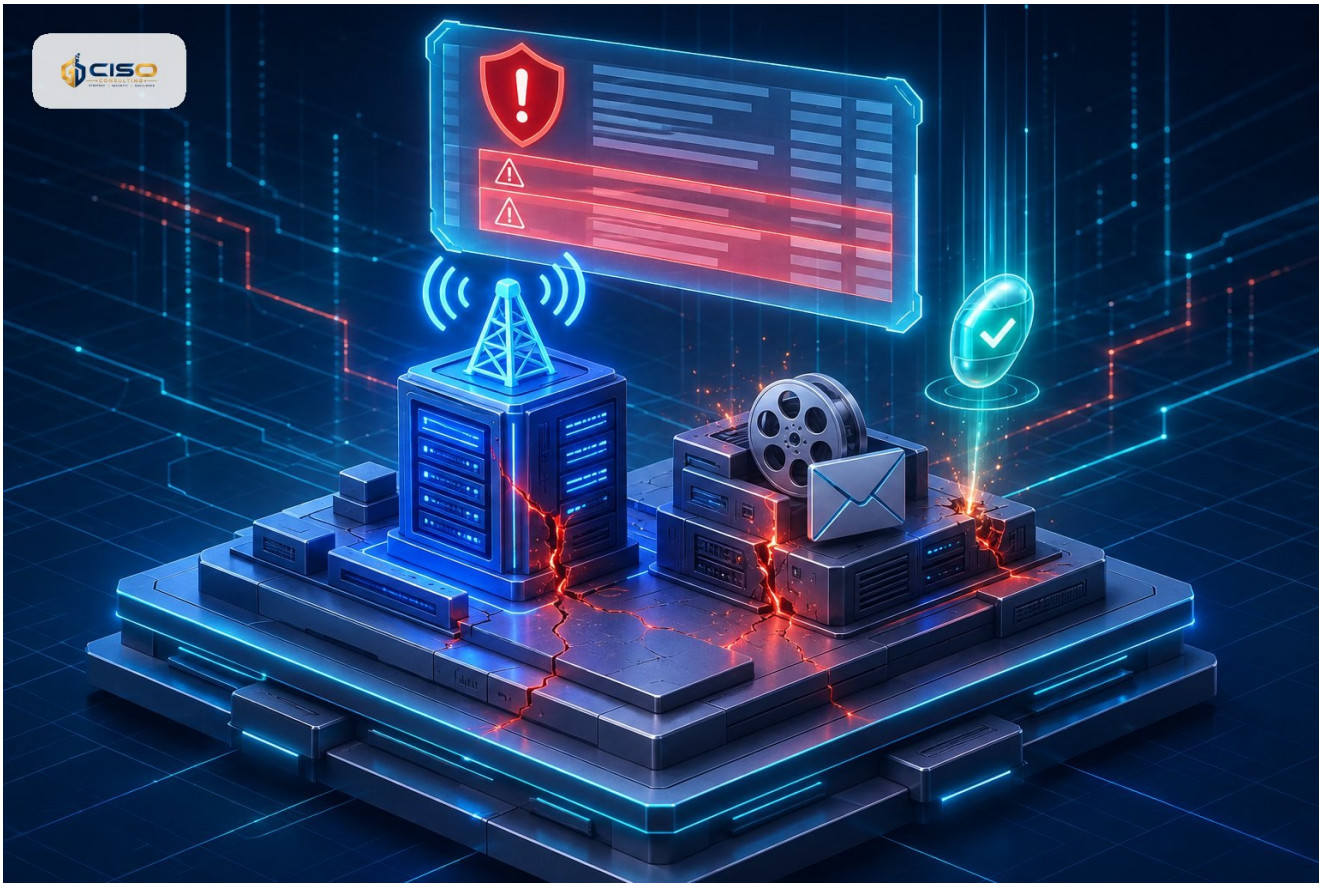
CISA Adds Cisco BroadWorks and Openwave Flaws to Exploited Vulnerabilities List



CISA has added two flaws, in Cisco BroadWorks and Openwave Messaging Webtop Media Transcoder, to its Known Exploited Vulnerabilities catalog, citing active exploitation. Patches are available, so affected organisations should apply them.

- CISA added two vulnerabilities to its KEV catalog, citing evidence of active exploitation.
- The affected products are Cisco BroadWorks and Openwave Messaging Webtop Media Transcoder.
- One flaw, CVE-2026-20320, has a CVSS score of 7.5 and involves improper restriction of XML external entity references.
- The headline states that patches are available despite the ongoing exploitation.

What happened

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added two security flaws to its Known Exploited Vulnerabilities (KEV) catalog. The agency cited evidence of active exploitation. The affected products are Cisco BroadWorks and Openwave Messaging Webtop Media Transcoder.

One of the flaws is tracked as **CVE-2026-20320** and carries a CVSS score of 7.5. It is described as an improper restriction of XML external entity references. The source excerpt does not give details of the second flaw, the exploitation activity or who is being targeted, so we do not speculate on them here.

Why it matters

Inclusion in the KEV catalog means exploitation is not theoretical. The source also notes that patches are available, which means exposure now depends largely on how quickly organisations apply them. Telecom and communications platforms such as these are often internet-facing, so unpatched instances deserve early attention.

What to do next

Confirm whether either product is present in your environment, including instances run by service providers on your behalf. If so, check the vendor advisories for the fixed versions and schedule deployment on a priority basis. Where patching cannot happen immediately, review exposure and monitor for unusual activity.

What to do now

1. Check asset inventories and service-provider arrangements for Cisco BroadWorks and Openwave Messaging Webtop Media Transcoder.
2. Review the vendor advisories for CVE-2026-20320 and the second flaw, and identify the fixed versions.
3. Prioritise patching of affected instances, starting with those reachable from the internet.
4. Where patching is delayed, restrict exposure and increase monitoring of the affected systems.
5. Add CISA KEV entries to your vulnerability management intake so exploited flaws are escalated.