# NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-72508

## Summary

CVE-2026-72508 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 multicloud-operators-subscription component of Red Hat Advanced Cluster Management (RHACM). This vulnerability allows a namespace-admin tenant to perform a confused-deputy attack by creating Subscription Custom Resources (CRs) that leverage a highly privileged ServiceAccount (SA). This enables the tenant to deploy arbitrary cluster-scoped resources, leading to privilege escalation and potential arbitrary code execution across the cluster.

## What we know

- **CVE:** CVE-2026-72508
- **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.*