

NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-76589

Summary

CVE-2026-76589 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. A vulnerability was found in TRENDnet TEW-755AP up to 20260702. Affected is the function FUN_401000 of the file /sbin/mycli. The manipulation of the argument ssid results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used.

What we know

- **CVE:** CVE-2026-76589
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.9 Critical, Network-exploitable, no user interaction (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 1%

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, limit network exposure of the affected service and tighten access until patched. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.