CISA Adds Four Actively Exploited Flaws in SAP, Cisco, VMware and Apache Products to KEV Catalog



CISA has added four vulnerabilities in SAP NetWeaver, Cisco Expressway, VMware vCenter and Apache Roller to its KEV Catalog, citing evidence of active exploitation. It urges all organizations to prioritize them.

- Four CVEs were added to the KEV Catalog based on evidence of active exploitation: CVE-2025-42884, CVE-2026-76466, CVE-2026-123890 and CVE-2026-129448.
- Affected products: SAP NetWeaver, Cisco Expressway Series, VMware vCenter and Apache Roller.
- The flaw types are improper neutralization in data query logic, hard-coded credentials, authentication bypass and deserialization of untrusted data.
- BOD 26-04 binds only US federal civilian agencies, but CISA encourages every organization to adopt risk-based vulnerability management and prioritize KEV entries.

CISA has added four vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog after finding evidence that they are being exploited in real attacks. CISA notes that these types of flaws are a frequent attack vector for malicious actors.

The four additions

- CVE-2025-42884: SAP NetWeaver, improper neutralization of special elements in data query logic
- CVE-2026-76466: Cisco Expressway Series, use of hard-coded credentials
- CVE-2026-123890: VMware vCenter, authentication bypass using an alternate path or channel
- CVE-2026-129448: Apache Roller, deserialization of untrusted data

The source does not give affected versions, patch details or exploitation specifics, so teams should consult the vendors' own advisories for those.

Why it matters beyond US agencies

CISA's Binding Operational Directive 26-04 requires US Federal Civilian Executive Branch agencies to remediate quickly the KEV-listed CVEs on publicly exposed assets that give full control once exploited, while deferring lower-risk items. It also sets baseline expectations for checking whether an attacker compromised a system before the patch was applied.

The directive does not apply to organizations outside those agencies. CISA nevertheless encourages all organizations to adopt risk-based vulnerability management and to prioritize KEV Catalog entries. For institutions in the Kingdom, the sensible step is to check quickly whether any of these four products are in use, and to treat any that are exposed to the internet as the first priority.

What to do now

1. Check your asset inventory for SAP NetWeaver, Cisco Expressway, VMware vCenter and Apache Roller instances.
2. Prioritize any of these that are reachable from the internet, and apply vendor fixes or mitigations as soon as they are available.
3. Review the vendors' advisories for affected versions and guidance for each CVE.
4. For exposed systems patched late, check logs and indicators for signs of compromise before the fix.
5. Add KEV Catalog monitoring to your vulnerability management process as a priority trigger.