CISA adds four actively exploited flaws in SAP, Cisco, VMware and Apache products to its KEV Catalog



CISA added four vulnerabilities in SAP NetWeaver, Cisco Expressway, VMware vCenter and Apache Roller to its KEV Catalog on 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.
- Affected products: SAP NetWeaver, Cisco Expressway Series, VMware vCenter and Apache Roller.
- Flaw types: query-logic injection, hard-coded credentials, authentication bypass and unsafe deserialization.
- BOD 26-04 binds only US federal civilian agencies, but CISA encourages all organizations to adopt risk-based vulnerability management.
- The source does not give patch versions or details of the attacks.

CISA has added four vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog after finding evidence that they are being exploited in the wild.

What was added

- **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.

CISA notes that these classes of weakness are a frequent attack vector for malicious actors.

Why it matters beyond the US federal sector

Binding Operational Directive 26-04 requires US federal civilian agencies to remediate quickly the KEV-listed CVEs on publicly exposed assets where exploitation gives total control of the asset, and to defer lower-risk items. It also sets baseline expectations for checking whether a system was compromised before the patch was applied.

The directive does not apply to organizations outside that group. Even so, CISA encourages every organization to adopt risk-based vulnerability management and to prioritize KEV Catalog entries. Organizations aware of an exploited flaw that is not listed can submit it through CISA's nomination form, provided it has a CVE ID, evidence of exploitation and clear mitigation guidance.

Suggested approach

The source does not list fixed versions or technical attack details, so consult each vendor's advisory for remediation guidance. Start by establishing whether these products exist in your environment and which are reachable from the internet.

What to do now

1. Check your asset inventory for SAP NetWeaver, Cisco Expressway, VMware vCenter and Apache Roller instances.
2. Identify which of these are exposed to the internet and treat them as first priority.
3. Follow each vendor's advisory to apply patches or mitigations for the four CVEs.
4. For exposed systems, review logs and check for signs of compromise that predate patching.
5. Add KEV Catalog monitoring to your vulnerability management process so listed CVEs are prioritized.