contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Tenda AC19: new CVE

CVE-2026-123966 · record published 7 November 2026

Analysis Report

CVE-2026-123966 in Tenda AC19, a new record scored 10 and not on CISA's exploited list when we read it. What it is, who is affected, and what to check first.

PREPARED BY	NamiQ	DATE	8 November 2026
FACTS AS OF	8 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 10.0**	STATUS	Not on CISA's exploited list; exploitation not recorded

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/tenda-ac19-cve-2026-123966

The bottom line

> *Check whether you run Tenda AC19. If you do, read the vendor's page for the fixed version and update. Nothing public says yet that anyone is using this flaw.*

At a glance

Fact	Detail
Product	Tenda AC19 (CVE-2026-123966)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 7 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 8 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No source we read names a fixed version
Who looks first	Anyone managing a Tenda AC19 router on firmware 16.03.10.07. The record states the attack is possible remotely; the degree of exposure depends on who can reach the router's web interface.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a Tenda AC19 router?	Nothing to do for this CVE.	Check the firmware version.
Is it on firmware 16.03.10.07?	The record does not list your version as affected — monitor for a Tenda update.	Check whether the admin interface is reachable from outside your network.
Is the router's web admin interface reachable from outside your local network?	Risk is reduced — apply a patch as soon as one is available.	Block that access immediately and ask your IT contact about a firmware update.

What it is

The record describes a heap-based buffer overflow in the router's saveParentControlInfo web endpoint. Sending a crafted request with an oversized deviceId value corrupts memory on the

device. The record states the attack can be carried out remotely and that a working exploit has been publicly disclosed.

Things people will get wrong

- The overflow is in one endpoint, so the rest of the router is unaffected. A heap-based buffer overflow in a web handler can allow code execution across the entire device, not just the endpoint where it occurs.

How we would triage it

This is our judgement.

Step 1: Find the firmware version on each AC19

- Log in to the router's web admin interface and locate the firmware or system status page, where the installed version is displayed.
- Confirm whether it reads 16.03.10.07, which is the version the record lists as affected.

Step 2: Restrict access to the admin interface

- Using your firewall or the router's own access-control settings, ensure the web admin interface is reachable only from trusted hosts on the local network, not from the internet.
- This reduces the attack surface while you wait for a patched firmware release.

Step 3: Check for a firmware update from Tenda

- Check Tenda's support pages for a firmware release for the AC19 that addresses this flaw. The record names no fixed version at the time of writing.
- Do not apply a release unless you can confirm it addresses CVE-2026-123966 or is published after 7 November 2026 and explicitly supersedes 16.03.10.07.

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.

The weakness behind it

The record classes this as CWE-122 and CWE-119.

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 web endpoint reachable over the network; exploiting it would likely be the initial access step, as the description names a remotely reachable form handler as the entry point.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	A heap-based overflow on an embedded router device would typically lead to arbitrary code execution, likely via the device's built-in command interpreter.
Exploitation of Remote Services (T1210): Exploiting a flaw in a service on another machine to move to it.	Lateral Movement: moving to other machines	A compromised perimeter router could be used to reach internal hosts; gaining control of the device would likely enable further movement into the local network.

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

The CVE record:

> *A vulnerability was determined in Tenda AC19 16.03.10.07. Affected by this issue is the function saveParentControlInfo of the file /goform/saveParentControlInfo. This manipulation of the argument deviceId causes heap-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.*

Versions of Tenda AC19 the record lists as affected:

- 16.03.10.07

The record gives no version ranges. Use the vendor's advisory for the affected versions.

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-2026-123966
```

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-2026-123966
```

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

- Whether authentication is required before the saveParentControlInfo endpoint can be reached — the record does not say.
- Whether Tenda plans to release a patched firmware for the AC19, and when.

- Whether the flaw affects other Tenda router models or other firmware versions of the AC19.
- What level of access a successful exploit provides on the device.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 8 November 2026. We have not read the vendor's advisory page and we have not tested it.
- The sections headed "Does this apply to you?", "What it is", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping" and "How we would triage it" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-123966: score 10, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:P`
As the CVE record gives it.

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.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
7 November 2026	CVE record published by VulDB.

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
AC19 on firmware 16.03.10.07, admin interface reachable from the internet	Medium	Block external access today

AC19 on firmware 16.03.10.07, admin interface on the LAN only	Medium	This week — apply patch when available
AC19 present but firmware version not yet confirmed	Medium	Confirm version today
AC19 running a firmware version other than 16.03.10.07	Low	Monitor; no action until a fix is confirmed
No Tenda AC19 in the estate	None	No action needed for this CVE

Appendix 4. Definition of done

- Every Tenda AC19 you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-123966: https://www.cve.org/CVERecord?id=CVE-2026-123966
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/432038
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/432038/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-123966