

NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-78168

Summary

CVE-2026-78168 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 security vulnerability has been detected in EFM ipTIME T24000M up to 14.20.0. This affects the function `httpcon_check_session_url` of the component Session Validation Handler. Such manipulation leads to improper authentication. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.

What we know

- **CVE:** CVE-2026-78168
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.8 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/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.