contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Tenda RX3: new CVE

CVE-2026-136553 · record published 25 November 2026

Analysis Report

Anyone running a Tenda RX3 on firmware 16.03.13.11_multi should act now: the record scores this 10 out of 10 under CVSS 4.0, the exploit is public, and no fixed version is recorded. Block access to …

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/tenda-rx3-cve-2026-136553

The bottom line

> *Anyone running a Tenda RX3 on firmware 16.03.13.11_multi should act now: the record scores this 10 out of 10 under CVSS 4.0, the exploit is public, and no fixed version is recorded. Block access to the router's admin interface from outside your local network immediately.*

At a glance

Fact	Detail
Product	Tenda RX3 (CVE-2026-136553)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 25 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	Anyone operating a Tenda RX3 router on firmware version 16.03.13.11_multi. Risk is highest where the router's admin web interface can be reached from outside the local network.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a Tenda RX3 router?	Nothing to do for this CVE.	Check the firmware version.
Is the firmware version 16.03.13.11_multi?	The record lists no other versions as affected; monitor the vendor for guidance.	Continue to the next question.
Can the router's web admin page be reached from outside your local network?	Lower immediate risk; still apply a patch when one is released.	Block that access now and treat this as urgent.

What it is

The record says an attacker can manipulate the loginPwd argument on the router's WiFi-setup endpoint to bypass authentication entirely, without knowing the password, over a network connection.

Why it matters

The flaw is in the WiFi-setup endpoint's handling of the login password parameter (CWE-287, Improper Authentication). A score of 10 under CVSS 4.0 reflects that the attack needs no prior access and can be launched remotely. The exploit is already public, as the record states, which removes any grace period. No fixed firmware version appears in the record. Our reading is that the main exposure is any path from the internet to the router's admin interface; closing that path is the most effective step available until a vendor patch is named.

Things people will get wrong

- A patch must exist because the score is 10. The record names no fixed version and lists no unaffected releases. A high score reflects severity, not vendor response.
- This is on CISA's exploited-vulnerabilities list. The record was not on CISA's list when read. The exploit is public, but CISA's listing is a separate determination.

How we would triage it

This is our judgement.

Step 1: Find which Tenda RX3 firmware you run

- Log in to the router's admin interface and check the firmware version shown on the status or about page.
- The record identifies 16.03.13.11_multi as the affected version; note whether yours matches.

Step 2: Block external access to the admin interface

- Check whether the router's admin web port is accessible from outside your local network.
- If it is, disable remote management in the router's settings or block that port at your network boundary.

Step 3: Watch for a vendor patch

- The record names no fixed firmware version; check Tenda's support pages for a release that addresses this flaw.
- Apply any update that names CVE-2026-136553 or covers this endpoint.

Step 4: Review for unexpected access if the router was exposed

- If the admin interface was reachable from outside, review the router's access logs for unexpected logins or configuration changes.
- Pay particular attention to WiFi settings, as the vulnerable endpoint handles WiFi setup.

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 our exposure to CVE-2026-136553, a publicly available authentication-bypass flaw in Tenda RX3 firmware 16.03.13.11_multi. The record scores this 10 out of 10 under CVSS 4.0. No fixed firmware version has been recorded. Please confirm whether we run this device and firmware version, whether its admin interface is reachable from outside our local network, what immediate steps have been taken to restrict that access, and when we can expect a patched firmware. We ask for written confirmation of the current version and any actions taken by a date you can commit to.*

The weakness behind it

The record classes this as CWE-287.

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 vulnerable endpoint is a web form reachable over a network; if the admin interface faces the internet, an attacker would likely exploit it directly for initial access.
External Remote Services (T1133): Using a remote-access service such as a VPN or remote desktop to get into the network.	Initial Access: getting in	The record says the attack can be launched remotely; bypassing router authentication via an external path would typically match external remote services as an entry point.
Modify Authentication Process (T1556): Changing how the system checks logins so that a wrong or empty password is accepted.	Credential Access: stealing logins	CWE-287 is Improper Authentication; the flaw is in the authentication mechanism itself, which an attacker would likely exploit to subvert the login check entirely.

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 vulnerability was detected in Tenda RX3 16.03.13.11_multi. Affected is an unknown function of the file /goform/fast_setting_wifi_set. Performing a manipulation of the argument loginPwd results in improper authentication. It is possible to initiate the attack remotely. The exploit is now public and may be used.*

Versions of Tenda RX3 the record lists as affected:

- 16.03.13.11_multi

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-2026-136553
```

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-2026-136553
```

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 Tenda has acknowledged this flaw or committed to a fix; the record names no vendor response.
- Whether firmware versions other than 16.03.13.11_multi are affected; the record lists only this one.
- Whether exploitation requires internet-facing exposure or whether a local network attacker is sufficient.
- Whether any workaround short of blocking the admin interface is available.
- 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 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-2026-136553: 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
25 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
Tenda RX3 on firmware 16.03.13.11_multi with admin interface reachable from the internet	Medium	Immediately — no patch available, exploit is public

Tenda RX3 on firmware 16.03.13.11_multi, admin interface on internal network only	Medium	This week — apply a vendor patch when one is available
Tenda RX3 on a firmware version other than 16.03.13.11_multi	Low	Monitor the vendor; the record lists no other affected versions
No Tenda RX3 in the estate	None	Nothing to do for this CVE

Appendix 4. Definition of done

- Every Tenda RX3 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-2026-136553: https://www.cve.org/CVERecord?id=CVE-2026-136553
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/443410
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/443410/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-136553