SECURITY VULNERABILITY NOTICE

CVE-2026-37243 — Cross-Site Scripting in PMP 450b High Gain Subscriber Module
Published: March 2026

Summary

A stored cross-site scripting (XSS) vulnerability has been identified in the web management interface of the Cambium Networks PMP 450b High Gain Subscriber Module. An authenticated attacker able to access the device management interface could inject malicious script content that would subsequently execute in the browser of another authenticated user viewing the affected page. Successful exploitation could allow session hijacking, unauthorised configuration changes, or further actions within the management context.

There is no evidence of exploitation in the wild.

CVE ID: CVE-2026-37243 *(reserved — full details will be published to the NVD and downstream databases as the record is enriched)* **CWE:** CWE-79 — Improper Neutralisation of Input During Web Page Generation (Cross-site Scripting)

Affected Products

Product	Affected Firmware
PMP 450b High Gain Subscriber Module	All versions prior to 25.0.1

Resolution

This vulnerability is resolved in firmware version **25.0.1**, released March 2026. Customers are strongly advised to upgrade.

Firmware is available from the Cambium Networks Support Portal

---

Recommended Mitigations (Until Upgrade Is Possible)

- Restrict management interface access to trusted administrative hosts using IP access controls or upstream firewall rules.
- Disable remote management access from untrusted or public-facing networks.
- Limit management interface access to the minimum number of authorised users.

Acknowledgements

Cambium Networks thanks Antonio De Turris from **Secure Network Srl** (www.securenetwork.it) for responsibly disclosing this vulnerability through coordinated disclosure.

References

- CVE-2026-37243 *(CVE reserved — customers are advised to check back as additional details are published)*
- NVD Entry *(pending enrichment)*
- Security contact: security@cambiumnetworks.com