contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

# Linksys E5350: new CVE

**CVE-2026-121932 · record published 4 November 2026**

## Analysis Report

Owners of a Linksys E5350 on firmware 1.0.00.037 should act now: the exploit is public, no patch exists, and the vendor has not responded. Check first whether the router's admin interface is ...

| | | | |
|---|---|---|---|
| PREPARED BY | NamiQ | DATE | 5 November 2026 |
| FACTS AS OF | 5 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-e5350-cve-2026-121932

## The bottom line

> *Owners of a Linksys E5350 on firmware 1.0.00.037 should act now: the exploit is public, no patch exists, and the vendor has not responded. Check first whether the router's admin interface is reachable from outside the local network, and restrict it if so.*

## At a glance

| Fact | Detail |
|---|---|
| Product | Linksys E5350 (CVE-2026-121932) |
| Severity | Critical: 10 (CVSS 4.0) |
| Status | A new CVE record, published by VulDB on 4 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 5 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 E5350 on firmware 1.0.00.037. The record names this as the affected version and says the attack can be launched remotely, so exposure is not limited to those with physical access. |

## Does this apply to you?

**Answer in order. Stop at the first no.**

| Question | If no | If yes |
|---|---|---|
| Do you run a Linksys E5350 router? | Nothing to do for this CVE. | Check the firmware version (next question). |
| Is the firmware version 1.0.00.037? | The record names only 1.0.00.037; check the vendor for guidance on other versions. | No patch exists; check whether the admin interface is exposed (next question). |
| Is the router's admin interface reachable from outside your local network? | Risk is reduced; monitor for a firmware update. | Disable remote admin access immediately and monitor for a patch. |

## What it is

An attacker who can reach the router's web interface can inject operating system commands by supplying crafted values in the ping_ip or traceroute_ip fields of the diagnostic endpoint. The record

says the attack can be initiated remotely.

## Things people will get wrong

- No patch means nothing can be done. Without a patch, reducing exposure is the available action: disable remote admin access and ensure the router's web interface is not reachable from outside the local network.
- Being behind NAT means the router's admin interface cannot be reached remotely. Many routers expose a remote management option on the WAN port independently of NAT. Confirm the setting in the admin panel rather than assuming it is off.

## How we would triage it

This is our judgement.

## Step 1: Find the firmware version running on the E5350

- Log in to the router's admin interface and go to the status or firmware page. The record names 1.0.00.037 as the affected version — confirm whether this matches what is installed.

## Step 2: Check and restrict remote admin access

- In the router's admin settings, find the remote management or remote access option. If it is enabled and the WAN interface is exposed, disable it. The record says the attack can be initiated remotely.

## Step 3: Monitor for a firmware update

- The record names no fixed version and no vendor advisory exists. Check the Linksys support page for the E5350 regularly for any new firmware release.
- If no update appears and the device handles internet-facing traffic, consider whether a replacement router is the appropriate next step.

## Step 4: Review the router if the admin interface was exposed

- If remote access was enabled and internet-facing, review connected devices for unexpected activity. The record identifies this as OS command injection (CWE-78, CWE-77) affecting the router's web interface.

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-2026-121932, an OS command injection flaw (CWE-78, CWE-77) in the Linksys E5350 router on firmware 1.0.00.037. The exploit is public, no patch has been released, and the vendor did not respond to disclosure. Please confirm: (1) whether we run a Linksys E5350 and on which firmware version; (2) whether the router's admin interface is reachable from outside our network; and (3) if so, that remote admin access has been disabled. As no fixed version exists, please also confirm you are monitoring for any update. Please provide written confirmation of the version installed and current remote-access setting by 12 November 2026.*

## The weakness behind it

The record classes this as CWE-78 and CWE-77.

## The sources, in their words

The CVE record:

> *A vulnerability was detected in Linksys E5350 1.0.00.037. This affects the function system of the file /wizard/apply.cgi. Performing a manipulation of the argument ping_ip/traceroute_ip results in os command injection. The attack may be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.*

Versions of Linksys E5350 the record lists as affected:

- 1.0.00.037

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-2026-121932
```

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 names of running container images 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-2026-121932
```

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. It reads the names of the running images, not what is 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

- No fixed firmware version is named in the record or any source. It is not known whether Linksys intends to release a patch.
- The record does not state whether authentication is required to reach the vulnerable endpoint, which would affect how easily the flaw can be exploited.
- It is not known whether Linksys E5350 firmware versions other than 1.0.00.037 are also affected; the record names only that version.
- 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 5 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", "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-2026-121932**: 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 |
|---|---|
| 4 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 E5350 on 1.0.00.037, admin interface restricted to the local network only | Low | Next patch cycle — apply any firmware update when released |

| | | |
|---|---|---|
| Linksys E5350 on 1.0.00.037, local network with no untrusted hosts | Low | Next patch cycle — monitor for a firmware update |
| Not running a Linksys E5350 | None | None for this CVE |

## Appendix 4. Definition of done

- Every Linksys E5350 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-2026-121932: https://www.cve.org/CVERecord?id=CVE-2026-121932
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/431044
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/431044/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-121932