CISA adds actively exploited Cisco BroadWorks flaw CVE-2026-20320 to KEV catalog



CISA has confirmed active exploitation of CVE-2026-20320, an unauthenticated XXE flaw in Cisco BroadWorks that exposes configuration data. Cisco patched it in August; organizations running BroadWorks should verify patching now.

- CVE-2026-20320 is an XXE weakness in the OCI XML parser of Cisco BroadWorks, exploitable remotely without authentication.
- CISA added it to the KEV Catalog and set a federal remediation deadline of November 24.
- Cisco released a fix in August; the flaw stems from external entity resolution being enabled by default.
- Malbear Labs reported an attack on a European telecom provider and thirteen organizations using its infrastructure, with stolen keys and certificates.

> - CISA urges private-sector teams to prioritize KEV vulnerabilities too.

The US Cybersecurity and Infrastructure Security Agency (CISA) has warned that **CVE-2026-20320**, a high-severity vulnerability in Cisco BroadWorks, is being exploited in real attacks. BroadWorks is a cloud unified communications platform used by telecom carriers and managed service providers to deliver cloud PBX, voice and collaboration services to business customers.

What is known

The flaw is an XML External Entity (XXE) weakness in the Open Client Interface (OCI) XML parser. An unauthenticated remote attacker can send a crafted XML message to the OCI-P service and read sensitive configuration information. Cisco explained that external entity resolution was allowed by default, and it patched the issue in August.

CISA added the flaw to its Known Exploited Vulnerabilities (KEV) Catalog and required US federal civilian agencies to remediate by November 24. The directive applies only to those agencies, but CISA encouraged all organizations to adopt risk-based vulnerability management and prioritize KEV entries.

Threat intelligence firm Malbear Labs reported that a Chinese-speaking threat actor used the flaw, aided by a jailbroken AI model, against a European telecom provider and thirteen organizations using its data centers and cloud infrastructure. According to the firm, the attacker recovered a system identity private key, several SSL credential sets and additional private keys from the XSP host. The system identity key authenticates BroadWorks components to each other, so possessing it allows impersonation of the XSP. The firm also found the Provisioning Server exposed through an unauthenticated directory listing.

What to do

Organizations that operate BroadWorks, or that rely on a provider that does, should confirm the August fix is applied and review whether any credentials could have been exposed.

What to do now

1. Confirm with your IT team or telecom/MSP provider whether BroadWorks is in use and that the August Cisco patch is applied.
2. Restrict network access to the OCI-P service (port 2208 per Malbear Labs) to trusted management networks.
3. If exposure is suspected, rotate the system identity key, SSL credentials and private keys, and reissue certificates.
4. Check that Provisioning Server directories are not publicly listable.
5. Add KEV Catalog entries to your vulnerability-management prioritization and ask third-party providers for patch confirmation.