contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

WAVLINK WN536AX6-A: new CVE

CVE-2026-120276 · record published 1 November 2026

Analysis Report

Anyone running WAVLINK WN536AX6-A on firmware V260507_2.0.0 should act this week: the record scores 10 on CVSS 4.0 and a working exploit is publicly available. No fixed version is known from any …

PREPARED BY	NamiQ	DATE	2 November 2026
FACTS AS OF	2 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-wn536ax6-a-cve-2026-120276

The bottom line

> *Anyone running WAVLINK WN536AX6-A on firmware V260507_2.0.0 should act this week: the record scores 10 on CVSS 4.0 and a working exploit is publicly available. No fixed version is known from any source; take the web management interface off any untrusted network as the first step.*

At a glance

Fact	Detail
Product	WAVLINK WN536AX6-A (CVE-2026-120276)
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 2 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 administering a WAVLINK WN536AX6-A router on firmware V260507_2.0.0, particularly where the web management interface is reachable from outside a trusted local network.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a WAVLINK WN536AX6-A router?	Nothing to do for this CVE.	Check the firmware version on the device.
Does the firmware version on the device show V260507_2.0.0?	The record lists only V260507_2.0.0; monitor the vendor for updates.	Check whether the web management interface can be reached from outside a trusted network.
Can anyone outside your trusted network reach the web management interface?	Risk is reduced; watch for a firmware update from the vendor.	Restrict access to the management interface immediately.

What it is

An attacker who can reach the web management interface can inject operating-system commands by manipulating the group_name argument handled by the function sub_416760 in /bin/ioos. The attack is fully remote and the record notes the exploit is publicly available.

Things people will get wrong

- This is low priority because it is not on CISA's exploitation list. The record scores 10 on CVSS 4.0 and a working exploit is publicly available. Absence from CISA's list reflects the timing of the record, not the severity of the flaw.
- Changing the router admin password removes the risk. The record describes command injection via a specific argument in the web interface, not a credential weakness. Network isolation of the management interface is the relevant control until a patch exists.

How we would triage it

This is our judgement.

Step 1: Find which firmware version the router runs

- Log in to the WAVLINK WN536AX6-A web management interface and locate the firmware version in the status or system information page.
- The record identifies V260507_2.0.0 as the affected version; note the exact string shown on the device.

Step 2: Restrict access to the web management interface

- If the device is on V260507_2.0.0, configure firewall or access-control rules so the web management interface is reachable only from a specific trusted host or management VLAN.
- If the interface is currently exposed to the internet or a guest network, remove that exposure immediately.

Step 3: Check the vendor for a firmware update

- No fixed version is named in any source read for this record; check WAVLINK's support pages for WN536AX6-A firmware newer than V260507_2.0.0.
- Install any update that post-dates 1 November 2026 and review its release notes for mention of CVE-2026-120276 or CWE-78.

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 writing to ask you to check whether we run a WAVLINK WN536AX6-A router on firmware version V260507_2.0.0. A vulnerability, CVE-2026-120276, published 1 November 2026, scores 10 on CVSS 4.0 and allows remote command injection through the web management interface. A working exploit is publicly available and no fixed firmware version is known at this time. Please confirm whether this device and version are present in our network, whether the web management interface is reachable from outside a trusted host, and what steps will be taken to restrict that access. We would like written confirmation of the current version and any planned remediation by the end of this week.*

The weakness behind it

The record classes this as CWE-78 and CWE-77.

The sources, in their words

The CVE record:

> *A weakness has been identified in WAVLINK WN536AX6-A V260507_2.0.0. This vulnerability affects the function sub_416760 of the file /bin/ioos of the component Web Management Interface. This manipulation of the argument group_name causes os command injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure.*

Versions of WAVLINK WN536AX6-A the record lists as affected:

- V260507_2.0.0

What we do not know yet

- No fixed firmware version is named in any source; it is not known whether a patch has been released or promised by the vendor.
- The record does not state whether authentication is required to reach the vulnerable function in the web management interface.

- It is not stated whether other WAVLINK models or firmware branches share the same vulnerable code path.
- The vendor's response to early disclosure is not detailed in the available record.
- 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 2 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", "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-2026-120276: 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
WN536AX6-A on V260507_2.0.0 with web management interface reachable from the internet	Medium	Immediately

WN536AX6-A on V260507_2.0.0 with management reachable from a guest or untrusted LAN segment	Medium	This week
WN536AX6-A on V260507_2.0.0 with management restricted to a single trusted host	Medium	Next patch cycle
WN536AX6-A running a firmware version other than V260507_2.0.0	Low	Monitor the vendor for updates
No WAVLINK WN536AX6-A in use	None	None for this CVE

Appendix 4. Definition of done

- Every WAVLINK WN536AX6-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-2026-120276: https://www.cve.org/CVERecord?id=CVE-2026-120276
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/429620
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/429620/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-120276