contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Tenda RX3: new CVE

CVE-2026-136547 · record published 25 November 2026

Analysis Report

Anyone running a Tenda RX3 on firmware 16.03.13.11_multi should act immediately — the exploit is publicly disclosed, the score is 10, and no fixed firmware is recorded. Disable remote management …

PREPARED BY	NamiQ	DATE	25 November 2026
FACTS AS OF	25 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-2026-136547

The bottom line

> *Anyone running a Tenda RX3 on firmware 16.03.13.11_multi should act immediately — the exploit is publicly disclosed, the score is 10, and no fixed firmware is recorded. Disable remote management access from the internet as a first step.*

At a glance

Fact	Detail
Product	Tenda RX3 (CVE-2026-136547)
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 25 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 of a Tenda RX3 router running firmware 16.03.13.11_multi, particularly where the router's management interface is reachable 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 (next question).
Is the firmware version 16.03.13.11_multi?	The record does not list your version as affected; monitor the vendor for updates.	Continue — check whether remote management is reachable from outside.
Is the router's management interface reachable from the internet?	Exposure is reduced; apply a firmware update when one is confirmed to fix this CVE.	Disable remote access immediately and check the router's logs.

What it is

The record says an attacker on the internet can bypass the router's login check without a valid password, exploiting a flaw in the web management component. The exploit has been publicly disclosed.

Why it matters

Our reading is that this warrants urgent attention. The score is 10, the highest possible under CVSS 4.0, and the exploit is publicly disclosed. The flaw (CWE-287) is in the router's authentication handler: the web server fails to verify who is making a request. A router controls network traffic and DNS; an authentication bypass may allow an attacker to redirect traffic, disable firewall rules, or open access paths into the network behind it. No fixed firmware is recorded.

Things people will get wrong

- Changing the admin password protects the router from this flaw. The record describes an authentication bypass, not a weak-password problem. CWE-287 means the authentication check itself is flawed; a strong password may not prevent the attack.
- Installing the latest Tenda firmware fixes this. No fixed firmware version is recorded in the CVE record or in any source available for this CVE. Do not treat a routine update as a fix unless it names CVE-2026-136547 specifically.

How we would triage it

This is our judgement.

Step 1: Find the firmware version on your Tenda RX3

- Log into the router's local management interface and locate the firmware version on the status or about page.
- If the version shown is 16.03.13.11_multi, the record identifies this router as affected.

Step 2: Disable remote management access from the internet

- In the router settings, find the remote or WAN management option and turn it off.
- This removes the publicly reachable attack surface while no patched firmware is recorded.

Step 3: Review the router's logs for unexpected access

- Check the router's system log for login attempts or management-interface connections from external IP addresses.
- Successful sessions from outside your local network at unexpected times warrant further investigation.

Step 4: Watch for a patched firmware from Tenda

- No fixed version is recorded; check the Tenda support site for a firmware release that names CVE-2026-136547.
- After installing any update, confirm that the firmware version shown on the router has changed.

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-2026-136547, a publicly disclosed authentication bypass affecting the Tenda RX3 router on firmware 16.03.13.11_multi. The flaw is in the router's web management component and can be exploited remotely without valid credentials. The score is 10, the highest possible under CVSS 4.0, and no fixed firmware version is recorded. Please confirm whether we have a Tenda RX3 running this firmware, whether its management interface is reachable from the internet, and whether remote access can be disabled. Please provide written confirmation of the router's current firmware version and the action taken by [date].*

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 record describes a remotely exploitable flaw in a web management interface; a publicly disclosed exploit would likely target it directly to gain access without credentials.
Account Manipulation (T1098): Changing an existing account, for example adding permissions or keys, to keep access.	Persistence: staying in	After bypassing authentication on a router, an attacker would likely modify admin credentials or add an account to maintain persistent access to the device.

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 determined in Tenda RX3 16.03.13.11_multi. Impacted is the function R7WebsSecurityHandler of the component httpd. Executing a manipulation can lead to improper authentication. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.*

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-2026-136547
```

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-2026-136547
```

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 released or intends to release a patched firmware version that addresses this flaw.
- Whether the bypass grants full administrative access or is limited to specific functions within the management interface.
- Whether other Tenda router models share the same httpd authentication handler and are equally exposed.
- 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 25 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-2026-136547: 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 management interface reachable from the internet	Medium	Immediately — disable remote management today

Tenda RX3 on firmware 16.03.13.11_multi, management reachable on the LAN only	Medium	Apply firmware update when one is confirmed to fix this CVE
Tenda RX3 on a firmware version other than 16.03.13.11_multi	Low	Monitor the Tenda support site for a security advisory
Network running a different router model entirely	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-2026-136547: https://www.cve.org/CVERecord?id=CVE-2026-136547
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/443405
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/443405/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-136547