NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-14450

Summary

CVE-2026-14450 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 MaaS API. This vulnerability allows any pod within the cluster to bypass the Kuadrant AuthPolicy gateway by forging HTTP headers, specifically `X-MaaS-Username` and `X-MaaS-Group`, which are trusted verbatim. This lack of first-party authentication enables an attacker to gain unauthorized access and escalate privileges. The concrete consequences include the ability to mint Kubernetes ServiceAccount tokens in other tenants' namespaces, revoke API keys, and exfiltrate sensitive model access configuration.

What we know

- **CVE:** CVE-2026-14450
- **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.