NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-60720

Summary

CVE-2026-60720 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. Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: OIM Legacy UI). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Identity Manager. While the vulnerability is in Oracle Identity Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Identity Manager. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).

What we know

- **CVE:** CVE-2026-60720
- **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)
- **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.