contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Cisco BroadWorks exploited

CVE-2026-20320 · on CISA's exploited list since 10 November 2026

Analysis Report

Anyone running Cisco BroadWorks must upgrade all affected components to release RI.2026.07 by 24 November 2026. If you do not run BroadWorks, this CVE does not apply; otherwise start by confirming …

PREPARED BY	NamiQ	DATE	13 November 2026
FACTS AS OF	13 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 7.5**	STATUS	On CISA's exploited list; due 24 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/cisco-broadworks-cve-2026-20320

The bottom line

> *Anyone running Cisco BroadWorks must upgrade all affected components to release RI.2026.07 by 24 November 2026. If you do not run BroadWorks, this CVE does not apply; otherwise start by confirming which components are deployed and their current release.*

At a glance

Fact	Detail
Product	Cisco BroadWorks (CVE-2026-20320)
Severity	High: 7.5 (CVSS 3.1)
CISA	On its exploited list since 10 November 2026. Deadline for US federal agencies: 24 November 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 13 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	RI.2026.07 for all four components — Application Delivery Platform, Application Server, Profile Server, and Xtended Services Platform — per the vendor's advisory.
Who looks first	Anyone running Cisco BroadWorks: the Application Delivery Platform, Application Server, Profile Server, or Xtended Services Platform. The vendor's advisory says all four are affected regardless of device configuration.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Cisco BroadWorks (Application Delivery Platform, Application Server, Profile Server, or XSP)?	Nothing to do for this CVE.	Check the installed release (next question).
Is the BroadWorks release earlier than RI.2026.07?	No upgrade needed; confirm the version in writing.	Plan upgrade to RI.2026.07 or later (see steps).
Is the OCI-P service reachable from untrusted networks?	Upgrade is still required; treat as lower urgency.	Treat as high priority; upgrade by 24 November 2026.

What it is

The flaw is in the XML parser of Cisco BroadWorks's Open Client Interface. External entity resolution is on by default, so an unauthenticated attacker who can reach the OCI-P service can send a crafted XML message and read files from the server filesystem with the privileges of the BroadWorks process.

Why it matters

The vendor's advisory says external entity resolution is on by default in the OCI XML parser, so the flaw is present in every affected release as shipped — no special configuration enables it. No authentication is required, so any host that can reach the OCI-P port is a potential attacker. Files readable by the BroadWorks process — which may include configuration, certificates, or subscriber data — are in scope. The vendor's advisory states no workarounds are available. The advisory was first published on 19 August 2026.

What the vendor's advisory says

We read one page on sec.cloudapps.cisco.com. In short:

- The vendor's advisory (cisco-sa-bworks-xxe-uwUd7CEt, 19 August 2026) covers only CVE-2026-20320 (Cisco Bug ID CSCwv48590). No other CVEs are mentioned. No workarounds available. First fixed release: RI.2026.07 for all four components.
- The advisory notes that for the Application Delivery Platform, the fix applies to the Open Client Server (OCS) and OCIOverSoap services specifically.

Things people will get wrong

- Only specific BroadWorks configurations are at risk. The vendor's advisory says all four affected components are vulnerable regardless of device configuration.
- Requiring a login to BroadWorks stops this attack. The CVSS vector shows no privileges are required (PR:N). The vendor's advisory describes an unauthenticated, remote attacker sending a crafted XML message directly to the OCI-P service.

The wording includes conditions the score may not show: it needs privileges. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page

before you run them. Words in capitals are for you to fill in.

Step 1: Find which BroadWorks components are installed

- Identify which of the four affected components are deployed: Application Delivery Platform, Application Server, Profile Server, or Xtended Services Platform.
- Record the current release of each. The vendor's advisory says any release earlier than RI.2026.07 is affected.

```
rpm -qa | grep -i broadworks
```

Step 2: Check whether OCI-P is network-accessible

- Determine whether the OCI-P service port is reachable from untrusted networks.
- The vendor's advisory says the attack path is a crafted XML message to the OCI-P service; reducing its exposure lowers risk while patching is arranged.

```
ss -tlnp
```

Step 3: Upgrade to RI.2026.07

- The vendor's advisory says RI.2026.07 is the first fixed release for all four components. No workarounds are available, so upgrade is the only remediation.
- Apply the update to each affected component and follow the vendor's restart procedure.

Step 4: Confirm the fixed release is in place

- After upgrading, verify each component reports RI.2026.07 or later.
- Record the confirmed version and date for your change log.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We are writing about CVE-2026-20320, a vulnerability in Cisco BroadWorks affecting the Application Delivery Platform, Application Server, Profile Server, and Xtended Services Platform. An unauthenticated attacker who can reach the OCI-P service can read files from the server filesystem. CISA requires remediation by 24 November 2026. The vendor's advisory says the first fixed release is RI.2026.07 for all four components. Please confirm whether any of these components run in our environment, which release is installed, and whether RI.2026.07 has been applied or is scheduled. We would appreciate written confirmation of the installed version and fix status by 21 November 2026.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unusual XML requests to the OCI-P service containing DOCTYPE declarations or SYSTEM or PUBLIC keyword references in service request logs.
- Unexpected read access to configuration or credential files in BroadWorks process logs or filesystem audit logs, particularly around times the OCI-P service was contacted from unfamiliar addresses.

The weakness behind it

The record classes this as CWE-611 (Improper Restriction of XML External Entity Reference).

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so

Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The flaw is in a network-facing XML parser (OCI-P) requiring no authentication (PR:N, AV:N). An attacker would likely exploit it directly over the network, which would typically follow this technique.
File and Directory Discovery (T1083): Listing files and folders to find what is there.	Discovery: looking around	XXE allows reading arbitrary file paths. An attacker would likely probe filesystem paths to discover configuration files, certificates, or other sensitive data on the host.
Unsecured Credentials: Credentials In Files (T1552.001): Finding passwords or keys left in files.	Credential Access: stealing logins	The record says sensitive configuration files are readable via the exploit. BroadWorks configuration files would likely contain credentials, making credential-in-files access a probable follow-on goal.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *Cisco BroadWorks contains an improper restriction of XML external entity reference vulnerability that could allow an unauthenticated, remote attacker to read sensitive configuration information on an affected system.*

The CVE record, published by Cisco on 19 August 2026:

> *A vulnerability in the Open Client Interface (OCI) XML Parser of Cisco BroadWorks could allow an unauthenticated, remote attacker to read sensitive configuration information on an affected system. This vulnerability exists because XML entries are improperly parsed due to external entity resolution being allowed by default. An attacker could exploit this vulnerability by sending a crafted XML message to the Open Client Interface – Provisioning (OCI-P) service. A successful exploit could allow the attacker to view sensitive files from the filesystem with the privileges of the Cisco BroadWorks user.*

Versions of Cisco BroadWorks the record lists as affected:

- N/A

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-20320
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-20320
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The sources do not say which specific files or directories are most likely to be accessible via this exploit.
- The sources do not say whether the OCI-P service is network-exposed in a default BroadWorks deployment.

- The source record includes a word-search result of 'it needs privileges', though the CVSS (PR:N) and the advisory both describe an unauthenticated attack; the sources do not explain the phrase.
- The sources do not state whether RI.2026.07 addresses any other flaws in BroadWorks beyond CVE-2026-20320.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 13 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-20320: score 7.5, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	None	Nothing can be altered.
Availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
19 August 2026	CVE record published by Cisco.
10 November 2026	CISA added it to its list of exploited vulnerabilities.
24 November 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
BroadWorks OCI-P service reachable from untrusted networks, running a release before RI.2026.07	High	By 24 November 2026
BroadWorks running internally only, on a release before RI.2026.07	High	This week
BroadWorks confirmed at RI.2026.07 or later — verify and document the version	Medium	Next patch cycle

Cisco BroadWorks not installed in the estate	None	No action needed for this CVE

Appendix 4. Definition of done

- Every Cisco BroadWorks you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-20320: https://www.cve.org/CVERecord?id=CVE-2026-20320
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/c: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bworks-xxe-uwUd7CEt