Westermo-24-08: Potential arbitrary code execution vulnerability in WeOS

Severity: **MEDIUM** 2024-11-20

Description

WeOS utilizes several different third-party components that provide vital services to Westermo products. The *Busybox* open-source component provides a wide set of utility commands foundational to WeOS. A security related update of Busybox has been released to fix multiple vulnerabilities that impact Westermo WeOS devices, including the vulnerability CVE-2022-48174 and CVE-2022-28391.

Affected versions

Affects Westermo products running WeOS 5 to and including version 5.19.1

Affects Westermo products running WeOS 4 to and including version 4.32.2

Impact

WeOS utilizes the open-source component Busybox to provide many of its internal functions.

Severity

With the release of several vulnerabilities have been removed including the CVE-2022-48174:

Base score	The CVSS 3.1 severity base score is 9.8
Environmental	The CVSS Environmental score have been calculated to 6.7
Vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV :L/MPR:H

Mitigation

We recommend updating to the latest version of WeOS 4 or WeOS 5 to resolve the vulnerabilities mentioned in this advisory.

If an update is not possible, we recommend the following mitigations that do not require an update:

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

Updates

Mitigated in WeOS version 5.34.0, which is available for download.

Mitigated in WeOS version 5.20.0, which is available for download.

References

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

CVE-2022-48174: Busybox: https://nvd.nist.gov/vuln/detail/CVE-2022-48174

https://www.busybox.net/about.html

Revision History

Nov 20, 2024: Initial release