contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Arize-ai phoenix: new CVE

CVE-2026-53998 · record published 16 November 2026

Analysis Report

If you run Phoenix from 13.0.0 up to but not including 15.7.0, update to 15.7.0 this week. If you do not run Phoenix, stop reading. First find the version and whether anyone untrusted can reach the …

PREPARED BY	NamiQ	DATE	16 November 2026
FACTS AS OF	16 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 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/arize-ai-phoenix-cve-2026-53998

The bottom line

> *If you run Phoenix from 13.0.0 up to but not including 15.7.0, update to 15.7.0 this week. If you do not run Phoenix, stop reading. First find the version and whether anyone untrusted can reach the service.*

At a glance

Fact	Detail
Product	Arize-ai phoenix (CVE-2026-53998)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by GitHub on 16 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 16 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	15.7.0. The record says it is fixed there. The release notes dated 13 May 2026 list 'prevent format-string injection in f-string template formatter'.
Who looks first	Anyone running Arize Phoenix from 13.0.0 up to but not including 15.7.0. Default installs without authentication come first. With authentication on, any account can still reach the endpoint.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Arize Phoenix, the AI observability and evaluation platform?	Nothing to do for this CVE.	Check the version (next question).
Is the version 13.0.0 or later but below 15.7.0?	Outside the range the record lists. Nothing to do for this CVE.	Plan the update to 15.7.0.
Can anyone beyond trusted staff reach Phoenix over the network?	Lower risk, but still update: with authentication on, any account can reach it.	Update first. Restrict access until then.
Does Phoenix run with authentication off, as default installs do?	An attacker would need an account, but any account is enough.	Treat as open to anyone who can reach it. Update now.

What it is

An attacker sends a crafted template to the applyChatTemplate query and can read the server's environment variables and internal module state. The record says the endpoint needs no login on default installations.

Why it matters

Our reading: the record names PHOENIX_SECRET as the prize. It says exposure can allow forged administrative session tokens and decryption of credentials protected by keys derived from that secret. So a read-only bug could become admin control and stolen stored credentials. The score of 10 reflects no login, network reach and a changed scope. Other environment variables may hold secrets too.

What the vendor's advisory says

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

- The 15.7.0 release notes are dated 13 May 2026. The CVE record was published on 16 November 2026.
- The release note entry is 'prevent format-string injection in f-string template formatter'. It does not name this CVE. The record itself says the issue is fixed in 15.7.0.
- The release notes list other changes (feature work and two other bug fixes). They give no other security fixes and no workaround.
- The advisory lists two weaknesses: use of an externally controlled format string (CWE-134) and exposure of sensitive information (CWE-200).

Things people will get wrong

- "We turned authentication on, so we are safe." The record says any account can reach the endpoint when authentication is enabled. It only removes anonymous callers.
- "It only reads data, so it cannot do real harm." The record says exposed PHOENIX_SECRET can allow forged administrative session tokens and decryption of credentials protected by keys derived from it.
- "Nothing is listed as exploited, so we can wait." The record is new and CISA does not list it. That says nothing about whether others exploit it. The record scores it 10 and needs no login on default installs.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find the versions you run

- Check every place Phoenix runs, including test machines and containers. The affected range is 13.0.0 up to but not including 15.7.0.
- Ask your team whether anyone runs it that IT does not know about.

```
pip show arize-phoenix
pip list | grep -i phoenix
docker images | grep -i phoenix
```

Step 2: Reduce exposure

- Until patched, limit network access to Phoenix to the people who need it. The record says it is reachable without login on default installs.
- Check whether authentication is on; it limits callers to account holders but does not close the flaw.

Step 3: Update to 15.7.0

- Move to 15.7.0, the version the record names as the fix.
- Consider replacing PHOENIX_SECRET and any credentials the service holds, if it was reachable by anyone untrusted. That is our reading, not the record's.

Step 4: Check the result

- Confirm the running version is 15.7.0 or later, not just that the package was updated.
- Ask for the version in writing from whoever runs it.

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 whether we run Arize Phoenix, and where. CVE-2026-53998 affects versions from 13.0.0 up to but not including 15.7.0. An unauthenticated caller can read environment variables, including PHOENIX_SECRET. Please tell us which Phoenix instances we have, their versions, and who can reach them. If any is affected, please update to 15.7.0 and confirm the version and the fix in writing by the end of this week. Please also tell us whether the secret should be replaced. Thank you.*

The weakness behind it

The record classes this as CWE-134 and 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	The record describes an unauthenticated network endpoint on default installs. Such a flaw would likely be reached by sending a crafted request to a public-facing application.
Use Alternate Authentication Material (T1550): Using a stolen token or hash instead of a password to log in.	Defense Evasion: avoiding detection	The record says a leaked PHOENIX_SECRET can allow forged administrative session tokens. That would likely let an attacker act as an admin using forged material instead of a password.

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:

> *Phoenix is an AI observability and evaluation platform. From 13.0.0 until 15.7.0, the applyChatTemplate GraphQL query passed attacker-controlled F-string templates to FStringTemplateFormatter._format, while DotDict.__getattr__ did not prevent traversal through Python private attributes. A crafted field could traverse object internals such as __class__, __init__, and __globals__ to read process environment variables and internal module state. The endpoint is unauthenticated on default installations, and any account can reach it when authentication is enabled. Exposure of PHOENIX_SECRET can allow administrative session-token forgery and decryption of credentials protected by keys derived from ...*

Versions of Arize-ai phoenix the record lists as affected:

- >= 13.0.0, < 15.7.0

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-2026-53998
```

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-2026-53998
```

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 anyone has exploited this flaw; the record does not say, and CISA does not list it.
- Whether the release fixes other flaws; the notes name no other security fix.
- Why the record was published months after the 15.7.0 release; the sources do not say.
- Whether secrets other than PHOENIX_SECRET are at risk; the record names only environment variables and module state.
- 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 16 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-2026-53998: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/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	High	Total loss of integrity.
Availability	Low	Reduced performance or interruptions.

Appendix 2. Timeline

Date	Event
16 November 2026	CVE record published by GitHub.

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
Phoenix on an affected version, no authentication, reachable from the internet	High	Now; no login is needed over a network
Affected version with authentication on, reachable by many users	High	This week; any account can reach it
Affected version, reachable only from a small trusted network	Medium	This week or next patch cycle
Phoenix at 15.7.0 or later	None	None for this CVE
Phoenix below 13.0.0	None	None; the record lists no such version

Appendix 4. Definition of done

- Every Arize-ai phoenix 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-2026-53998: https://www.cve.org/CVERecord?id=CVE-2026-53998
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/Arize-ai/phoenix/security/advisories/GHSA-gfv3-: https://github.com/Arize-ai/phoenix/security/advisories/GHSA-gfv3-m769-5xm3
- Advisory or release notes read: github.com/Arize-ai/phoenix/releases/tag/arize-phoenix-v15: https://github.com/Arize-ai/phoenix/releases/tag/arize-phoenix-v15.7.0
- Reference in the CVE record: github.com: https://github.com/Arize-ai/phoenix/pull/13197
- Reference in the CVE record: github.com: https://github.com/Arize-ai/phoenix/commit/e7224a685589f2ffae1fefcc68ff210bd6ad28b8