WEOS-24-03: Potential information disclosure vulnerability in WeOS

CRITICAL / HIGH / **MEDIUM** / LOW 2024-11-11

Original release date: Apr 05, 2024

Description

Unauthorized exposure of information through directory listing.

It is possible to use the WebDAV PROPFIND method to browse web directories on the server and discover content that would normally remain hidden. This could potentially allow an attacker to obtain sensitive information, such as data files and backup pages, or give them information about the directory structure that could be useful in mounting a more sophisticated attack later.

Affected versions

Westermo products running any of the following WeOS operating system versions are susceptible to the vulnerability:

- WeOS 4 from and including version 4.24.0
- WeOS from and including version 5.14.0 to and including 5.20.1

Impact

A specific HTTP request utilizing WebDAV could be constructed to determine and browse the web directories of a unit.

It's been verified that the same service cannot be used to perform a destructive operation (PUT, DELETE, MKCOL, PATCH).

Severity

Base score	The CVSS severity base score is 5.3.
Environmental	The CVSS severity environmental score is 4.6
Vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/CR:L

Mitigation

Workarounds

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.
- Additionally, disable the WebGUI to remove 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

CWE - CWE-548: Exposure of Information Through Directory Listing (4.14) (mitre.org)

Revision History

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

Apr 05, 2024: Initial release