NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-18616

Summary

CVE-2026-18616 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 identified in GL-iNet GL-MT3000 up to 4.4.5. The impacted element is the function server.set_peer of the file /cgi-bin/glc of the component wg-server.so Native Plugin. The manipulation of the argument public_key leads to command injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure and confirmed the existence of the vulnerability.

What we know

- **CVE:** CVE-2026-18616
- **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):** 2%

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.