contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Jet Admin Cloud Platform: new CVE

CVE-2026-123965 · record published 13 November 2026

Analysis Report

Anyone running Jet Admin Cloud Platform must act now: the record scores this 9.9 CRITICAL and states no fixed version exists. Contact Jet Admin to confirm the sandbox mitigation of around 29 October …

PREPARED BY	NamiQ	DATE	13 November 2026
FACTS AS OF	13 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.9**	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/jet-admin-cloud-platform-cve-2026-123965

The bottom line

> *Anyone running Jet Admin Cloud Platform must act now: the record scores this 9.9 CRITICAL and states no fixed version exists. Contact Jet Admin to confirm the sandbox mitigation of around 29 October 2026 covers your deployment, and rotate any credentials stored in .env files immediately.*

At a glance

Fact	Detail
Product	Jet Admin Cloud Platform (CVE-2026-123965)
Severity	Critical: 9.9 (CVSS 3.1)
Status	A new CVE record, published by Cisa-cg on 13 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 13 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No fixed version is named in the record; remediation status is 'none available'. A source states mitigation via a sandbox component around 29 October 2026, but no release number is given.
Who looks first	Anyone who runs Jet Admin Cloud Platform in any version — the record lists all versions as affected. Teams whose deployment connects to external systems via credentials stored in .env files face the most direct risk.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Jet Admin Cloud Platform — cloud, self-hosted, or on-premise?	Nothing to do for this CVE.	Treat all versions as affected and move to the next question.
Does your Jet Admin deployment use .env files that hold connection credentials?	Credential theft risk is lower; still verify the sandbox mitigation is in place.	Treat those credentials as potentially exposed; begin rotation.
Can external or untrusted users register free accounts on your Jet Admin instance?	Exposure is reduced but the platform remains without a confirmed fix.	Risk is elevated; rotate credentials and restrict new account creation now.

What it is

A prompt injection flaw lets a remote attacker holding a free account craft input that exposes the application's .env configuration files and exfiltrates the credentials stored in them.

Why it matters

The 9.9 CRITICAL score reflects network reachability, low complexity, no meaningful prior access beyond a free account, and changed scope — a successful exploit can reach resources beyond Jet Admin itself. The practical danger is credential theft: whoever obtains .env credentials can connect directly to the underlying data sources. Our reading is that any internet-facing deployment warrants immediate credential rotation, because the sandbox mitigation is dated approximately 29 October 2026 with no version number, making it impossible to confirm a patched state from the version alone.

Things people will get wrong

- The sandbox fix around 29 October 2026 means the platform is now patched. The record's remediation status is 'none available'. The sandbox mitigation is noted in a source but no fixed version is named and the record lists no unaffected release.
- Only attackers with no account at all can trigger this. The description requires a free account, which may be open to anyone who registers. The CVSS vector scores PR:N (no prior privileges), which the record does not explain.

How we would triage it

This is our judgement.

Step 1: Find whether you run Jet Admin Cloud Platform

- Check your IT asset inventory or ask your IT provider whether Jet Admin Cloud Platform is deployed in cloud, self-hosted, or on-premise form.
- Note whether it is reachable from outside your network, as the CVSS vector scores network access with no prior credentials required.

Step 2: Identify credentials in .env files connected to Jet Admin

- Locate the .env files your Jet Admin deployment uses and list each credential and the system it connects to.
- These are the credentials the record says a successful exploit can exfiltrate.

Step 3: Rotate any credentials in .env files

- For each credential found, generate a new value in the target system and update the .env file.
- Check whether the same credentials are reused in other systems and rotate those too.

Step 4: Confirm mitigation status with Jet Admin

- Contact Jet Admin support and ask whether the sandbox mitigation applied around 29 October 2026 covers your deployment type.
- Request written confirmation and ask whether a versioned fix is planned, since the record currently shows no fixed version.

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.

> *We use Jet Admin Cloud Platform and have learned of CVE-2026-123965, a prompt injection flaw scored 9.9 CRITICAL. It allows a remote attacker with a free account to expose .env configuration files and steal credentials. The record states no fixed version is available; a source notes a sandbox mitigation around 29 October 2026 but gives no version number. Please confirm whether Jet Admin Cloud Platform is deployed in our environment, which version is running, and whether the sandbox mitigation has been applied to our deployment. Please also identify which credentials are held in .env files so we can consider rotation. We ask for written confirmation of the deployment and mitigation status by 20 November 2026.*

The weakness behind it

The record classes this as CWE-200.

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	Exploitable over the network against a web platform; CWE-200 and the description both point to unauthorised information disclosure from an internet-accessible application, which would typically map here.
Unsecured Credentials: Credentials In Files (T1552.001): Finding passwords or keys left in files.	Credential Access: stealing logins	The stated outcome is exfiltration of credentials from .env configuration files; this would typically involve reading credential material stored on the filesystem, matching credentials-in-files.
Data from Local System (T1005): Copying data stored on the machine.	Collection: gathering data	The description explicitly names .env configuration files as the target; reading those files from the server is consistent with collecting data from the local system.

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:

> *A prompt injection vulnerability in all versions of Jet Admin Cloud Platform allows a remote attacker with a free account to expose sensitive .env configuration files and exfiltrate critical credentials. Mitigated via sandbox component around October 29, 2026.*

Versions of Jet Admin Cloud Platform the record lists as affected:

- all versions before *

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-2026-123965
```

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-2026-123965
```

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

- The record does not state which version introduced the sandbox mitigation, making it impossible to confirm a fixed state from a version number alone.
- The record does not say whether the free-account requirement applies to the cloud service only or also to self-hosted and on-premise instances.
- The record does not describe which specific types of credentials or .env variables are reachable through the injection path.
- The CVSS vector scores PR:N (no privileges required) but the description states a free account is needed; the record does not explain this difference.
- 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 13 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-2026-123965: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L` 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.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	Low	Some data or behaviour can be altered.
Availability	Low	Reduced performance or interruptions.

Appendix 2. Timeline

Date	Event
13 November 2026	CVE record published by Cisa-cg.

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
Jet Admin Cloud Platform reachable from the internet, any version	Medium	Immediately; rotate credentials and verify mitigation
Internal deployment where any user can register a free account	Medium	This week; restrict account creation and verify mitigation
Internal deployment with controlled account creation, no confirmed mitigation	Medium	This patch cycle; confirm sandbox mitigation with the vendor
Deployment confirmed by vendor to have sandbox mitigation in place	Low	Next patch cycle; monitor for a versioned fix

Appendix 4. Definition of done

- Every Jet Admin Cloud Platform 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-2026-123965: https://www.cve.org/CVERecord?id=CVE-2026-123965
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: www.jetadmin.io/changelog: https://www.jetadmin.io/changelog
- Advisory or release notes read: www.jetadmin.io: https://www.jetadmin.io/
- Advisory or release notes read: raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2026/v: https://raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2026/va-26-317-01.json
- Reference in the CVE record: www.cve.org: https://www.cve.org/CVERecord?id=CVE-2026-123965