contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

VeloCloud Orchestrator

CVE-2026-114625 · on-premises VCO, three release trains

Assessment & Action Plan

A SQL injection in the on-premises VeloCloud Orchestrator lets any logged-in user, down to the read-only role, take operator privileges. CISA listed it on 23 October. Which releases fix it, who holds the accounts you should worry about, and what to look for on the host.

PREPARED BY	Hung Le, NamiQ	DATE	2 November 2026
FACTS AS OF	29 October 2026	VERSION	1.1
SEVERITY	**Critical: CVSS 3.1 9.9**	STATUS	Fixed in 5.2.3.18, 6.1.3.10, 6.4.2.12; exploited in the wild

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/arista-velocloud-orchestrator-cve-2026-114625

Update, 2 November 2026: this note now ends with a section on checking your own servers and projects with lattice-scan, for IT admins, AI agent skills and CI/CD, and the analysis report is reissued with it. Everything else is as of 29 October 2026; check CISA's catalog for any change since.

Most flaws that need a login are ranked below the ones that do not. This one is worth reading closely because the login it needs is the weakest one the product has. Arista's record says the minimum role that can use it is Enterprise Read Only, the lowest built-in tenant role. CISA lists it as exploited, and the deadline it set was 26 October.

This note is for you if you run an on-premises VeloCloud Orchestrator, or manage one for others. Everything is as of 29 October 2026, and every claim links to its source at the end.

The short version

- CVE-2026-114625 (CWE-89, SQL injection): an on-premises VeloCloud Orchestrator may allow a remote attacker to reach privileged internal functionality and affect the VCO host. CVSS 3.1 9.9; CVSS 4.0 9.4.
- On an affected system any authenticated user can gain operator privileges and act as a local superuser operator, including functions intended for internal use only. The minimum role needed is Enterprise Read Only.
- The record says the product is exposed by default, requires network access to the web interface and a valid authenticated session, and that no configuration prevents it.
- Fixed in VCO 5.2.3.18 and later in the 5.2 train, 6.1.3.10 and later in 6.1, and 6.4.2.12 and later in 6.4. Hosted, including dedicated, versions were affected and have already been patched.
- CISA lists it as exploited since 23 October. Ransomware use is recorded as Unknown, which means not recorded.

What the bug is

The weakness class is SQL injection: input that reaches a database query without being neutralised. The record describes the result rather than the request: a logged-in user's request can reach functionality that is not meant to be reachable remotely, and the user ends up as a superuser operator. We have not seen the request, and the vendor has not published one that we found. We do not describe the mechanism further than the record does.

Why the account list is the exposure

A flaw that needs a login is usually a flaw for insiders. Here the lowest role is enough, and an orchestrator is the kind of product that has many accounts: your staff, the customers or tenants you serve, partners, contractors, and the accounts people created for a project and forgot. Each is a way in.

The useful question is not whether your administrators are trustworthy. It is how many people and systems can sign in at all, and whether you could say today who they are.

Things people will get wrong

- "It needs a login." It needs the lowest login the product has. Count the accounts before you decide that is a barrier.
- "EPSS is 0.01, so it is unlikely." EPSS is a modelled probability. CISA lists it because exploitation has been seen. A low model figure and an exploited list entry can both be true.
- "We turned something off." The record says no configuration prevents the exposure. A restriction on who can reach the interface reduces who can try. It is not a fix.
- "Arista patched it." For the hosted and dedicated service, yes. For software you run yourself, you patch it.
- "Our tenant users only have read access." Read-only is exactly the role the record names.

How we would triage it

This is our judgement, built on the record.

- Find every on-premises VCO first. A hosted orchestrator is the vendor's job and is already done.
- Cut who can reach the web interface before you schedule the upgrade. That is quick, it is the vendor's own first workaround, and it shrinks the people who can try.
- Upgrade to a fixed release in your train. Then review the accounts and the host as if someone had been there, because the listing says someone has been somewhere.

Step 1: find the version

In the orchestrator's administration interface the software version is shown on its about or system page. Compare it with the three trains:

```
5.2 train:  fixed in 5.2.3.18 and later
6.1 train:  fixed in 6.1.3.10 and later
6.4 train:  fixed in 6.4.2.12 and later
```

A version below your train's number is affected. We do not know of earlier trains beyond these three, so if you run another, ask Arista.

Step 2: reduce reach, then upgrade

- Restrict the web interface to trusted administrative networks. The vendor lists this first.
- Upgrade to the fixed release in your train. The vendor's guidance is to do so at your earliest convenience; CISA's date has already passed.
- If you cannot upgrade this week, keep the restriction in place and add the monitoring below.

Step 3: review the accounts

- Export the list of portal accounts with their roles and last sign-in.
- Remove accounts nobody can account for, and any that have not signed in for a long time.
- For accounts you keep, make sure the password is not reused and sign-in is as strong as the product allows.
- Review recent administrator and operator activity for changes nobody made.

What to look for on the host

The vendor's workaround section names these. They are checks for compromise, not a fix:

- Accesses to the orchestrator from known malicious source addresses. Your threat feed supplies the list; we do not publish one.
- Unexpected outbound network activity from the orchestrator host. A management system rarely needs to start connections to the internet.
- Backdoor daemons and web shells: processes or script files that are not part of the product.
- Outbound ports the host does not need for normal activity. Consider blocking them.

```
# Established connections the host has opened outward (Linux)
ss -tnp state established

# Listening services, to compare with what the product should run
ss -tlnp
```

We do not know the product's directory layout, so we do not give a find command for it. Ask Arista where the product's script and web files live, and compare them with a clean copy.

What CISA now asks for

CISA's required action is to apply the vendor's mitigations under its binding directive BOD 26-04, to follow its forensics triage requirements, and to discontinue use of the product if mitigations are not available. The directive covers federal agencies. Its logic does not stop there: for a flaw already used on real systems, the question includes whether you were reached before you patched.

Check your own servers and projects

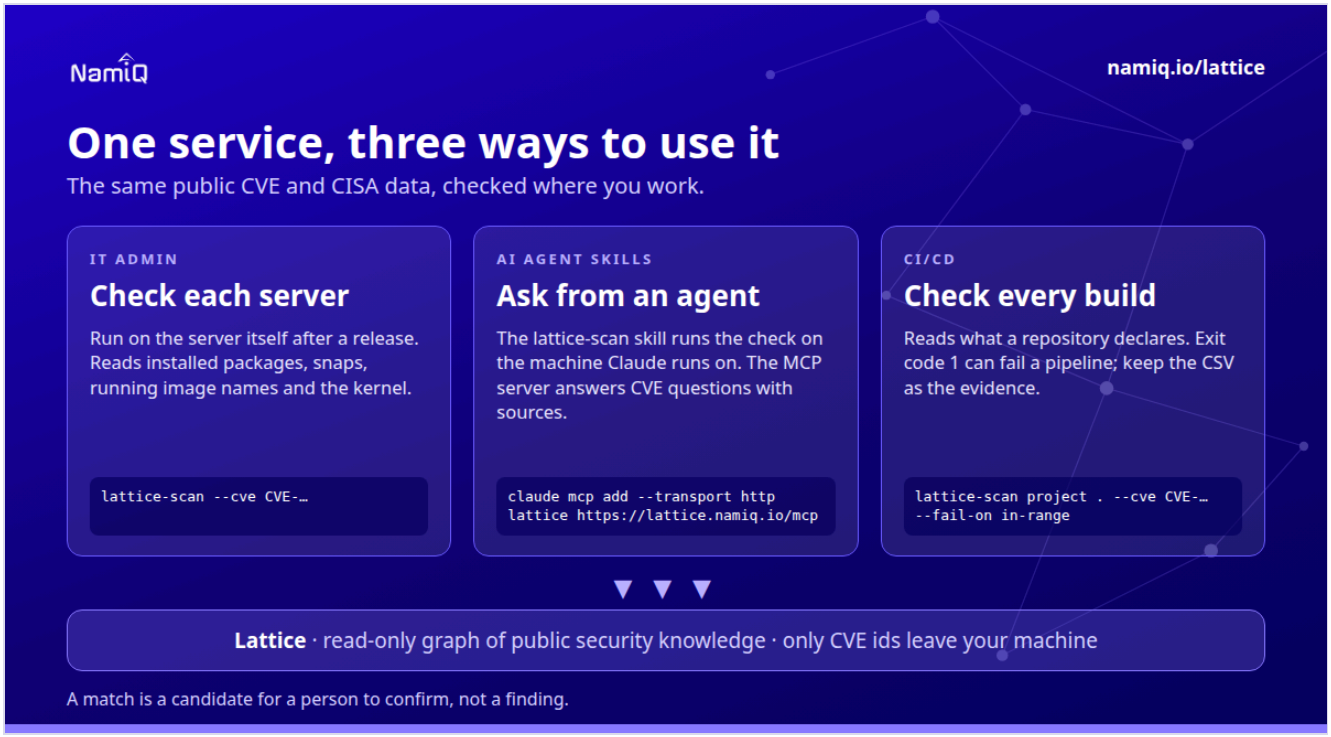
The facts above are as of 29 October 2026. lattice-scan, the open-source command line for checking this CVE against your own estate, cannot check this product: VeloCloud Orchestrator is a network

management appliance with its own operating system, which neither check reads. A match from it would also never be a finding, only a candidate for a person to confirm.

What you can do instead: ask an AI agent connected to the Lattice MCP server to look up CVE-2026-114625. The keyless graph_lookup returns CISA's entry (listed, due date, required action) and the NVD entry (affected products and version ranges), each with its source. Then check the vendor's own advisory for your version. If you run Linux servers or build software around it, the command line still covers those parts.

Who can use it, and how

For	What to do	Command
AI agent skills	The lattice-scan skill runs the check on the machine Claude runs on. The Lattice MCP server answers questions about the CVE with its sources.	claude mcp add --transport http lattice https://lattice.namiq.io/mcp



Where the same check is used. The three ways read the same public data; only CVE ids leave your machine.

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

- How the request is made. The vendor and the record do not give it.
- Who is using it, against whom, or how many orchestrators were reached.
- Whether earlier release trains than the three listed are affected.

- Why the score is high while the modelled probability is low. We have not tested the product.

If you take one thing from this: when a flaw needs only the lowest login, your list of logins is your exposure. Know who is on it.

Appendix 1. Severity decoded

CVE-2026-114625, CVSS 3.1: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H` Privileges Required is Low: any account on the portal is enough, down to the lowest tenant role.

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.
Privileges required	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

CVE-2026-114625, CVSS 4.0: score 9.4, `CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H` Subsequent-system impact is High on all three, which is why the score stays near the top.

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	Low	An ordinary account is enough.
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
22 October 2026	The CVE record is published by Arista, with the fixed releases and workarounds.
23 October 2026	CISA adds it to the Known Exploited Vulnerabilities catalog, due 26 October. CISA's exploitation decision is Active, automatable No, technical impact Total.
26 October 2026	The CISA due date passes.
29 October 2026	EPSS is 0.01 (percentile 0.64): a high score with a low modelled probability, on the exploited list regardless.

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
On-premises VCO, web interface reachable from the internet, any customer or partner accounts	Critical	Upgrade or restrict today
On-premises VCO, reachable only from an administrator network, with accounts for a few staff	High	Upgrade this week; review accounts now
On-premises VCO with many read-only accounts for customers, partners or contractors	Critical	The account list is the exposure: upgrade today
Hosted or dedicated VCO run by Arista	Already patched by the vendor	Confirm with your account team

Appendix 4. Definition of done

- Every on-premises VCO is listed with its release train and version.
- Each is on 5.2.3.18, 6.1.3.10 or 6.4.2.12 or later.
- The web interface is reachable only from administrator networks, or the exposure is documented.
- Every account on the portal has been reviewed, including read-only ones, and unused ones removed.
- The host was checked for unexpected outbound connections, web shells and backdoor daemons, and recent administrator changes were reviewed.

Sources

- CVE-2026-114625 record (Arista CNA): description, CWE-89, scores, workarounds, fixed releases, configuration note: https://www.cve.org/CVERecord?id=CVE-2026-114625
- Arista security advisory 0199: https://www.arista.com/en/support/advisories-notices/security-advisory/24838-security-advisory-0199
- CISA Known Exploited Vulnerabilities catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-114625
- FIRST EPSS, CVE-2026-114625: https://api.first.org/data/v1/epss?cve=CVE-2026-114625