnerable software could introduce arbitrary JavaScript by injecting a cross-site scripting payload into the “forward.0.domain” parameter.
2. **CVE-2023-42765**: An attacker with access to the vulnerable software could introduce arbitrary JavaScript by injecting a cross-site scripting payload into the "username" parameter in the SNMP configuration.
3. **CVE-2023-45222**: An attacker with access to the web application that has the vulnerable software could introduce arbitrary JavaScript by injecting a cross-site scripting payload into the "autorefresh" parameter.
4. **CVE-2023-45227**: An attacker with access to the web application with vulnerable software could introduce arbitrary JavaScript by injecting a cross-site scripting payload into the "dns.0.server" parameter.

Affected versions

Westermo products susceptible to one or more of the vulnerabilities listed in this document:

- WeOS 4 to and including version 4.33.2,
- WeOS 5 to and including version 5.20.1

Impact

When a user is authorized as administrator, it’s possible to introduce arbitrary JavaScript by injecting cross-scripting payload and by that change access data transferred between the device and the client.

Classified as Public - Contains information intended for public use

Severity

Base score	1. CVE-2023-40143: **5.4** 2. CVE-2023-42765: **5.4** 3. CVE-2023-45222: **5.4** 4. CVE-2023-45227: **5.4**
Environmental score	As the base score is within the medium classification range (CVSSv3.1 severity base score between 4.0 and 6.9) no environmental score has been calculated.
Vector string	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N (5.4)

Mitigation

Workarounds

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 minimize the risk associated with the vulnerability and there by disable the web service capability.

Updates

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

References

Download WeOS | Westermo Operating System

ICS Advisory: Westermo Lynx 206-F2G | CISA

CVEs

1. https://nvd.nist.gov/vuln/detail/CVE-2023-40143
2. https://nvd.nist.gov/vuln/detail/CVE-2023-42765
3. https://nvd.nist.gov/vuln/detail/CVE-2023-45222
4. https://nvd.nist.gov/vuln/detail/CVE-2023-45227

Revision History

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

Feb 23, 2024: Initial release

Classified as Public - Contains information intended for public use