Westermo-26-07: Linux Kernel IPv4 TCP Use-After-Free (CVE-2026-98432)

Impact: **HIGH** Publication date: 2026-11-11

Description

Westermo products utilize several third-party components that provide vital services. The Linux kernel, which provides IPv4 TCP networking capabilities, contains the vulnerability CVE-2026-98432.

For this vulnerability to be exploitable the adversary must be able to send multiple IPv4 TCP packets with maliciously crafted IP options to a listening service, with precise timing between concurrent connections managed by a multi-core processor. Public reporting has focused on multipath TCP (MPTCP), but any IPv4 TCP listener may reach the vulnerable code.

Westermo is not aware of any active exploitation of this vulnerability in Westermo products.

Affected products

The affected products are determined by the Linux kernel version included in each release. Linux kernel 4.4 and later is affected.

OS	Products and versions	Fixed in version
WeOS 5	All WeOS 5 products: - From 5.15.0 up to latest	Not yet released
WeOS 4	Viper-112A/-212A/-120A/-220A/-108/-208: - From 4.22.0 up to latest	Not yet released
WeRT OS	All WeRT OS-driven products - All WeRT OS releases	Not yet released
VAWRT	All Merlin-series and GW-series products.	Not yet released
IbexOS	All IbexOS driven products	Not yet released

Impact

An adversary with network access to an IPv4 TCP service on a vulnerable device could send maliciously crafted packets to trigger a use-after-free condition, potentially disclosing or corrupting kernel memory or causing a kernel crash. Successful exploitation may result in code execution or interrupt the operation of the targeted device.

Any service accepting incoming IPv4 TCP connections may be affected, including SSH, HTTP/HTTPS, DNS and SSL VPN via TCP or multipath TCP.

Classified as Public - Contains information intended for public use

Westermo rates the attack complexity as high, as successful exploitation depends on winning a race condition between concurrent connections and additional preparation of kernel memory.

Severity

CVSS	Westermo	NVD
Base score	8.1	9.8
Vector string	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Mitigation

Updates

As of the time this advisory is published, none of the listed products have been released with a patched Linux kernel. Westermo is actively monitoring the issue and plan to release patched versions.

Westermo recommends upgrading to the latest release that includes the fix once it is available.

Workarounds

If an upgrade is not possible, the following actions can be performed to reduce exposure to the vulnerability:

- Disable IPv4 TCP services that are not needed.
- Apply firewall rules to restrict IPv4 TCP services to trusted networks.
- If upstream firewalls support it, discard IPv4 packets carrying IP options. This may affect legitimate traffic, see Red Hat and Amazon references for firewall rules.
- Change configurations from multipath TCP to regular TCP. This will not mitigate the vulnerability but remove exposure to a known exploit path.

Recommendations

After performing any of the mitigations, the following steps are recommended:

- Minimize network exposure of the management interfaces.
- Actively monitor networks for IPv4 TCP packets with IP options.
- Monitor logs and device status for unexpected reboots.
- Remove unused accounts.
- Update the login credentials for previously vulnerable devices.
- Use best practices for account passwords.

Contact

Westermo strongly encourages anyone who is experiencing a product security issue to contact Westermo PSIRT. Details are available under Report a vulnerability | Westermo.

References

- Westermo Products:
  https://www.westermo.com/products/product-lines-and-brands
- CWE-416: Use After Free:
  https://cwe.mitre.org/data/definitions/416.html
- NVD – CVE-2026-98432:
  https://nvd.nist.gov/vuln/detail/CVE-2026-98432
- Ubuntu Blog – Fixes available in -proposed pocket for CVE-2026-98432:
  Fixes available in -proposed pocket for CVE-2026-98432 | Ubuntu
- Red Hat – Security Bulletin RHSB-2026-016 (CVE-2026-98432):
  https://access.redhat.com/security/vulnerabilities/RHSB-2026-016
- Amazon AWS – CVE-2026-98432 - Linux kernel IPv4 TCP use-after-free Issue
  https://aws.amazon.com/security/security-bulletins/2026-160-aws/
- Akamai - CVE-2026-98432: Remote use-after-free in the Linux kernel TCP stack:
  https://www.akamai.com/blog/security-research/cve-2026-98432-remote-uaf-linux-kernels-tcp-stack

Revision history

- 2026-11-11: Initial release

Classified as Public - Contains information intended for public use