TransilienceAI

CVE-2026-20320

Vulnerability Report · TLP:CLEAR

Cisco · Cisco BroadWorks

25 Nov 2026

Version 63 · 1 sources

TLP:CLEAR — Transilience Newsroom

Compiled by Transilience from public reporting. May be shared without restriction.

Table of Contents

BRIEF . . . 3

- Bottom line . . . 3
- For the board . . . 3
- Are you exposed? . . . 3
- What to do . . . 3

TIMELINE . . . 4

AFFECTED PRODUCTS AND VERSIONS . . . 4

FIXED IN . . . 4

EXPLOITATION . . . 4

WHO IS EXPLOITING IT . . . 4

MITIGATIONS AND DETECTION . . . 5

ATT&CK; TECHNIQUES . . . 5

INDICATORS . . . 5

NOT KNOWN YET . . . 5

SOURCES . . . 5

ABOUT THIS REPORT . . . 5

Brief

EXPLOITED IN THE WILD
“Two weeks ago, CISA also flagged a high-severity Cisco BroadWorks vulnerability (CVE-2026-20320) as actively exploited in attacks and ordered federal agencies to patch their systems by November 24.” [1]

Bottom line

An unauthenticated Cisco BroadWorks flaw (CVE-2026-20320) is being actively exploited to steal credentials and keys; prioritize BroadWorks patching or CISA KEV actions and investigate exposed systems for compromise. [1]

For the board

A critical Cisco BroadWorks vulnerability is actively exploited to steal credentials and keys; treat BroadWorks systems as high-priority for patching and compromise assessment.

Are you exposed?

Affects	How to check
Cisco BroadWorks; versions before the fix (not reported) [1]	Check BroadWorks appliance/software version via vendor management interfaces or inventory; vendor advisory for affected builds is not reported.

What to do

1. **Prioritize applying BroadWorks patches or CISA KEV-directed mitigations immediately.** [1]
   CISA flagged CVE-2026-20320 as actively exploited and ordered federal agencies to patch by November 24.
2. **Investigate internet-exposed BroadWorks instances and related data-center assets for compromise.** [1]
   Malbear Labs reported exploitation targeting a European telecom provider and 13 organisations, indicating credential and data theft risk.
3. **Hunt for credential exfiltration and key access (logs, file access, outbound connections).** [1]
   Articles report attackers used the flaw to exfiltrate credentials and other sensitive information after compromise.

Timeline

Date	Kind	What happened
2026-11-23 published	ADVISORY	CISA flagged CVE-2026-20320 as actively exploited and ordered federal agencies to patch by November 24. [1] *“Two weeks ago, CISA also flagged a high-severity Cisco BroadWorks vulnerability (CVE-2026-20320) as actively exploited in attacks and ordered federal agencies to patch their systems by November 24.”* [1]
2026-11-23 published	CAMPAIGN	Malbear Labs reported exploitation targeting a European telecom provider and 13 organisations. [1] *“According to threat intelligence firm Malbear Labs, a Chinese-speaking threat actor abused CVE-2026-20320 in autonomous AI attacks targeting a European telecommunications provider and 13 organizations that used its data centers and cloud infrastructure.”* [1]

Affected products and versions

- Cisco BroadWorks (versions before the fix; specific affected builds not reported) [1]
  “Two weeks ago, CISA also flagged a high-severity Cisco BroadWorks vulnerability (CVE-2026-20320) as actively exploited in attacks and ordered federal agencies to patch their systems by November 24.” [1]

Fixed in

No fixed version is named in the sources.

Exploitation

Count	Detail
—	Actively exploited in the wild; CISA flagged it as exploited and ordered patching. [1] *“Two weeks ago, CISA also flagged a high-severity Cisco BroadWorks vulnerability (CVE-2026-20320) as actively exploited in attacks and ordered federal agencies to patch their systems by November 24.”* [1]
14 targets reported	Malbear Labs reported actor abused CVE-2026-20320 in attacks against a European telecom provider and 13 organisations. [1] *“According to threat intelligence firm Malbear Labs, a Chinese-speaking threat actor abused CVE-2026-20320 in autonomous AI attacks targeting a European telecommunications provider and 13 organizations that used its data centers and cloud infrastructure.”* [1]

Who is exploiting it

- A Chinese-speaking threat actor (per Malbear Labs) [1]
  “According to threat intelligence firm Malbear Labs, a Chinese-speaking threat actor abused CVE-2026-20320 in autonomous AI attacks targeting a European telecommunications provider and 13 organizations that used its data centers and cloud infrastructure.” [1]

Mitigations and detection

None given in the sources.

ATT&CK techniques

The sources do not describe the attacker's behaviour closely enough to map.

Indicators

None published in the sources.

Not known yet

- affected BroadWorks versions
- technical vulnerability vector and exploit details
- patch/fixed version or advisory link
- number of compromised systems confirmed

Sources

#	Outlet	Article	Copy
1	**BleepingComputer** 23 Nov 2026	CISA flags critical Cisco RCE flaw as actively exploited in attacks	archived copy

About this report

Compiled by Transilience Newsroom from 1 public source. Every quotation is checked against the article it cites; 3 statements were left out because the source did not bear them out. The status is never stated more strongly than its quote shows. ATT&CK techniques marked “mapped by Newsroom” are our reading of the quoted behaviour, not the source's claim. Version 63, written 25 November 2026, 23:11 UTC (cve-report-2026-09-25c). TLP:CLEAR — may be shared without restriction. The live report: https://threatnews.transilience.cloud/report/cve/cve-2026-20320