WAVLINK-SA-2026-091301: Arbitrary File Write in WN535M1

Published 2026-09-13 10:00 UTC+8 Severity **Critical**

Status **Analyzed**

Abstract

WAVLINK WN535M1 and WN535M3 routers running firmware prior to M35M1_V250922 contain an unauthenticated arbitrary file write vulnerability that allows remote attackers to overwrite any file on the device by sending a crafted payload to the sync_server daemon on TCP port 13136. The daemon, which runs as root and requires no authentication, accepts a 100-byte filename field in its protocol header without path canonicalization, allowing attackers to supply an absolute path and write arbitrary content to overwrite startup scripts or credential stores to achieve persistent system compromise. This vulnerability was reported together with CVE-2026-89010 (unauthenticated OS command injection in the same sync_server daemon on TCP port 13136); both issues affect the same models and are addressed by the same firmware release.

Affected Products

Product	Affected Firmware	Fixed Firmware	Availability
WN535M1 Wi-Fi Router	`Prior to M35M1_V250922` and earlier	`M35M1_V250922 or later`	Available now · Download

Detail

WAVLINK WN535M1 and WN535M3 routers running firmware prior to M35M1_V250922 contain an unauthenticated arbitrary file write vulnerability that allows remote attackers to overwrite any file on the device by sending a crafted payload to the sync_server daemon on TCP port 13136. The daemon, which runs as root and requires no authentication, accepts a 100-byte filename field in its protocol header without path canonicalization, allowing attackers to supply an absolute path and write arbitrary content to overwrite startup scripts or credential stores to achieve persistent system compromise. This vulnerability was reported together with CVE-2026-89010 (unauthenticated OS command injection in the same sync_server daemon on TCP port 13136); both issues affect the same models and are addressed by the same firmware release. Tracked as `CVE-2026-89009` · CVSS v3.1 **9.1** `(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)`

Solution

Update the firmware to version `M35M1_V250922 or later` or later.

Acknowledgement

Thanks to **Cam Smith** for reporting this vulnerability.

Reference

`CVE-2026-89009` · NVD entry

Coordinated disclosure practice · security@wavlink.com