CISA warns of active exploitation of SAP NetWeaver and Cisco Expressway flaws



CISA says attackers are exploiting a medium-severity SAP NetWeaver flaw and a critical Cisco Expressway flaw. Both have patches available; the Expressway issue affects clustered devices.

- CVE-2025-42884 in SAP NetWeaver (CVSS 6.5) could let unauthenticated attackers leak or modify server information; SAP patched it in November 2025.
- CVE-2026-76466 in Cisco Expressway (CVSS 9.8) is a hardcoded credentials weakness that could allow system commands with root privileges.
- It affects Expressway-C and Expressway-E devices on vulnerable versions that are configured in a cluster; the fix is in release X15.5.20, issued on October 21.
- CISA added the Expressway flaw to its KEV catalog on November 20 and gave US federal agencies three days to patch.

> - F6 reported exploitation began shortly after public proof-of-concept code appeared.

The US cybersecurity agency CISA has warned that attackers are exploiting vulnerabilities in SAP NetWeaver and Cisco Expressway. Both issues already have fixes, so the priority for most organisations is to confirm that those fixes are in place.

SAP NetWeaver

CVE-2025-42884 carries a CVSS score of 6.5. It could allow an unauthenticated attacker to leak or modify server information, by injecting JNDI environment properties or passing a URL used in JNDI lookups, which leads to an unintended JNDI provider. SAP fixed it in its November 2025 security updates. The source indicates no earlier reports of exploitation before CISA's alert.

Cisco Expressway

CVE-2026-76466 is rated critical at 9.8. It stems from hardcoded credentials. Persistent cookies, combined with weak validation of client certificates in certain conditions, could let an attacker holding the cookies connect to the database service and invoke specific RPC commands, ultimately running system commands as root.

Expressway Core (Expressway-C) and Expressway Edge (Expressway-E) devices are affected when they run vulnerable versions and are configured in a cluster. Cisco patched the flaw on October 21 in Expressway Series release X15.5.20.

CISA added the flaw to its Known Exploited Vulnerabilities catalog on November 20 and set a three-day deadline for federal agencies. The Russian firm F6 had reported that exploitation began soon after proof-of-concept code was published.

What it means

The Expressway device often sits at the network edge, so a critical flaw with public exploit code deserves prompt review. The SAP issue is rated lower, but active exploitation justifies checking its patch status too.

What to do now

1. Identify all Cisco Expressway-C and Expressway-E devices and check whether they run a version earlier than X15.5.20, especially those in clusters.
2. Apply the Expressway fix as an emergency change and review logs for unexpected database service or RPC activity.
3. Confirm that SAP NetWeaver systems have the November 2025 security updates, including CVE-2025-42884.

4. Add CISA's KEV catalog as an input to your vulnerability prioritisation, so exploited flaws are patched ahead of their CVSS rank.
5. Record the exposure and remediation status for your risk register and report any suspected compromise through your incident process.