

NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-73034

Summary

CVE-2026-73034 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. DB-GPT v0.8.1 contains an unauthenticated path traversal vulnerability that allows remote attackers to write arbitrary files to any location on the server by injecting directory traversal sequences into the user_id HTTP header of the Python file-upload endpoint. Attackers can send a crafted multipart upload request with a traversal-poisoned user_id header to escape the intended upload directory and write attacker-controlled content to locations such as Python startup hooks, cron directories, or agent scripts, resulting in remote code execution.

What we know

- **CVE:** CVE-2026-73034
- **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):** 1%

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.