NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-78050

Summary

CVE-2026-78050 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 Comfast CF-N1-S 2.6.0.1. The affected element is the function sub_41AD7C of the file /cgi-bin/mbox-config?method=SET&section=ntp_timezone of the component Web Management. The manipulation of the argument timestr/ntp_client_enabled results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been made public and could be used.

What we know

- **CVE:** CVE-2026-78050
- **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.