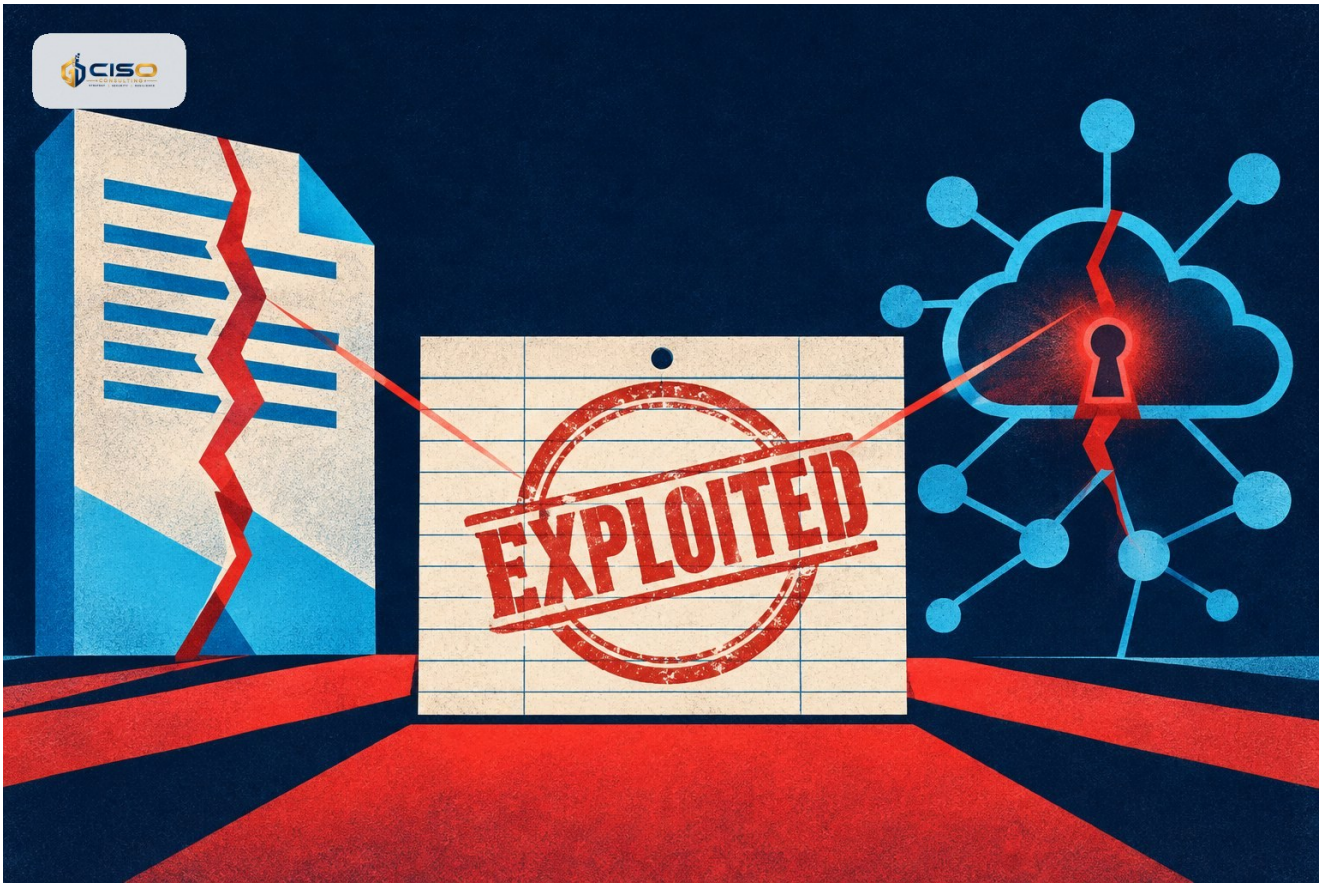
CISA adds critical Collabora Online and Arista VeloCloud flaws to its exploited-vulnerabilities list



CISA has added two critical vulnerabilities, in Collabora Online Built-in CODE Server and Arista VeloCloud Orchestrator, to its KEV catalogue after reports of active exploitation. One is CVE-2026-110447 (CVSS 9.2).

- CISA added two vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue.
- The affected products are Collabora Online Built-in CODE Server and Arista VeloCloud Orchestrator (VCO).
- CISA cites reports of active exploitation in the wild.
- Both flaws are rated critical; CVE-2026-110447 has a CVSS score of 9.2.
- The available source excerpt does not give full technical details or patch information.

What was reported

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added two vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalogue on Friday. The agency pointed to reports that both are being exploited in the wild.

The affected products are Collabora Online Built-in CODE Server and Arista VeloCloud Orchestrator (VCO). Both flaws are rated critical. One of them, CVE-2026-110447, carries a CVSS score of 9.2.

What we do not yet know

The source excerpt is limited. It does not describe the second CVE, the affected versions, the attack method or the status of vendor fixes. Organisations should therefore rely on the vendors' own advisories and the CISA KEV entries for those details rather than assume them.

Why it matters

Inclusion in the KEV catalogue signals that exploitation is not theoretical. For institutions that use these products for document collaboration or for managing wide-area network infrastructure, the sensible step is to confirm quickly whether they are exposed, then prioritise remediation according to the vendor guidance.

Recommended next steps

- Check whether either product is deployed, including in test or branch environments.
- Review vendor advisories and apply fixes or mitigations as directed.
- Look for signs of compromise where the products are reachable from untrusted networks.

What to do now

1. Inventory all Collabora Online CODE Server and Arista VeloCloud Orchestrator instances, including test and branch deployments.
2. Read the vendor advisories and CISA KEV entries to confirm affected versions and available fixes.
3. Apply patches or vendor mitigations on an emergency basis for any exposed instance.
4. Restrict internet access to management and collaboration interfaces where possible.
5. Review logs on these systems for unusual activity and escalate through your incident process if found.