NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-56793

Summary

CVE-2026-56793 is a newly disclosed High vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. Dell OpenManage Server Administrator, versions prior to 11.1.0.2, contains an Improper Authentication vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.

What we know

- **CVE:** CVE-2026-56793
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 7.7 High, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L)

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. 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.