Westermo-26-08: Viper 3000- and Lynx 3000-series Bootloader Signature Bypass

Impact: **HIGH** Publication date: 2026-11-16

Description

Westermo products running WeOS utilize several third-party components that provide vital services. The component providing the bootloader capability has introduced a vulnerability in the Viper 3000- and Lynx 3000-series with Secure Boot enabled. Even if the firmware boot image signature check is successful the bootloader may be tricked into loading unsigned parts.

For this vulnerability to be exploitable the adversary must either be authenticated with permission to perform an upgrade or have physical access to a vulnerable device and be able to supply a modified boot image.

Affected products

Product	**Vulnerable versions**	**Fixed in version**
Viper 3000	Bootloader up to and including v2024.03.0-5 delivered with WeOS 5: - From 5.22.0 up to and including 5.31.0	Bootloader v2024.03.0-6 delivered with WeOS 5: - 5.31.1 and later
Lynx 3000	Bootloader up to and including v2024.03.0-5 delivered with WeOS 5: - From 5.22.0 up to and including 5.31.0	Bootloader v2024.03.0-6 delivered with WeOS 5: - 5.31.1 and later

Impact

An attacker with access right allowing performing firmware upgrades may cause the bootloader to load parts of a boot image that are not covered by the signature verification. This compromises the chain of trust required for Secure Boot.

Westermo rates the impact severity as HIGH due to its potential impact on the operating system integrity.

Severity

CVSS	**Westermo**
Base score	7.8
Vector string	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Classified as Public - Contains information intended for public use

Mitigation

Updates

Westermo recommends upgrading to the latest WeOS version available at the Westermo Network Technologies support site. The vulnerability has been removed with the following release:

- Bootloader v2024.03.0-6 delivered with WeOS 5:
    - From 5.31.1 and later

Detailed instructions for upgrading the bootloader are available in the WeOS 5 release notes.

Workarounds

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

- Only upgrade using signed WeOS packages (.pkg) downloaded from the Westermo Network Technologies support site.
- Manually verify the hash sum of Westermo signed images before applying updates.
- Restrict Operator, Engineer and Administrator accounts to trusted users only.
- Limit physical access to the device.

Recommendations

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

- Minimize exposure of the management interface.
- Monitor logs and device status for unexpected changes and reboots.
- Remove unused accounts.
- Update login credentials for previously vulnerable devices.
- Follow best practices for account passwords.

Contact

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

Classified as Public - Contains information intended for public use

References

- Westermo Products – Product Lines and Brands
  https://www.westermo.com/products/product-lines-and-brands
- Westermo Products – Viper 3000-series:
  https://www.westermo.com/products/product-lines-and-brands/viper/viper-3000
- Westermo Products - Lynx 3000-series
  https://www.westermo.com/products/product-lines-and-brands/lynx/lynx-3000
- Westermo Operating System - WeOS:
  https://www.westermo.com/solutions/weos
- WeOS 5 – User Guide:
  https://docs.westermo.com/weos/5/
- CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data
  https://cwe.mitre.org/data/index.html

Revision history

- 2026-11-16: Initial release

Classified as Public - Contains information intended for public use