NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-67324

Summary

CVE-2026-67324 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. GitPython 3.1.50 fails to recognize joined short-option forms such as -u (the short form of --upload-pack=) when enforcing its default unsafe-option gate. When an application passes attacker-influenced clone options into Repo.clone_from(..., multi_options=..., allow_unsafe_options=False), an attacker can supply -u to bypass the gate that blocks --upload-pack/-u, causing Git to execute the specified helper command during clone. Fixed in 3.1.51.

What we know

- **CVE:** CVE-2026-67324
- **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):** 0%

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.