contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

TRENDnet TEW-751DR: new CVE

CVE-2026-138004 · record published 27 November 2026

Analysis Report

If you do not run a TRENDnet TEW-751DR or TEW-733GR router, you can stop reading. Anyone who does, on firmware 1.03B01, must act now: no patched version is recorded in any source, so isolate or plan …

PREPARED BY	NamiQ	DATE	27 November 2026
FACTS AS OF	27 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-751dr-cve-2026-138004

The bottom line

> *If you do not run a TRENDnet TEW-751DR or TEW-733GR router, you can stop reading. Anyone who does, on firmware 1.03B01, must act now: no patched version is recorded in any source, so isolate or plan to replace the device.*

At a glance

Fact	Detail
Product	TRENDnet TEW-751DR (CVE-2026-138004)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 27 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 27 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No source records a patched firmware version. The CVE record lists no unaffected releases.
Who looks first	Owners and operators of a TRENDnet TEW-751DR or TEW-733GR router running firmware 1.03B01. The CVE record names both models. If neither is on your network, nothing here applies to you.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a TRENDnet TEW-751DR or TEW-733GR router anywhere on your network?	Nothing to do for this CVE.	Check the firmware version (next question).
Is the installed firmware version 1.03B01?	The record lists only 1.03B01; confirm you have a later version.	No patched version is recorded; see the steps below.
Can port 49152 on the router be reached from outside your local network?	Risk is limited to users already on your LAN; still act promptly.	Isolate the device from internet access immediately.

What it is

The record says an unauthenticated attacker who can reach the router's UPnP control service can inject shell commands that run as root on the device. A researcher's notes say this gives full control:

settings can be changed, remote access opened, and the admin password overwritten, all without any credential.

Why it matters

A researcher's notes say the vulnerable endpoint runs as root and requires no credentials, so an attacker who can reach port 49152 gains immediate full control of the device. The source states WAN-side exposure was not verified, so the realistic immediate risk is from someone already on the LAN. No patched firmware is listed anywhere in the record or its sources. Our reading is that a score-10 unauthenticated flaw with no available fix makes isolation or replacement the right response even without a CISA deadline, because there is no documented way to close the exposure otherwise.

Things people will get wrong

- Only the TEW-751DR is affected The CVE record's description names both TEW-751DR and TEW-733GR on firmware 1.03B01. A researcher also notes both models share identical firmware at the vulnerable path.
- This only matters if the router faces the internet A researcher's notes say the service runs on the LAN side. No authentication is required, so any user or compromised device on the local network can exploit it.
- A newer firmware must exist because this is an older model No source records a fixed version. The CVE record's unaffected releases list is empty. Do not assume a patch exists without verifying it directly on TRENDnet's support pages.

How we would triage it

This is our judgement.

Step 1: Find every TRENDnet TEW-751DR and TEW-733GR on your network

- Log in to the router's admin interface and find the firmware version on the status or about page; the affected version is 1.03B01 as listed in the CVE record.
- If you are unsure whether these models are present, check your network documentation or scan your LAN for the device.

Step 2: Reduce exposure while you decide on a fix

- If your firewall or upstream device allows it, block external access to port 49152 on the affected router.

- A researcher's notes state WAN exposure was not verified; check whether port 49152 is reachable from outside your network.

Step 3: Check TRENDnet's support pages for updated firmware

- No patched firmware is recorded in the CVE record or any source reviewed; check TRENDnet's support pages for the TEW-751DR and TEW-733GR directly.
- A changelog entry that does not name this CVE is not proof that a release fixes it; look for a dedicated security advisory from TRENDnet.

Step 4: Isolate or replace the device if no patch is available

- If TRENDnet has not released patched firmware, treat the device as unmitigated and remove it from active service or replace it.
- If the device must remain temporarily, place it behind a firewall that restricts untrusted LAN hosts from reaching port 49152.

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-2026-138004, a score-10 unauthenticated command-injection flaw in TRENDnet TEW-751DR and TEW-733GR routers on firmware 1.03B01. An unauthenticated attacker who can reach the router's UPnP service on port 49152 gains full shell access as root. No patched firmware version is recorded. Please check whether we run either model on our network, confirm the firmware version installed, and advise whether TRENDnet has released a fix. If a patch exists, confirm the version and an application date. If not, please recommend isolation or replacement. We would like written confirmation by [date].*

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
Exploitation of Remote Services (T1210): Exploiting a flaw in a service on another machine to move to it.	Lateral Movement: moving to other machines	An attacker on the LAN would likely exploit this unauthenticated network-reachable injection to move from a host to controlling the router, fitting exploitation of a remote service for lateral movement.
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 is the recorded weakness; the description says the service argument leads to command execution, which would typically involve a shell interpreter running attacker-supplied strings as root.
Account Manipulation (T1098): Changing an existing account, for example adding permissions or keys, to keep access.	Persistence: staying in	A researcher's notes say the flaw allows the admin password to be rewritten. Overwriting credentials to gain persistent administrative access to the router would typically fit account manipulation.

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-751DR and TEW-733GR 1.03B01. Affected is the function soapcgi_main of the file /soap.cgi of the component UPnP Igd Control Endpoint. Such manipulation of the argument service leads to os command injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.*

Versions of TRENDnet TEW-751DR the record lists as affected:

- 1.03B01

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-2026-138004
```

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-2026-138004
```

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 TRENDnet has released or plans to release a firmware update that addresses this flaw.
- Whether the UPnP service on these models can be disabled through the admin interface as a workaround.
- Whether firmware versions other than 1.03B01 share the same vulnerable code.
- Whether the default factory configuration exposes port 49152 to the WAN interface.
- 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 27 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-2026-138004: 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
27 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
TEW-751DR or TEW-733GR on firmware 1.03B01 with port 49152 reachable from the internet	High	Immediately

TEW-751DR or TEW-733GR on firmware 1.03B01, active on a LAN; no WAN exposure confirmed	High	This week
One of the named devices is in use but firmware version has not yet been checked	Medium	This week
Device is connected but not actively routing traffic	Low	Next scheduled review
Neither TEW-751DR nor TEW-733GR is present on the network	None	None for this CVE

Appendix 4. Definition of done

- Every TRENDnet TEW-751DR 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-2026-138004: https://www.cve.org/CVERecord?id=CVE-2026-138004
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: gist.github.com/qwq-nm/251e7963d59f41beea2c7ad5ff7ca39f: https://gist.github.com/qwq-nm/251e7963d59f41beea2c7ad5ff7ca39f
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/444939
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/444939/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-138004