NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-69083

Summary

CVE-2026-69083 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. SiYuan versions before v3.7.3 contain SQL injection vulnerabilities in the fullTextSearchAssetContent endpoint reachable by unauthenticated users and publish RoleReader tokens. Attackers can execute arbitrary SQL on the read-write asset-content database via unescaped method parameters and REGEXP clauses to read, modify, or delete cross-notebook data.

What we know

- **CVE:** CVE-2026-69083
- **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:N)

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.