

NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-67342

Summary

CVE-2026-67342 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. ArcadeDB versions before 26.7.2 contain an authorization bypass vulnerability in HTTP handlers for time series, batch, Prometheus, and Grafana endpoints that fail to validate database access permissions. Attackers can access and modify databases they are not authorized to use by directly calling affected endpoints with arbitrary database parameters.

What we know

- **CVE:** CVE-2026-67342
- **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.