contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Linksys E8450: new CVE

CVE-2026-120283 · record published 2 November 2026

Analysis Report

Anyone running a Linksys E8450 on firmware 1.2.00.360516 should act now; the record scores this at 10 out of 10 under CVSS 4.0 and no patch exists. The vendor did not respond to disclosure, so check …

PREPARED BY	NamiQ	DATE	2 November 2026
FACTS AS OF	2 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/linksys-e8450-cve-2026-120283

The bottom line

> *Anyone running a Linksys E8450 on firmware 1.2.00.360516 should act now; the record scores this at 10 out of 10 under CVSS 4.0 and no patch exists. The vendor did not respond to disclosure, so check immediately whether the router's management interface is reachable from outside your network.*

At a glance

Fact	Detail
Product	Linksys E8450 (CVE-2026-120283)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 2 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 2 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	Operators of a Linksys E8450 running firmware 1.2.00.360516. If you do not run this device, or run it on a different firmware version, this record does not name you.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you operate a Linksys E8450 router?	Nothing to do for this CVE.	Check the firmware version (next question).
Is the firmware version 1.2.00.360516?	The record names only that version; monitor for further advisories.	Check whether the management interface is reachable from outside your network.
Is the router's management interface reachable from the internet or an untrusted network?	Restrict access to trusted hosts and monitor for a vendor patch.	Restrict access immediately; no patch is available.

What it is

A remotely exploitable stack-based buffer overflow in the router's portal.cgi handler. An attacker can send a crafted value for the hidden_timezone argument to overflow a stack buffer, which the record says can be done from across a network.

Why it matters

The record scores this at 10 under CVSS 4.0, the maximum possible. A stack-based buffer overflow via a remotely supplied CGI argument means an attacker who can reach the endpoint may overwrite the call stack and run code on the device. Our reading is that a router at the network edge is a high-value target: control of it gives an attacker a position inside the boundary before internal defences can act. The record states the vendor did not respond to the researcher's disclosure, so no official patch exists and no timeline for one is known.

Things people will get wrong

- A score of 10 means this is already being exploited. The score reflects severity if exploited, not confirmed exploitation. The record states this is a new CVE and it is not on CISA's list of exploited vulnerabilities.
- If my firmware version differs, I am safe. The record identifies 1.2.00.360516 as the tested version. It does not say other versions are unaffected; it only names the one that was confirmed.

How we would triage it

This is our judgement.

Step 1: Find which E8450 devices you run and their firmware version

- Log in to each Linksys E8450 admin interface; the firmware version is shown on the status or administration page.
- Record whether the version matches 1.2.00.360516 as named in the record.

Step 2: Restrict access to the management interface

- Disable remote management if it is enabled, so the admin interface is not reachable from outside the local network.
- Confirm no firewall rule or port forward exposes the router's management interface to the internet.

Step 3: Watch for a vendor patch

- The record states the vendor did not respond to disclosure; check Linksys support pages for firmware updates for the E8450.
- Apply any update that addresses CVE-2026-120283 as soon as one is available.

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.

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 reviewing CVE-2026-120283, a remotely exploitable stack-based buffer overflow in Linksys E8450 firmware version 1.2.00.360516, scored at 10 out of 10 under CVSS 4.0. No patch has been published and the vendor did not respond to the original disclosure. Please confirm whether we run any Linksys E8450 devices, which firmware version each is on, and whether the management interface is accessible from outside our network. As no fixed version is currently available, please advise when a patch is released and confirm what steps have been taken to restrict access in the meantime. We would like written confirmation of the version and steps taken by 9 November 2026.*

The weakness behind it

The record classes this as CWE-121 and CWE-119.

The sources, in their words

The CVE record:

> *A vulnerability was identified in Linksys E8450 1.2.00.360516. Affected is the function strcpy of the file /www/cgi-bin/portal.cgi. Such manipulation of the argument hidden_timezone leads to stack-based buffer overflow. The attack can be executed remotely. The vendor was contacted early about this disclosure but did not respond in any way.*

Versions of Linksys E8450 the record lists as affected:

- 1.2.00.360516

What we do not know yet

- Whether authentication is required before the hidden_timezone argument is processed.

- Whether the vendor has acknowledged the vulnerability or intends to release a patch.
- Whether firmware versions other than 1.2.00.360516 are also affected.
- 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 2 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- 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", "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-2026-120283: 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
2 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
Linksys E8450 on 1.2.00.360516 with management interface reachable from the internet	Medium	This week

Linksys E8450 on 1.2.00.360516 with management interface on internal LAN only	Medium	Next patch cycle; monitor for vendor update
Linksys E8450 on a firmware version other than 1.2.00.360516	Low	Monitor for further advisories
No Linksys E8450 in the estate	None	No action required

Appendix 4. Definition of done

- Every Linksys E8450 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-2026-120283: https://www.cve.org/CVERecord?id=CVE-2026-120283
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: www.linksys.com: https://www.linksys.com/
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/429627
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/429627/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-120283