NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-75913

Summary

CVE-2026-75913 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. CodeWhale (codewhale / codewhale-tui) versions >= 0.8.41 and < 0.8.64 contain an argument injection vulnerability in the git_show tool. The model-supplied rev parameter is passed unvalidated into the git show argv without an --end-of-options sentinel, so a value beginning with --output= is interpreted as a git flag. Because the tool is registered as auto-approved and advertised as read-only, an attacker (via a malicious repository combined with prompt injection) can cause an unprompted arbitrary file write at the privilege of the invoking user, targeting sensitive files such as ~/.ssh/authorized_keys, ~/.bashrc, or ~/.gitconfig. Fixed in 0.8.64 by adding rev validation.

What we know

- **CVE:** CVE-2026-75913
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.3 Critical, Network-exploitable, no privileges required (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/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.