contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

TOTOLINK A7100RU: new CVE

CVE-2026-134882 · record published 23 November 2026

Analysis Report

Anyone running TOTOLINK A7100RU on firmware 7.4cu.2313_B20191024 should act now: the record scores this at 10 and the attack is possible remotely, with no fixed version yet named. Block the router's ...

PREPARED BY	NamiQ	DATE	24 November 2026
FACTS AS OF	24 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/totolink-a7100ru-cve-2026-134882

The bottom line

> *Anyone running TOTOLINK A7100RU on firmware 7.4cu.2313_B20191024 should act now: the record scores this at 10 and the attack is possible remotely, with no fixed version yet named. Block the router's admin interface from untrusted networks immediately.*

At a glance

Fact	Detail
Product	TOTOLINK A7100RU (CVE-2026-134882)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 23 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 24 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 TOTOLINK A7100RU on firmware version 7.4cu.2313_B20191024. The record does not list other TOTOLINK models or firmware versions as affected.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a TOTOLINK A7100RU router?	Nothing to do for this CVE.	Check the firmware version (next question).
Is the firmware version 7.4cu.2313_B20191024?	The record does not list your version as affected.	Check whether the admin interface is reachable from untrusted networks.
Can untrusted users reach the router's admin interface from outside your network?	Reduce exposure further and monitor for a firmware patch.	Block that access immediately and check for a firmware update.

What it is

By manipulating the Username argument sent to the exportOvpn function in the router's CGI handler, an attacker can inject operating-system commands. The record says the attack can be carried out remotely, so no local access to the router is required.

Why it matters

The record's score of 10 is the maximum for CVSS 4.0. CWE-78 (OS Command Injection) and CWE-77 (Command Injection) indicate the injection point is well understood, and a successful attack gives arbitrary command execution on the device. The attack is described as remotely possible. Our reading is that a router with a remotely exploitable command-injection flaw, scored at the maximum, is a full-compromise risk for any network it protects, even though this CVE is not yet on CISA's exploited list.

Things people will get wrong

- Only the VPN export feature is at risk, so disabling VPN is enough. The record names the exportOvpn function in the CGI handler as the vulnerable entry point. The record does not state that disabling VPN removes the attack surface from the CGI handler.

How we would triage it

This is our judgement.

Step 1: Find the firmware version on your router

- Log in to the router's admin panel and locate the firmware version, usually shown on a status or system information page.
- Compare what you see against the affected version: 7.4cu.2313_B20191024.

Step 2: Block admin interface access from untrusted networks

- Confirm the router's admin interface is not reachable from outside your local network.
- If a firewall or modem sits in front of this router, verify no port-forwarding rule exposes the CGI handler externally.

Step 3: Check for a firmware update from TOTOLINK

- The record names no fixed version. Check TOTOLINK's support pages for the A7100RU to see whether a newer firmware has been released.

- Do not rely on this record alone; the vendor's own support pages are the authoritative source for patch availability.

Step 4: Monitor the record for a fixed version

- No source names a patched firmware. Continue checking the VulDB record and TOTOLINK's support pages until a confirmed fix 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 writing to ask you to check our TOTOLINK A7100RU router. A vulnerability, CVE-2026-134882, has been published affecting firmware version 7.4cu.2313_B20191024. The flaw allows an attacker to inject operating-system commands via the CGI handler remotely, and the record gives it a maximum score of 10. No fixed firmware version has been named yet. Please confirm whether we run this router, which firmware version it carries, and whether its admin interface is reachable from outside our network. If a firmware update is available, please apply it. We would like written confirmation of the current version and what action has been taken by 1 December 2026.*

The weakness behind it

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

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 CGI handler on a router is network-reachable; remote OS command injection via a crafted request would likely follow the pattern of exploiting a public-facing application for initial access.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	CWE-78 and CWE-77 describe OS command injection, which would typically result in arbitrary command execution on the device via a shell or scripting interpreter.

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 weakness has been identified in TOTOLINK A7100RU 7.4cu.2313_B20191024. This issue affects the function exportOvpn of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument Username causes os command injection. The attack is possible to be carried out remotely.*

Versions of TOTOLINK A7100RU the record lists as affected:

- 7.4cu.2313_B20191024

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-2026-134882
```

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-2026-134882
```

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 authentication is required to reach the exportOvpn function, or whether the attack is possible without credentials.
- Whether TOTOLINK has a firmware update planned or already released for the A7100RU.
- Whether other TOTOLINK models share the same CGI handler code and are equally affected.
- Whether disabling the VPN export feature removes the attack surface or whether the CGI handler remains reachable regardless.
- 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 24 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", "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-2026-134882: 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:X`
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
23 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
TOTOLINK A7100RU on affected firmware, admin interface reachable from the internet	Medium	Immediately

TOTOLINK A7100RU on affected firmware, admin interface restricted to the local network	Medium	This week
TOTOLINK A7100RU on affected firmware, no patch yet available	Medium	Check daily until a patch is confirmed
TOTOLINK A7100RU on a different firmware version	Low	Monitor for record updates

Appendix 4. Definition of done

- Every TOTOLINK A7100RU 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-2026-134882: https://www.cve.org/CVERecord?id=CVE-2026-134882
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: www.totolink.net: https://www.totolink.net/
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/442238
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/442238/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-134882