contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Circutor PowerStudio SCADA Wave: new CVE

CVE-2026-120387 · record published 17 November 2026

Analysis Report

If you run PowerStudio SCADA WAVE desktop at 24.8.0 or later but before 24.11.17.0, update to 24.11.17.0 or later this week. Start by finding the installed version. If you do not run this product ...

PREPARED BY	NamiQ	DATE	17 November 2026
FACTS AS OF	17 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/circutor-powerstudio-scada-wave-cve-2026-120387

The bottom line

> *If you run PowerStudio SCADA WAVE desktop at 24.8.0 or later but before 24.11.17.0, update to 24.11.17.0 or later this week. Start by finding the installed version. If you do not run this product, you can stop here.*

At a glance

Fact	Detail
Product	Circutor PowerStudio SCADA Wave (CVE-2026-120387)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by Circutor on 17 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 17 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	24.11.17.0 or later (the vendor's remediation text in the record; no date given)
Who looks first	Anyone running the PowerStudio SCADA WAVE desktop version, and the IT provider or integrator who installed it. The record lists no other Circutor product.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run CIRCUTOR PowerStudio SCADA WAVE, desktop version?	Nothing to do for this CVE.	Check the version (next question).
Is the version 24.8.0 or later but before 24.11.17.0?	Not in the record's range. 24.11.17.0 or later is the fixed release.	You are in range. Go to the next question.
Can anyone untrusted reach the application over a network?	Lower urgency, but still update at the next patch cycle.	Reduce exposure now and update to 24.11.17.0 or later.

What it is

An attacker on the network, with no account, can send a login token that has no signature (algorithm set to “none”). The software accepts it. The attacker then acts as another user and reaches that user's functions.

Why it matters

Our reading is that a forged token skips the login altogether, so strong passwords and lockout rules do not help. The record scores it 10 on CVSS 4.0 and names the weakness as CWE-347. The attacker gets the rights of whichever user they pick, so an administrator account would give the most. The record does not say which functions are exposed.

What the vendor's advisory says

We read two pages on circutor.com and github.com. In short:

- The vendor's cybersecurity page we read is general. It describes a disclosure process and a table of resolved cases, but gives no detail for this CVE.
- A public repository of AI-found flaw disclosures was also among the sources. Its text does not name this CVE, so we do not treat it as evidence about this flaw.

Things people will get wrong

- “It is only a desktop version, so nobody can reach it.” The record describes an unauthenticated remote attacker. It does not say the desktop version is shielded from the network.
- “We have strong passwords, so we are covered.” The flaw accepts a token with no signature, so the attacker never needs a password.
- “Any newer version is fixed.” The record names 24.11.17.0 as the first unaffected release. Check you are at that version or later.

The wording includes conditions the score may not show: needs privileges. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

Step 1: Find the versions you run

- Ask who installed PowerStudio SCADA WAVE and on which machines. The record covers the desktop version.

- Read the installed version and compare it with the range 24.8.0 up to, but not including, 24.11.17.0.

Step 2: Reduce exposure

- Remove any route from the internet to the application until it is updated, because the attack needs no account.
- Allow access only from the machines and people who need it.

Step 3: Update

- Update to 24.11.17.0 or later, as the vendor's remediation text in the record says.
- Do not rely on a changelog or forum post for this flaw; the sources we read name no other fix.

Step 4: Confirm the fix

- Read the version again after the update and keep a record of it.
- Ask your provider for written confirmation of the version on every machine.

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 need to check CVE-2026-120387 in CIRCUTOR PowerStudio SCADA WAVE (desktop version). Please tell us whether we run it, on which machines, and which version. The affected range is 24.8.0 up to, but not including, 24.11.17.0. The fixed version is 24.11.17.0 or later. Please also tell us whether any installation can be reached from the internet. Could you confirm in writing the installed version and that the update is done, by [date]? Thank you.*

The weakness behind it

The record classes this as CWE-347.

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The record describes an unauthenticated remote attacker, so the flaw would likely be reached over a network and used to get into the application.
Use Alternate Authentication Material (T1550): Using a stolen token or hash instead of a password to log in.	Defense Evasion: avoiding detection	A token with no signature is accepted as proof of identity, so a forged token would likely stand in for real credentials.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

The CVE record:

> *An improper JWT signature verification vulnerability in CIRCUTOR PowerStudio SCADA WAVE desktop version allows an unauthenticated remote attacker to bypass authentication by submitting an unsigned JWT with the algorithm set to “none”. The shared JWT validation component accepts the token without verifying a cryptographic signature, allowing the attacker to impersonate another user and access protected functionality with that user's privileges.*

Versions of Circutor PowerStudio SCADA Wave the record lists as affected:

- 24.8.0 up to, but not including, 24.11.17.0

It lists these as unaffected:

- 24.11.17.0

What the record says to do about it, in the vendor's words:

> *Update CIRCUTOR PowerStudio SCADA WAVE to version v24.11.17.0 or later.*

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-2026-120387
```

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 hardware (maker, model, firmware), the running container images with their operating system and packages, 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-2026-120387
```

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. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages 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 this flaw is being used in attacks. The record is new and CISA did not list it when we read it.

- Which functions an impersonated user can reach, and whether an administrator can be impersonated.
- How the desktop version is exposed to a network, and on which port.
- Whether the vendor has published a separate advisory for this CVE. The page we read gives no detail.
- 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 17 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- 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", "Likely ATT&CK mapping", "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-2026-120387: 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` 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
17 November 2026	CVE record published by Circutor.

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
An affected version that can be reached from the internet	High	Immediately; restrict access, then update

An affected version reachable only from an internal network	Medium	This week
Version 24.11.17.0 or later	None	None for this CVE
A version below 24.8.0	Low	Ask the vendor; the record does not list it
The product is not run at all	None	None for this CVE

Appendix 4. Definition of done

- Every Circutor PowerStudio SCADA Wave 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-2026-120387: https://www.cve.org/CVERecord?id=CVE-2026-120387
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: circutor.com/soporte/ciberseguridad/: https://circutor.com/soporte/ciberseguridad/
- Advisory or release notes read: github.com/Exploit-Garbage/0day-Rubbish: https://github.com/Exploit-Garbage/0day-Rubbish?utm_source=chatgpt.com
- Reference in the CVE record: 0day-rubbish.com: https://0day-rubbish.com/blog/circutor-powerstudio-jwt-alg-none-identity-forgery?utm_source=chatgpt.com