NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-77946

Summary

CVE-2026-77946 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 determined in TRENDnet TEW-821DAP 2.2.01b05. Affected by this vulnerability is the function uci_safe_get of the file /cgi-bin/apply_time.cgi of the component NTP Timezone Configuration Handler. Executing a manipulation of the argument system.ntp.server/system.ntp.enable_server/cameo.time.time_zone/cameo.cameo.syslog_server can lead to stack-based buffer overflow. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.

What we know

- **CVE:** CVE-2026-77946
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 10.0 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/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, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. 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.