NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-65321

Summary

CVE-2026-65321 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. PyAthena prior to 3.35.4 contains a sql injection vulnerability that allows unauthenticated attackers to inject arbitrary SQL by exploiting improper quote-escaping in DefaultParameterFormatter.format(), which routes DELETE and CTAS statements to the _escape_hive function that backslash-escapes single quotes rather than doubling them. Because Athena and Trino do not treat backslashes as escape characters inside string literals, attacker-supplied input such as a single quote followed by SQL syntax causes the parser to terminate the string literal prematurely, enabling data exfiltration via UNION SELECT, execution of destructive statements, and attacker-controlled CTAS destination and content.

What we know

- **CVE:** CVE-2026-65321
- **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)

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.