NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-71472

Summary

CVE-2026-71472 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. A flaw was found in acm-search-v2-rhel9. This vulnerability allows an authenticated attacker, such as a hub administrator or a Search Custom Resource (CR) editor, to inject malicious shell commands or SQL statements. This occurs because the WORK_MEM string provided in the Search CR is not properly validated before being used in a bash script and an SQL query. Successful exploitation could lead to arbitrary code execution within the privileged postgres pod, potentially compromising the system.

What we know

- **CVE:** CVE-2026-71472
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.1 Critical, Network-exploitable, no user interaction (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/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, limit network exposure of the affected service and tighten access until patched. 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.