contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Edimax BR6478ACV2: new CVE

CVE-2026-129250 · record published 14 November 2026

Analysis Report

CVE-2026-129250 in Edimax BR6478ACV2, a new record scored 9.9 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	14 November 2026
FACTS AS OF	14 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.9**	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/edimax-br6478acv2-cve-2026-129250

The bottom line

> *Check whether you run Edimax BR6478ACV2. 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	Edimax BR6478ACV2 (CVE-2026-129250)
Severity	Critical: 9.9 (CVSS 3.1)
Status	A new CVE record, published by VulDB on 14 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 14 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 running an Edimax BR6478ACV2 router, above all where its web management interface can be reached from the internet or by untrusted users on a shared network.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run an Edimax BR6478ACV2 router anywhere?	Nothing to do for this CVE.	Check which firmware it runs (next question).
Is it on the firmware the record names as affected?	It may not be affected; still confirm with the vendor.	Check who can reach its web interface.
Can the router's web management interface be reached from the internet or by untrusted users?	Risk is much lower; still plan a fix.	Restrict that access now and seek fixed firmware.

What it is

The record says changing the PPTP user-name field on the router's web interface overflows a memory buffer. Someone who can reach that interface over the network could trigger it, crashing the device or corrupting how it runs.

Why it matters

The record describes a memory-safety flaw in the router's web server, in the code that handles PPTP set-up. An attacker who can reach the web interface could use it to take the device over or knock it offline. A router sits between everything on the network and the internet, so a compromised one is a strong foothold. Our reading is that a 9.9 score, a publicly disclosed exploit and no vendor response make this worth treating urgently, even though it is not on the exploited-vulnerabilities list.

Things people will get wrong

- It is not on CISA's exploited list, so we can wait. The record says a working exploit is already public and the vendor has not responded, so the exposure is real now.
- We do not use PPTP, so this does not affect us. The flaw is in the router's web server code that serves the PPTP set-up page; the record does not say the feature must be switched on, so do not assume you are safe.

How we would triage it

This is our judgement.

Step 1: Confirm the model and firmware

- Check the device label and the router's admin page to confirm it is an Edimax BR6478ACV2 and note the firmware version, because only this model and version are named in the record.

Step 2: Reduce exposure now

- Make sure the web management interface is not reachable from the internet, because the attack needs to reach that interface.

Step 3: Seek a fix from the vendor

- Ask Edimax or your supplier whether fixed firmware exists, because no source here names one and the record says the vendor did not respond to the disclosure.
- Until a fix is confirmed, consider isolating or replacing the device if it must face the internet.

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-120 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 record describes a remotely reachable flaw in the router's web server; exploiting that network-facing interface would typically be the initial way in.
Endpoint Denial of Service (T1499): Crashing or overloading a single system or application.	Impact: causing damage or disruption	A buffer overflow in the web server could crash the device, so an attacker would likely be able to knock the router offline.

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 security vulnerability has been detected in Edimax BR6478ACV2 1.23. The impacted element is the function formPPTPSetup of the file webs. The manipulation of the argument pptpUserName leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.*

Versions of Edimax BR6478ACV2 the record lists as affected:

- 1.23

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-2026-129250
```

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-2026-129250
```

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 the attack works without logging in to the router first; the record does not say whether authentication is needed.
- Whether fixed firmware exists; the vendor did not respond and no source names a fixed version.

- Whether firmware other than the version named is affected; only that one is listed.
- Whether the flaw allows running code or only crashes the device; the record says only that it is a buffer overflow.
- 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 14 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", "Why it matters", "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-2026-129250: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:X/RC:C` 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.
Privileges required	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
14 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
An Edimax BR6478ACV2 whose web management interface is reachable from the internet	Medium	this week
The router managed only from the local network, but by untrusted users such as guest wifi or a shared office	Medium	this week
The router on a trusted, internal-only network behind another firewall	Low	next review
You do not run this model	None	none for this CVE

Appendix 4. Definition of done

- Every Edimax BR6478ACV2 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-2026-129250: https://www.cve.org/CVERecord?id=CVE-2026-129250
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/437280
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/437280/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-129250