contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

ASUS Control Center Express: new CVE

CVE-2026-114202 · record published 18 November 2026

Analysis Report

If you run ASUS Control Center Express, your IT contact should find the installed version this week and ask ASUS for the fixed release. If you do not run it, you can stop reading.

PREPARED BY	NamiQ	DATE	18 November 2026
FACTS AS OF	18 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/asus-control-center-express-cve-2026-114202

The bottom line

> *If you run ASUS Control Center Express, your IT contact should find the installed version this week and ask ASUS for the fixed release. If you do not run it, you can stop reading.*

At a glance

Fact	Detail
Product	ASUS Control Center Express (CVE-2026-114202)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by ASUS on 18 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 18 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 ASUS Control Center Express, usually an IT provider managing a fleet of ASUS devices. The record's wording points to the product's agent component.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run ASUS Control Center Express?	Nothing to do for this CVE.	Find the installed version (next question).
Is the version inside the affected range in the record?	Keep a written note of the version and check again when ASUS updates its advisory.	Treat it as exposed and see the next question.
Can anyone untrusted reach the Control Center Express service over a network?	Lower urgency, but still ask ASUS for the fix.	Restrict network access now, then patch.

What it is

The record says the product uses a hard-coded cryptographic key. A remote user can use it to forge an authentication token and gain administrative privileges, without needing a valid login.

Why it matters

Our reading is that a forged token is useful to an attacker as a way past the login. The record gives a score of 10 and says a remote user can gain administrative rights. A management console with admin rights is normally a strong foothold, because it can reach many machines. The CVE is new and the record does not say it is exploited, so the score and the admin access are the reasons to act.

What the vendor's advisory says

We read one page on www.asus.com. In short:

- The record points to a section titled 'Security Update for ASUS Control Center Express Agent' on the ASUS Security Advisory page.
- The advisory text we hold is the page's general introduction. It names no fixed version, workaround or other flaw.

Things people will get wrong

- It is not on the CISA list, so it is not a problem The record is new. The listing only says CISA had not listed it when read. It does not say nobody is exploiting it.
- A fix is available, so we only need to update No source we hold names a fixed version. Confirm the release with ASUS before you call it fixed.

How we would triage it

This is our judgement.

Step 1: Find the versions you run

- List every machine with Control Center Express and note the version, because the record's affected range is stated by version.

Step 2: Reduce exposure

- Block access to the service from the internet and from networks that do not need it, because the flaw is reachable remotely.

Step 3: Get the fix in writing

- Ask ASUS or your provider which release fixes this CVE, since no source we hold names one.
- Apply it once confirmed.

Step 4: Check afterwards

- Record the new version on each machine and review admin accounts for any you do not recognise.

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, ASUS published CVE-2026-114202 on 18 November 2026. It affects ASUS Control Center Express and lets a remote user gain administrative privileges with a forged token. Please tell us whether we run this product, where, and which version. Please also tell us which ASUS release fixes it, as the sources we hold do not name one. Until then, please restrict network access to it. We would like written confirmation of the versions and the fix by the end of this week.*

The weakness behind it

The record classes this as CWE-321.

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 says a remote user can reach the flaw, so it would likely be used against an exposed service as a way in.
Use Alternate Authentication Material (T1550): Using a stolen token or hash instead of a password to log in.	Defense Evasion: avoiding detection	A forged authentication token is likely to be accepted in place of a real login, which fits using alternate authentication material.

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:

> *Use of Hard-coded Cryptographic Key in ASUS Control Center Express allows a remote user to gain administrative privileges via a forged authentication token. Refer to the ' Security Update for ASUS Control Center Express Agent ' section on the ASUS Security Advisory for more information.*

Versions of ASUS Control Center Express the record lists as affected:

- through v1.7.27

The record gives no version ranges. Use the vendor's advisory for the affected versions.

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-2026-114202
```

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-2026-114202
```

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

- Which release fixes this flaw. The advisory text we hold does not name one.
- Whether any workaround exists short of patching.
- Whether the service is reachable by default or only in some setups.
- Whether attackers are using it. The record is new and not on CISA's list.
- 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 18 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-2026-114202: 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
18 November 2026	CVE record published by ASUS.

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
Control Center Express on an affected version, reachable from the internet	Medium	Now: restrict access first, then patch

Affected version, reachable only from an internal network	Medium	This week
Affected version, access limited to a few admin machines	Medium	Within the next patch cycle
Product not installed anywhere in your estate	None	None for this CVE

Appendix 4. Definition of done

- Every ASUS Control Center Express 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-2026-114202: https://www.cve.org/CVERecord?id=CVE-2026-114202
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: www.asus.com/security-advisory: https://www.asus.com/security-advisory