NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-73678

Summary

CVE-2026-73678 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. MindsDB Minds Platform version 26.1.0 and earlier contains an unauthenticated remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary OS commands by submitting crafted prompts to the unprotected POST /api/v1/responses/ endpoint, which reaches the Anton agent's scratchpad tool that calls exec() on attacker-influenced Python source without sandboxing. Attackers can first configure their own LLM API key through the unauthenticated PUT /api/v1/settings/ endpoint, then POST a prompt directing the agent to invoke the scratchpad tool with arbitrary Python code, achieving full OS command execution as the user running the desktop application and enabling access to SSH keys, stored credentials, and environment secrets.

What we know

- **CVE:** CVE-2026-73678
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 10.0 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/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.