NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-73268

Summary

CVE-2026-73268 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 the cluster-curator-controller component of multicluster engine (MCE). A tenant with create or update permissions on ClusterCurator resources can inject an arbitrary Job specification. This is possible because the CreateJob() function does not validate user-controlled input when unmarshaling the spec.install.overrideJob raw extension. Successful exploitation allows the injected Job to run with the controller's elevated privileges, leading to arbitrary code execution and privilege escalation, potentially accessing cluster-wide secrets.

What we know

- **CVE:** CVE-2026-73268
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.9 Critical, Network-exploitable, no user interaction (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)

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.