NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-70615

Summary

CVE-2026-70615 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. boringproxy through 0.10.0 contains a newline injection vulnerability that allows authenticated low-privileged users with tunnel-creation permission to inject arbitrary lines into the server account's SSH authorized_keys file by supplying a percent-encoded newline character in the domain parameter of the tunnel creation endpoint. Attackers can insert an unrestricted public key entry into authorized_keys to gain persistent shell access, and subsequently read cleartext credentials from the database file including all user tokens, tunnel private keys, and TLS certificates.

What we know

- **CVE:** CVE-2026-70615
- **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)

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.