contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

WAVLINK WN551X3-A: new CVE

CVE-2026-120344 · record published 2 November 2026

Analysis Report

CVE-2026-120344 in WAVLINK WN551X3-A, 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	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-wn551x3-a-cve-2026-120344

The bottom line

> *Check whether you run WAVLINK WN551X3-A. 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	WAVLINK WN551X3-A (CVE-2026-120344)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulDB on 2 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	Owners and IT providers responsible for a WAVLINK WN551X3-A running firmware version M51X3_V251020-WO-182e965, particularly where the device 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 have a WAVLINK WN551X3-A router on your network?	Nothing to do for this CVE.	Check the firmware version (next question).
Is the firmware version M51X3_V251020-WO-182e965?	The record names only this firmware version; monitor for updates.	Restrict access immediately and check whether WireGuard is enabled (next question).
Is the device reachable from outside your local network or by untrusted parties?	Reduce exposure to the local network; still patch when a fix is available.	Treat as high priority; block external access to the management interface now.
Is the WireGuard feature enabled on the device?	Lower risk; the record does not confirm WireGuard must be active; still patch.	Prioritise patching or disabling the WireGuard feature.

What it is

An attacker who can reach the router over the network can inject operating-system commands through the WireGuard CLI Group Handler by manipulating the group_name argument, which can give full control of the device.

Why it matters

The record gives this a CVSS 4.0 score of 10, the maximum possible. The weaknesses are CWE-78 and CWE-77, both forms of command injection, which allow an attacker to run arbitrary operating-system commands as the process owner. The record states the exploit has been disclosed to the public. Our reading is that a maximum-severity, remotely exploitable, publicly disclosed command injection flaw in a network device warrants immediate action even without a CISA listing.

Things people will get wrong

- It is not on CISA's exploited list, so we can wait. The record scores it 10 out of 10 and states the exploit is public. CISA's list records confirmed exploitation; absence from it does not mean the exploit is not in use.
- Only sites actively using WireGuard VPN are at risk. The record names the WireGuard CLI Group Handler as the attack path but does not confirm WireGuard must be active; the firmware version alone is the affected condition named in the record.

How we would triage it

This is our judgement.

Step 1: Find the firmware version on the device

- Log in to the WAVLINK WN551X3-A administration interface and locate the firmware version on the system or status page.
- The affected version the record names is M51X3_V251020-WO-182e965; confirm whether the device matches before taking further action.

Step 2: Restrict access to the management interface

- If the device is internet-facing or reachable by untrusted parties, block external access to the administration and WireGuard interfaces immediately.
- The record states the attack may be performed remotely; reducing who can reach the device reduces exposure while a patch is sought.

Step 3: Check for a firmware update

- No fixed version is named in the public record and no vendor page could be read; check the WAVLINK support site directly for a firmware update for the WN551X3-A.
- Do not apply a firmware version that the vendor has not confirmed addresses this flaw.

Step 4: Review recent device logs for unexpected activity

- Check the device's system logs for unexpected commands, new accounts, or configuration changes made while the device was reachable from untrusted networks.
- The attack leads to OS command injection; look for processes or commands that would not be expected in normal router operation.

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-78 and CWE-77.

The sources, in their words

The CVE record:

> *A vulnerability has been found in WAVLINK WN551X3-A M51X3_V251020-WO-182e965. This affects the function system of the file /bin/ioos of the component WireGuard CLI Group Handler. Such manipulation of the argument group_name leads to os command injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure.*

Versions of WAVLINK WN551X3-A the record lists as affected:

- M51X3_V251020-WO-182e965

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-2026-120344
```

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-2026-120344
```

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

- No fixed firmware version is named in any source; it is not known whether the vendor has issued or plans to issue a patch for this flaw.
- The record does not state whether the attack requires the WireGuard feature to be enabled, or merely that the firmware contains the vulnerable code.
- It is not stated whether authentication is required before the vulnerable function in the WireGuard CLI Group Handler can be reached.
- No vendor advisory or workaround has been published; the analysis rests on the VulDB record alone.
- 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 "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-2026-120344: 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
2 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
WN551X3-A on firmware M51X3_V251020-WO-182e965 reachable from the internet	Medium	Immediately

WN551X3-A on firmware M51X3_V251020-WO-182e965 on an internal network with untrusted users	Medium	Immediately
WN551X3-A on firmware M51X3_V251020-WO-182e965 on a trusted internal network only	Medium	This week
WN551X3-A on firmware M51X3_V251020-WO-182e965 with WireGuard disabled and no remote access	Low	Next patch cycle
WN551X3-A on a different firmware version	None	None for this CVE

Appendix 4. Definition of done

- Every WAVLINK WN551X3-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-2026-120344: https://www.cve.org/CVERecord?id=CVE-2026-120344
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/429669
- Reference in the CVE record: vuldb.com: https://vuldb.com/vuln/429669/cti
- Reference in the CVE record: vuldb.com: https://vuldb.com/cve/CVE-2026-120344