contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Comfast CF-WR632AX: new CVE

CVE-2026-122013 · record published 4 November 2026

Analysis Report

CVE-2026-122013 in Comfast CF-WR632AX, a new record scored 10 and not on CISA's exploited list when we read it. What it is, who is affected, and what to check first.

PREPARED BY	NamiQ	DATE	5 November 2026
FACTS AS OF	5 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/comfast-cf-wr632ax-cve-2026-122013

The bottom line

> *Check whether you run Comfast CF-WR632AX. If you do, read the vendor's page for the fixed version and update. Nothing public says yet that anyone is using this flaw.*

At a glance

Fact	Detail
Product	Comfast CF-WR632AX (CVE-2026-122013)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 4 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 5 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 running a Comfast CF-WR632AX router on firmware 2.6.0.1 whose web management interface is reachable from untrusted networks or the internet.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a Comfast CF-WR632AX router?	Nothing to do for this CVE.	Check the firmware version (next question).
Is the firmware version 2.6.0.1?	The record lists only 2.6.0.1 as affected; monitor for vendor updates.	Check whether the management interface is reachable by untrusted users (next).
Can anyone untrusted reach the router's web management interface?	Risk is lower; still apply a patch when the vendor releases one.	Restrict access to the management interface immediately.

What it is

An attacker who can reach the router's web management interface can supply a crafted filename to the multipart parser and traverse directory paths. The GitHub source in the record names this an arbitrary file write.

Why it matters

The multipart parser does not constrain the filename argument, allowing a crafted value to traverse directory boundaries. The GitHub source names this an arbitrary file write; the record describes path traversal via the filename. Our reading is that an attacker who can reach the management interface could write files anywhere on the device, potentially overwriting configuration or system files. The CVSS 4.0 score is 10, the maximum on that scale. The exploit is public and the vendor did not respond to disclosure.

Things people will get wrong

- If the router is on an internal network, it cannot be exploited. The record says the attack is possible remotely. Any user who can reach the web management interface, including internal users, can attempt it.
- A patched firmware version is available to update to. The record lists no unaffected releases. No fixed firmware version is recorded and the vendor did not respond to disclosure.

How we would triage it

This is our judgement.

Step 1: Find the firmware version on your router

- Log in to the Comfast CF-WR632AX web management interface and locate the firmware or system information page.
- If the version shown is 2.6.0.1, the device is in the version the record names as affected.

Step 2: Restrict access to the web management interface

- Block access to the router's management interface from untrusted networks, including the internet.
- Limit management access to specific administrator IP addresses where the router supports it.

Step 3: Watch for a vendor firmware update

- No fixed version is recorded and the vendor did not respond to the researcher's disclosure.
- Check the Comfast support or downloads page for new firmware; apply it when one that addresses this flaw appears.

Step 4: Check for unexpected file changes if the interface was exposed

- If the management interface was reachable by untrusted users while on firmware 2.6.0.1, review the router's configuration and system files for unexpected additions or changes.
- Consider replacing the device if its integrity cannot be confirmed.

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.

The weakness behind it

The record classes this as CWE-22.

The sources, in their words

The CVE record:

> *A vulnerability was detected in Comfast CF-WR632AX 2.6.0.1. Affected by this vulnerability is an unknown functionality of the file /usr/bin/webmgnt of the component Multipart Parser. Performing a manipulation of the argument filename results in path traversal. It is possible to initiate the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.*

Versions of Comfast CF-WR632AX the record lists as affected:

- 2.6.0.1

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-2026-122013
```

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 names of running container images 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-2026-122013
```

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. It reads the names of the running images, not what is 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 authentication is required to trigger the flaw, or whether it can be reached before login.
- Whether any firmware version other than 2.6.0.1 is affected.
- Whether the vendor has acknowledged the report or plans a fix.
- 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 5 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- The sections headed "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong" and "How we would triage it" are our interpretation

of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-122013: 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
4 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
CF-WR632AX on firmware 2.6.0.1, web management interface reachable from the internet	Medium	Immediately

CF-WR632AX on firmware 2.6.0.1, management interface reachable from internal network with untrusted users	Medium	This week
CF-WR632AX on firmware 2.6.0.1, management interface restricted to trusted administrators only	Medium	Next patch cycle
CF-WR632AX on a firmware version other than 2.6.0.1	Low	Monitor for vendor updates

Appendix 4. Definition of done

- Every Comfast CF-WR632AX 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-2026-122013: https://www.cve.org/CVERecord?id=CVE-2026-122013
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/FoundTL/COMFAST-CF-WR632AX-Wi-Fi-6-Router: https://github.com/FoundTL/COMFAST-CF-WR632AX-Wi-Fi-6-Router
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/431080
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/431080/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-122013