contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

WAVLINK WL-WN530BE1-A: new CVE

CVE-2026-120198 · record published 1 November 2026

Analysis Report

If you run a WAVLINK WL-WN530BE1-A on firmware V251117, find out this week whether its web interface can be reached from outside, and cut that access first. If you have no such device, you can stop …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 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/wavlink-wl-wn530be1-a-cve-2026-120198

The bottom line

> *If you run a WAVLINK WL-WN530BE1-A on firmware V251117, find out this week whether its web interface can be reached from outside, and cut that access first. If you have no such device, you can stop reading.*

At a glance

Fact	Detail
Product	WAVLINK WL-WN530BE1-A (CVE-2026-120198)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 1 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 1 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 with a WAVLINK WL-WN530BE1-A on firmware V251117, and the IT provider who installed or manages it. The record names no other model or version.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a WAVLINK WL-WN530BE1-A?	Nothing to do for this CVE.	Check the firmware version (next question).
Is the firmware version V251117?	The record lists only V251117; ask the vendor about your version.	Treat the device as exposed (next question).
Can the device's web interface be reached from the internet or by untrusted users?	Lower urgency, but still plan to fix it.	Remove that access now, then ask for a fix.

What it is

The record says a crafted value in the group_name or IP-FROM argument of /protocol.csp lets an attacker run their own commands on the device. It says the attack can be launched remotely and that the exploit has been disclosed publicly.

Why it matters

Our reading: command injection on a network device can give an attacker control of a box that sits between your staff and the internet. The score is 10, and the record says no login is mentioned and the attack can be remote. The exploit is public, so waiting for CISA to list it is not a safe plan.

Things people will get wrong

- "It is not on the CISA list, so nobody is using it." The record is new and not listed when read. That does not mean no one is exploiting it, and the record says the exploit is public.
- "The vendor has already patched it." No source we could read names a fixed version. The record says only that the vendor was contacted early.
- "It needs a login, so it is low risk." The description mentions no login. It says the attack can be launched remotely.

How we would triage it

This is our judgement.

Step 1: Find the devices and versions you run

- List every WAVLINK WL-WN530BE1-A, including ones installed by others.
- Read the firmware version from the device's admin page. The record names only V251117 as affected.

Step 2: Reduce exposure

- Block access to the device's web interface from the internet.
- Limit who on the internal network can reach it, because the flaw is in a web request handler.

Step 3: Ask for a fix

- Ask WAVLINK or your supplier for a fixed firmware version. No source we read names one.
- If no fix exists, ask your IT provider whether to replace the device.

Step 4: Check after the change

- Confirm from outside your network that the admin page no longer answers.
- Record the firmware version once a fix is installed.

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 are checking exposure to CVE-2026-120198, a command injection flaw (CWE-77, CWE-74) in the WAVLINK WL-WN530BE1-A, firmware V251117. Please tell us whether we run this device, where, and which firmware version. Please confirm that its web interface is not reachable from the internet. We cannot find a fixed version in the record, so please ask the vendor for one. Please confirm the version and the fix to us in writing by the date you suggest. Thank you.*

The weakness behind it

The record classes this as CWE-77 and CWE-74.

The sources, in their words

The CVE record:

> *A vulnerability has been found in WAVLINK WL-WN530BE1-A V251117. Affected is the function con_check_read_finish of the file /protocol.csp. Such manipulation of the argument group_name/IP-FROM leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure.*

Versions of WAVLINK WL-WN530BE1-A the record lists as affected:

- V251117

What we do not know yet

- Whether the vendor has released a fixed firmware version; no source we could read names one.
- Whether a login is required to reach the vulnerable function; the description does not say.

- Whether other WAVLINK models or firmware versions are affected; the record lists only V251117.
- Whether anyone is exploiting this in practice; the record says the exploit is public, but CISA had not listed it when read.
- 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 1 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", "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-2026-120198: 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
1 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 V251117 device whose web interface faces the internet	Medium	Now: remove the exposure this week

A V251117 device on an internal network that visitors or guests can join	Medium	This week
A V251117 device reachable only by trusted staff	Medium	Next patch cycle, once a fix exists
A WAVLINK device on another firmware version	Low	Ask the vendor; the record is silent
No WAVLINK WL-WN530BE1-A in the estate	None	None for this CVE

Appendix 4. Definition of done

- Every WAVLINK WL-WN530BE1-A 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-2026-120198: https://www.cve.org/CVERecord?id=CVE-2026-120198
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/429561
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/429561/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-120198