contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

TOTOLINK A950RG: new CVE

CVE-2026-121597 · record published 4 November 2026

Analysis Report

CVE-2026-121597 in TOTOLINK A950RG, 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	3 November 2026
FACTS AS OF	3 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/totolink-a950rg-cve-2026-121597

The bottom line

> *Check whether you run TOTOLINK A950RG. 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	TOTOLINK A950RG (CVE-2026-121597)
Severity	Critical: 9.9 (CVSS 3.1)
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 3 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 who operates a TOTOLINK A950RG router on firmware V4.1.2cu.5268_B20221104. A device whose management interface is reachable from the LAN or from the internet carries the highest risk.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a TOTOLINK A950RG router?	Nothing to do for this CVE.	Check the firmware version (next question).
Does your router show firmware version V4.1.2cu.5268_B20221104?	This version is the only one listed as affected; monitor for further advisories.	Check whether the management interface is reachable by untrusted users (next question).
Can untrusted users reach the router's web management interface?	Risk is reduced; apply a firmware update as soon as one is available.	Restrict access immediately — see the steps below.

What it is

The router's easy-setup wizard handler copies a user-supplied wireless network name into a twelve-byte stack buffer without checking its length. An attacker who can reach the management interface can send an oversized name, overwrite the call stack, and run arbitrary code on the router.

Things people will get wrong

- 'Authentication is required, so only logged-in users are a threat.' The gist states that this flaw combined with A950RG-INFO-01 removes the authentication requirement entirely. The authenticated-only condition cannot be assumed if both flaws are present.
- 'No CISA listing means this is low priority.' The record is newly published and a working exploit is already public. Absence from the CISA list reflects timing, not severity; the VulDB record scores it 9.9.
- 'Only the functionType argument is dangerous.' The source records that rootSsid and apcliSsid are the parameters that cause the overflow; functionType selects the branch that processes them.

How we would triage it

This is our judgement.

Step 1: Find the firmware version running on your router

- Log in to the router's web interface and look for the firmware or system information page; confirm whether the version shown is V4.1.2cu.5268_B20221104.
- If you cannot log in, the sticker on the device or your purchase records may show the hardware revision; confirming the firmware version requires login or a network scanning tool.

Step 2: Restrict access to the management interface

- Block access to the router's web management port from any network segment that untrusted users can reach.
- The gist records the attack vector as Network; if the management interface was accessible from the internet, disable that path immediately.

Step 3: Check for a firmware update

- No fixed firmware version is named in any source available at the time this note was written; check the TOTOLINK support pages for a release newer than V4.1.2cu.5268_B20221104.

- The researcher's gist was created on 10 October 2026 and the VulDB record was published on 4 November 2026; allow time for a vendor response before concluding none is forthcoming.

Step 4: Assess exposure from the companion flaw A950RG-INFO-01

- The gist names A950RG-INFO-01 as a flaw that, combined with this one, removes the authentication requirement entirely.
- If the router is on the affected firmware, treat the combined risk as unauthenticated-network-reachable until both issues are resolved.

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-121 and CWE-119.

The sources, in their words

The CVE record:

> *A weakness has been identified in TOTOLINK A950RG 4.1.2cu.5268_B20221104. This affects the function setAppEasyWizardConfig of the file /cgi-bin/cstecgi.cgi of the component Easy Setup Wizard Handler. Executing a manipulation of the argument functionType can lead to stack-based buffer overflow. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.*

Versions of TOTOLINK A950RG the record lists as affected:

- 4.1.2cu.5268_B20221104

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-2026-121597
```

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-2026-121597
```

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 any source; it is not known whether TOTOLINK has issued or plans a patch for V4.1.2cu.5268_B20221104.
- The CVE identifier and severity score for the companion flaw A950RG-INFO-01 are not given in the sources.
- Whether the management interface is exposed by default or only after an administrator configuration change is not stated in the sources.
- Whether other firmware versions of the A950RG share the same vulnerable code path is not addressed in any source.
- 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 3 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- The sections headed "Does this apply to you?", "What it is", "Exposure by situation", "Things people will get wrong" 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-2026-121597: 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:R` 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
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
Management interface on LAN; untrusted devices share the same network segment	Medium	This week
Management interface restricted to trusted admins only; no patch yet available	Medium	Next patch cycle
Affected firmware, but management interface blocked from all untrusted paths by a firewall	Low	When a patch is released
Different TOTOLINK model or firmware version not listed as affected	None	None for this CVE

Appendix 4. Definition of done

- Every TOTOLINK A950RG 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-2026-121597: https://www.cve.org/CVERecord?id=CVE-2026-121597
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: gist.github.com/H3rmesk1t/49d6ccded59379651568e0bdc6b5624c: https://gist.github.com/H3rmesk1t/49d6ccded59379651568e0bdc6b5624c
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/430439
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/430439/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-121597