NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-67622

Summary

CVE-2026-67622 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. Flowise through 3.1.4 contains an insecure direct object reference vulnerability in the OpenAI Assistants integration that allows authenticated attackers to access credentials belonging to other workspaces by supplying an arbitrary credential UUID to Assistants endpoints without workspace ownership verification. Attackers can enumerate cross-workspace assistant metadata, retrieve file and vector store listings, and upload files into victim workspaces by exploiting the missing workspace-scoped authorization check in the credential lookup logic.

What we know

- **CVE:** CVE-2026-67622
- **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:L)

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.