contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

TOTOLINK N350RT: new CVE

CVE-2026-137043 · record published 26 November 2026

Analysis Report

Anyone running a TOTOLINK N350RT on firmware 9.3.5u.6466_B20250825 or 9.3.5u.6468_B20250827 should act now: the exploit is public and the record scores this 10 out of 10. First, check whether the …

PREPARED BY	NamiQ	DATE	26 November 2026
FACTS AS OF	26 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-n350rt-cve-2026-137043

The bottom line

> *Anyone running a TOTOLINK N350RT on firmware 9.3.5u.6466_B20250825 or 9.3.5u.6468_B20250827 should act now: the exploit is public and the record scores this 10 out of 10. First, check whether the router's management interface is reachable from outside your internal network.*

At a glance

Fact	Detail
Product	TOTOLINK N350RT (CVE-2026-137043)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 26 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 26 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	Owners or administrators of TOTOLINK N350RT routers running firmware 9.3.5u.6466_B20250825 or 9.3.5u.6468_B20250827.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you have a TOTOLINK N350RT router on your network?	Nothing to do for this CVE.	Check the firmware version (next question).
Is the firmware 9.3.5u.6466_B20250825 or 9.3.5u.6468_B20250827?	The record does not list your version as affected; monitor for updates.	Check whether the management interface is reachable from outside (next question).
Can anyone outside your internal network reach the router's web management page?	Exposure is reduced; apply any vendor patch when available.	Block that access immediately, then apply any vendor patch when available.

What it is

An attacker who can reach the router's web management interface can send a crafted request to modify the device's configuration without logging in or supplying any credentials.

Things people will get wrong

- Only the language setting can be changed, so the impact is minor. The researcher used the language setting as the example. The record describes a broader authorization bypass on the management endpoint itself, not a limit to that one function.
- This only matters if the router's admin page is exposed to the internet. The record says the attack can be executed remotely. Any device on the same local network, or reachable through another compromised system, can reach the management interface.

How we would triage it

This is our judgement.

Step 1: Find which TOTOLINK N350RT units you run and their firmware

- Log in to each TOTOLINK N350RT's management web interface and locate the firmware version on the device status or about page.
- Check whether the version matches 9.3.5u.6466_B20250825 or 9.3.5u.6468_B20250827, as listed in the CVE record.

Step 2: Block external access to the management interface

- Confirm that the router's web management port is not forwarded to the internet or bound to the WAN interface.
- If it is externally reachable, block that access at the upstream firewall or disable remote management in the router's own settings.

Step 3: Watch for a patched firmware from the vendor

- No fixed firmware version is recorded in the CVE record as of 26 November 2026. Check the TOTOLINK support pages for firmware updates referencing CVE-2026-137043.
- Once a patch is available, apply it and verify the firmware version afterwards.

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 have been made aware of CVE-2026-137043, a flaw affecting TOTOLINK N350RT routers on firmware 9.3.5u.6466_B20250825 or 9.3.5u.6468_B20250827. The flaw allows anyone to change the router's configuration without logging in; the CVE record scores it 10 out of 10 under CVSS 4.0 and no fixed version is recorded as of 26 November 2026. Please confirm: whether we run any TOTOLINK N350RT units; the exact firmware version on each; whether the management interface is reachable from outside our network; and what steps are planned to address this. We would like written confirmation of the firmware version and your planned action by [date].*

The weakness behind it

The record classes this as CWE-639 and CWE-285.

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 flaw is in a web-facing management endpoint reachable without login; exploiting it would likely serve as initial access for any attacker with network reach to the device.
Data Manipulation: Stored Data Manipulation (T1565.001): Changing stored data without permission.	Impact: causing damage or disruption	The record and the researcher's proof of concept describe persistent modification of device configuration as the direct outcome; a successful exploit would likely result in permanently altered stored settings.

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 security vulnerability has been detected in TOTOLINK N350RT 9.3.5u.6468_B20250827/9.3.5u.6466_B20250825. The affected element is the function setLanguageCfg of the file /cgi-bin/cstecgi.cgi. Such manipulation of the argument lang leads to authorization bypass. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.*

Versions of TOTOLINK N350RT the record lists as affected:

- 9.3.5u.6466_B20250825
- 9.3.5u.6468_B20250827

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-2026-137043
```

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-2026-137043
```

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 the vendor has acknowledged the flaw or intends to release a patched firmware, and when.
- Whether other management endpoints in cstecgi.cgi are reachable without authentication beyond the one the researcher demonstrated.
- Whether the management interface is exposed on the WAN port by default in the affected firmware builds.
- Whether any workaround, such as disabling remote management, fully prevents exploitation on an unpatched device.
- 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 26 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", "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-2026-137043: 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
26 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 N350RT on affected firmware with management interface reachable from the internet	High	Immediately

TOTOLINK N350RT on affected firmware, management interface on internal network only	Medium	This week
TOTOLINK N350RT on affected firmware, management access restricted to a single trusted host	Low	Next patch cycle
TOTOLINK N350RT present but firmware version not listed as affected in the record	None	None for this CVE

Appendix 4. Definition of done

- Every TOTOLINK N350RT 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-2026-137043: https://www.cve.org/CVERecord?id=CVE-2026-137043
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: gist.github.com/aslanbekthedefender/15846cb866cab1e7a1dfb197a84: https://gist.github.com/aslanbekthedefender/15846cb866cab1e7a1dfb197a84ee823
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/443967
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/443967/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-137043