Westermo-26-01: Viper 3000 Bootloader Signature Verification Bypass

Severity: **HIGH** Publication date: 2026-03-31

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-series with Secure Boot enabled, where the verification of Westermo signed images can be bypassed due to an improper verification of the cryptographic signature.

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.

Affected products

Product	Vulnerable versions	Fixed in version
Viper 3000-series	Bootloader up to and including v2024.03.0-3 delivered with WeOS 5.22.0 up to and including 5.28.0	Pending

Impact

An adversary authenticated as an Operator, Engineer, or Administrator on a vulnerable Viper 3000-device can potentially bypass the bootloader signature check, enabling to load an altered image, compromising the chain of trust required for Secure Boot.

Severity

CVSS	WeOS 5
Base score	7.1
Vector string	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Mitigation

Updates

As of the time this advisory is published, a version of WeOS 5 has not been released with a patched bootloader.

When a new WeOS 5 release package is available it is necessary to verify that the bootloader has been upgraded to mitigate the vulnerability.

Workarounds

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

- Limit roles Operator, Engineer and Administrator account access to trusted parties

- Remove unused accounts
- Use best practices for account passwords
- Minimize network exposure of management interface
- Minimize physical access to the device console port

Recommendations

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

- Monitor logs and device status for unexpected changes and reboots
- Update the login credentials for previously vulnerable devices

References

- Westermo Products - Viper-3000 series: https://www.westermo.com/products/product-lines-and-brands/viper/viper-3000
- Westermo Operating System - WeOS: https://www.westermo.com/solutions/weos
- WeOS 5 - User Guide: https://docs.westermo.com/weos/weos-5/
- CWE-347: Improper Verification of Cryptographic Signature: https://cwe.mitre.org/data/definitions/347.html

Revision History

- 2026-03-31: Initial release