contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

TRENDnet TEW-657BRM: new CVE

CVE-2026-129351 · record published 14 November 2026

Analysis Report

If you still have a TRENDnet TEW-657BRM in use, plan to replace it: the vendor says it has been out of support for more than 15 years and no fix is recorded. First, find it and make sure its web …

PREPARED BY	NamiQ	DATE	15 November 2026
FACTS AS OF	15 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/trendnet-tew-657brm-cve-2026-129351

The bottom line

> *If you still have a TRENDnet TEW-657BRM in use, plan to replace it: the vendor says it has been out of support for more than 15 years and no fix is recorded. First, find it and make sure its web interface cannot be reached from the internet. If you have none, you can stop reading.*

At a glance

Fact	Detail
Product	TRENDnet TEW-657BRM (CVE-2026-129351)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 14 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 15 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 still runs a TRENDnet TEW-657BRM router, especially on firmware 1.00.1, the only version the record lists. Look first at any unit whose web management page can be reached from the internet or from an untrusted network.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you still have a TRENDnet TEW-657BRM router anywhere in use?	Nothing to do for this CVE.	Check which firmware it runs (next question).
Does it run firmware 1.00.1, or can you not tell?	The record lists only 1.00.1, but no fix exists, so plan to replace it anyway.	Treat it as affected and check who can reach it (next question).
Can its web management page be reached from the internet or by untrusted users?	Lower urgency. Plan to replace it in your next hardware cycle.	Block that access now and replace the device as soon as you can.

What it is

The record says a request to the router's setup page, /setup.cgi in its built-in web server, can write past the end of a memory buffer. The record says this can be done remotely. Writing out of bounds

like this can crash the device. In some cases it can also let an attacker run their own code on it.

Why it matters

The record gives this its top score of 10. It says the attack works remotely and that an exploit has been published. The vendor will not fix it because the product is out of support. Our reading is that a router is a useful foothold: it sits between your network and the internet and sees all the traffic that passes through it. Taking over the device would typically give an attacker that position. With no fix coming, the only lasting remedy is to replace the router.

Things people will get wrong

- "A firmware update will fix this." No fixed version is recorded. The vendor says the product has been out of support for more than 15 years and that it cannot confirm the flaw exists.
- "The vendor couldn't confirm it, so it probably isn't real." The record says an exploit has been published. The vendor only says it cannot check a product it stopped supporting. That is not a finding that the flaw is absent.
- "Only firmware 1.00.1 matters, so other versions are safe." The record lists only 1.00.1. It says nothing about other versions, and no version is recorded as unaffected.

How we would triage it

This is our judgement.

Step 1: Find any TEW-657BRM still in use

- Check your asset list, and the label or status page of each router, for the model name TEW-657BRM. Old routers often stay running long after people stop thinking about them.
- Note the firmware version shown on its status page. The record lists 1.00.1 as affected.

Step 2: Cut off access to its web management page

- Make sure remote management is turned off. The flaw is in /setup.cgi in the device's web server, and the record says it can be reached remotely.
- Limit the management page to one trusted machine on the local network until the device is replaced.

Step 3: Replace the device

- Order a supported router to replace it. The vendor says this model has been out of support for more than 15 years, and no fix is recorded.

- Move its settings across by hand rather than importing a backup taken from the old unit.

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.

> *Hello, we have seen CVE-2026-129351, a flaw in the TRENDnet TEW-657BRM router. It lets an attacker write past the end of a memory buffer through the router's web setup page, and the record says this can be done remotely. Could you check whether we have any TEW-657BRM in use, where it sits, and which firmware it runs? The record lists version 1.00.1. No fixed version is recorded, and the vendor says the product has been out of support for more than 15 years. If we have one, please turn off any access to its management page from outside, and propose a replacement. Please confirm in writing what you found and what you changed within two weeks. Thank you.*

The weakness behind it

The record classes this as CWE-787 and CWE-119.

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	Likely: the record says the flaw is in /setup.cgi in the router's built-in web server and can be used remotely. That points to an attack on an exposed web service.
Endpoint Denial of Service (T1499): Crashing or overloading a single system or application.	Impact: causing damage or disruption	Likely: an out-of-bounds memory write in the web server would typically be able to crash the device. That would cut off the network it serves.

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 TRENDnet TEW-657BRM 1.00.1. This vulnerability affects the function sprintf of the file /setup.cgi of the component mini_httpd. Such manipulation leads to out-of-bounds write. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The vendor explains: ""I am not able to confirm if such vulnerability exists as the product has been EOL for more than 15 years. We will send out an announcement letting customers know." This vulnerability only affects products that are no longer supported by the maintainer.*

Versions of TRENDnet TEW-657BRM the record lists as affected:

- 1.00.1

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-2026-129351
```

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-2026-129351
```

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 firmware versions other than 1.00.1 are affected. The record lists only that one.
- Whether an attacker must log in to the router before sending the harmful request. The record does not say.
- What the vendor's planned customer announcement will say, or when it will be sent.
- 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 15 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-2026-129351: 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
14 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 TEW-657BRM on firmware 1.00.1 with its management page reachable from the internet	Medium	this week

A TEW-657BRM reachable only from a shared or guest network	Medium	within the month
A TEW-657BRM reachable only from a small, trusted office network	Low	next hardware replacement cycle
No TEW-657BRM anywhere in the estate	None	none for this CVE

Appendix 4. Definition of done

- Every TRENDnet TEW-657BRM 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-2026-129351: https://www.cve.org/CVERecord?id=CVE-2026-129351
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/437397
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/437397/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-129351