contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

WAVLINK WL-WN579A3-A: new CVE

CVE-2026-120195 · record published 1 November 2026

Analysis Report

If you run a WAVLINK WL-WN579A3-A, find out this week whether its admin pages can be reached from the internet, and ask your supplier for a fixed firmware. If you do not run this model, 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-wn579a3-a-cve-2026-120195

The bottom line

> *If you run a WAVLINK WL-WN579A3-A, find out this week whether its admin pages can be reached from the internet, and ask your supplier for a fixed firmware. If you do not run this model, you can stop reading.*

At a glance

Fact	Detail
Product	WAVLINK WL-WN579A3-A (CVE-2026-120195)
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 running a WAVLINK WL-WN579A3-A on firmware 2026-03-10-94f93d4, and the IT provider who manages it, especially if its web admin pages can be reached from outside.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a WAVLINK WL-WN579A3-A?	Nothing to do for this CVE.	Check the firmware version (next question).
Does the device run firmware 2026-03-10-94f93d4?	The record lists only that version. Ask WAVLINK or your supplier about yours.	You are in the affected range. Check who can reach it.
Can the device's web admin pages be reached from the internet or from untrusted networks?	Exposure is lower, but still plan to apply a fix once one exists.	Restrict access now, then press your supplier for a fix.

What it is

The record says the setup wizard's handling of the wlan_ssid value lets an attacker make the device run operating system commands. It says the attack can be made remotely and that the exploit has been disclosed publicly.

Why it matters

The score is 10 out of 10, and the weakness ids are CWE-78 and CWE-77, both command injection. Our reading is that a device that runs an attacker's commands can be used to watch or redirect the traffic of everything behind it. The record also says the exploit is public, so waiting for a CISA listing 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 CISA does not list it yet. The record itself says the exploit is public and may be used.
- "There is a patch, so we are covered." No source we could read names a fixed version. Do not assume one exists until the vendor says so in writing.
- "Only the setup wizard is affected, and we finished setup long ago." The record does not say the handler is switched off after setup. Treat the device as exposed until the vendor says otherwise.

How we would triage it

This is our judgement.

Step 1: Find the devices and versions you run

- List every WAVLINK WL-WN579A3-A on your sites, including ones installed by others.
- Read the firmware version from the device's admin page and compare it with 2026-03-10-94f93d4, the version the record lists.

Step 2: Reduce exposure

- Make sure the admin pages cannot be reached from the internet, and turn off any remote management setting.
- Allow admin access only from one trusted management address or network.

Step 3: Ask for a fix

- The record says the vendor was contacted early, but no source names a fixed version. Ask WAVLINK or your supplier for one in writing.
- If no fix is offered, consider replacing the device where it faces untrusted networks.

Step 4: Confirm the result

- Once a fix is applied, read the firmware version again and record it.
- Check that the admin pages are still not reachable from outside.

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 our exposure to CVE-2026-120195, a command injection flaw in the WAVLINK WL-WN579A3-A. The record says firmware 2026-03-10-94f93d4 is affected and that the exploit is public. Please tell us whether we run this model, where, and which firmware each unit has. Please confirm whether the admin pages can be reached from the internet. No fixed version is named in what we found, so please ask the vendor for one. Please send written confirmation of the versions and the fix, or of the steps taken to limit exposure, by the date you propose. Thank you.*

The weakness behind it

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

The sources, in their words

The CVE record:

> *A security vulnerability has been detected in WAVLINK WL-WN579A3-A 2026-03-10-94f93d4. The impacted element is the function set_wzdgwMesh of the file /cgi-bin/adm.cgi of the component Initial Setup Wizard. The manipulation of the argument wlan_ssid leads to os command injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure.*

Versions of WAVLINK WL-WN579A3-A the record lists as affected:

- 2026-03-10-94f93d4

What we do not know yet

- Which firmware version, if any, fixes the flaw; no vendor page could be read.
- Whether an attacker needs to log in first; the record does not say.
- Whether the flaw is being used in real attacks; CISA does not list it yet.
- Whether other firmware versions or WAVLINK models are affected.
- 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-2026-120195: 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
Affected firmware, admin pages reachable from the internet	Medium	This week, before anything else

Affected firmware, admin pages reachable only from your internal network	Medium	This week; limit who can reach the admin pages
Affected firmware, admin pages reachable only from a small management network	Low	Next patch cycle, once a fix exists
A different WAVLINK model or firmware version	Low	Ask your supplier whether it is affected
You do not run this device	None	None for this CVE

Appendix 4. Definition of done

- Every WAVLINK WL-WN579A3-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-2026-120195: https://www.cve.org/CVERecord?id=CVE-2026-120195
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/429558
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/429558/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-120195