contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Linksys EA8100: new CVE

CVE-2026-127275 · record published 12 November 2026

Analysis Report

If you run a Linksys EA8100 router, check its firmware now. CISA has not listed this, but working attack code is public and there is no fix, so make sure the router's management cannot be reached …

PREPARED BY	NamiQ	DATE	13 November 2026
FACTS AS OF	13 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-ea8100-cve-2026-127275

The bottom line

> *If you run a Linksys EA8100 router, check its firmware now. CISA has not listed this, but working attack code is public and there is no fix, so make sure the router's management cannot be reached from the internet first.*

At a glance

Fact	Detail
Product	Linksys EA8100 (CVE-2026-127275)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 12 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 13 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 a Linksys EA8100 router on firmware 1.0.3.216940, most urgently where its management page can be reached from the internet rather than only the local network.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a Linksys EA8100 router?	Nothing to do for this CVE.	Check its firmware version next.
Is it on firmware 1.0.3.216940?	The record lists only this build; still keep management off the internet.	Treat it as affected; reduce exposure.
Can the router's management interface be reached from the internet?	Risk is much lower; keep it that way.	Disable remote management now.

What it is

The record says two functions in the router's management interface, reached through its JNAP API, do not check who is calling. Someone able to reach the router over the network can change its remote-management and WiFi-warning settings without logging in.

Why it matters

The weakness is missing authentication: the record says the affected functions do not check who is calling, so no login stands in the way of anyone who can reach them. The record says the exploit is public and the vendor did not respond, so no patched firmware is named. Our reading is that this mix - no login needed, code public, no fix - makes exposure, not the version, the thing to control. Keep the management interface off the internet until a fix appears.

Things people will get wrong

- It's not on CISA's list, so it can wait. The record says working attack code is already public and no login is needed, and no fixed firmware has been named.
- Our admin password protects the router. The weakness is missing authentication in these functions, so the record says they act without checking a login at all.

How we would triage it

This is our judgement.

Step 1: Find the firmware you run

- Log into the router's admin page and read its firmware version.
- Compare it with 1.0.3.216940, the build the record names as affected.

Step 2: Take the management interface off the internet

- Turn off remote or internet-facing management so the JNAP API cannot be reached from outside, because no login protects the affected functions.
- Limit who on the local network can reach the router's admin page.

Step 3: Watch for a fix

- Check for newer firmware; the record says the vendor did not respond and names no fixed build.
- Plan to apply a fix as soon as the vendor publishes one.

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 would like your help with a security issue, CVE-2026-127275, affecting the Linksys EA8100 router. Could you confirm in writing whether we run any of these routers, where they are, and which firmware version each one is on? The record names firmware 1.0.3.216940 as affected and says the problem is missing authentication, with attack code already public. No fixed firmware version has been named yet, and this is not on CISA's exploited list at the moment. For now, please make sure the router's management interface cannot be reached from the internet, and let us know by the end of this week what you find and what you have changed.*

The weakness behind it

The record classes this as CWE-306 and CWE-287.

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 says the flaw is in a JNAP API reached over the network and needs no authentication, so an attacker would likely exploit this public-facing management interface directly.
External Remote Services (T1133): Using a remote-access service such as a VPN or remote desktop to get into the network.	Initial Access: getting in	If remote management is exposed, an attacker would likely reach the router's remote-access service from outside, since the record says no login is checked.

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 Linksys EA8100 1.0.3.216940. This issue affects the function SetRemoteSetting/SetUnsecuredWiFiWarning of the file ui_server.lua of the component JNAP API. This manipulation of the argument isEnabled/enabled causes missing authentication. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.*

Versions of Linksys EA8100 the record lists as affected:

- 1.0.3.216940

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-2026-127275
```

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-2026-127275
```

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 other EA8100 firmware versions are affected; the record lists only 1.0.3.216940.
- Whether the vendor plans a fix; the record says it did not respond.
- Whether the flaw is being used against real routers, beyond the exploit being public.
- Whether remote management must be enabled for the attack, or the local network is enough.
- 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 13 November 2026. We have not read the vendor's advisory page and we have not tested it.
- 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-2026-127275: 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
12 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
A Linksys EA8100 whose management page is reachable from the internet, on the affected firmware	Medium	this week

A Linksys EA8100 on the affected firmware with management only on the local network	Medium	next patch cycle
An untrusted device or guest on the same network as an affected router	Medium	this week
No Linksys EA8100 router in use	None	none for this CVE

Appendix 4. Definition of done

- Every Linksys EA8100 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-2026-127275: https://www.cve.org/CVERecord?id=CVE-2026-127275
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/436430
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/436430/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-127275