Westermo-24-10: Potential denial-of-service vulnerability

Severity: **LOW** 2024-11-11

Description

Due to a vulnerability in a software component in WeOS, certain versions of WeOS could be vulnerable to a Denial-of-Service attack.

Affected versions

Affects WeOS 5 from version 5.3.0 to and including version 5.20.1

Impact

The vulnerability could allow attackers with admin access to cause a denial of service (stack consumption and application crash) via a crafted JSON file.

Severity

Base score	The CVSS severity base score is 7.5
Environmental	The CVSS Environmental score has been calculated to 3.9
Vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/ MAV:L/MAC:H/MPR:H/MUI:N/MS:U/MA:H

Mitigation

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

Workarounds

Additional general recommendations that reduce but not eliminates risk associated with the above vulnerabilities:

- Limit administration access from external interfaces, by e.g. disable administrative access on outward facing interfaces
- Limit administration account access to trusted parties.
- Use best practices for passwords related to administration accounts.

Updates

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

References

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

CVE-2016-4074: jq https://nvd.nist.gov/vuln/detail/CVE-2016-4074

Revision History

Nov 11, 2024: Initial release