CISA Adds Four Exploited Flaws in Apache Roller, Cisco Expressway, SAP NetWeaver and VMware vCenter to KEV



CISA has added four flaws affecting Apache Roller, Cisco Expressway, SAP NetWeaver and Broadcom VMware vCenter to its KEV catalog, citing evidence of active exploitation. One is rated CVSS 9.8.

- CISA added four vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog on Friday.
- The affected products are Apache Roller, Cisco Expressway, SAP NetWeaver and Broadcom VMware vCenter.
- CISA cited evidence of active exploitation for all four.
- One listed flaw, CVE-2026-129448, is rated CVSS 9.8 and involves deserialization of untrusted data.

> - The source headline also points to emerging espionage attacks, but the excerpt gives no further detail.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added four vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog, saying there is evidence they are being exploited in the wild.

What was added

The affected products are Apache Roller, Cisco Expressway, SAP NetWeaver and Broadcom VMware vCenter. The source excerpt details only one entry: CVE-2026-129448, rated CVSS 9.8, a deserialization of untrusted data vulnerability. The remaining CVE identifiers and technical descriptions are not given in the material available to us, so we do not repeat them here.

The source headline also refers to espionage attacks emerging alongside this exploitation. The excerpt does not say who is behind them, which sectors are targeted or how the flaws are chained, so no attribution should be assumed.

Why it matters

KEV inclusion signals that exploitation is happening now, not only in theory. Products such as virtualization management, collaboration gateways and enterprise application platforms often sit in privileged positions, so institutions running any of these four should treat the listing as a prompt to verify their exposure promptly.

Suggested approach

Confirm whether the affected products are in your estate, including those run by third parties, then consult each vendor's advisory for fixed versions and mitigations. Prioritise internet-facing and management-plane systems, and review logs for unusual activity while patching is arranged.

What to do now

1. Check asset inventories for Apache Roller, Cisco Expressway, SAP NetWeaver and VMware vCenter, including third-party-managed instances.
2. Review each vendor's security advisory and apply fixed versions or recommended mitigations, starting with internet-facing and management systems.
3. Add the four KEV entries to vulnerability management tracking with a short remediation deadline.
4. Review logs and alerts on affected systems for signs of compromise before and after patching.
5. Restrict management interfaces to trusted networks where patching cannot be done immediately.