contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Kafka admin API, no auth

CVE-2026-115644 · Apache Kafka Connect

Assessment & Action Plan

If you gave Kafka Connect's admin API its own listener, the authentication you configured for the main API does not apply to it. What an attacker can do with that, which versions fix it, and the one-line mitigation.

PREPARED BY	Hung Le, NamiQ	DATE	2 November 2026
FACTS AS OF	28 October 2026	VERSION	1.1
SEVERITY	**Not yet scored (Apache CNA)**	STATUS	Fixed in Kafka 4.2.2, 4.3.2 and 4.4.0

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/apache-kafka-connect-cve-2026-115644

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 28 October 2026; check CISA's catalog for any change since.

The most useful advice in security is to expose less. This bug punishes someone for following it. Kafka Connect lets you serve its admin REST API on its own listener so that it can be kept apart from the main API. Do that, and the authentication you set up for the main API is not applied to the admin one. The thing you did to protect it left it with no login.

This note is for you if you run Kafka Connect. Everything is as of 28 October 2026 and every claim links to its source at the end. Apache has not given the CVE a severity score, and we do not invent one.

The short version

- CVE-2026-115644 is an authentication bypass in the Kafka Connect admin REST API. It applies when admin.listeners is configured with a separate listener from the main listeners property.
- In that setup, REST extensions named in rest.extension.classes, for example BasicAuthSecurityRestExtension, are not registered or applied to the admin resources. The /admin/loggers endpoint accepts unauthenticated read and write requests even though security extensions are active on the main listener.
- Affected: Apache Kafka from 2.4.0 up to but not including 4.2.2, and from 4.3.0 up to but not including 4.3.2. Fixed in 4.2.2, 4.3.2 and 4.4.0.
- Mitigation if you cannot upgrade: remove the admin.listeners setting, or leave it unset. The admin resources then share the regular listener and inherit its extensions.
- Credit: Bartłomiej Dmitruk of Striga, and Mickael Maison.

What an attacker can do

The admin endpoint in question manages log levels. An attacker with network access to the admin listener can:

- Read the complete list of logger names and levels, which discloses the names of loaded classes and shows which security extensions are in use.
- Change logger levels, including with cluster scope, which propagates the change to every worker in the Connect cluster.

The record says this can be used to suppress logging, by setting the root level to OFF, or to generate excessive output, by setting it to TRACE. The impact it names is on availability and observability. It does not name data access or code execution, and we are not going to.

Why it matters more than "just logging"

Two things make it worth acting on. First, the first thing the read gives an attacker is information: loaded classes, and which security extensions are in play. That is reconnaissance for the next step.

Second, the write lets an attacker turn off your logs across the whole cluster with one request, and Connect workers are often where data moves between systems. A cluster that has stopped logging is a cluster whose later problems you cannot reconstruct. It is the same shape of problem as a logging gap on a hypervisor: the damage is to your ability to find out what happened.

Who is exposed

Only deployments that set admin.listeners. If you never set it, the admin resources share the main listener and inherit its security, and this bug does not apply. If you did set it, your exposure is the set of hosts that can reach the admin port. A common reason to set it is to isolate the admin interface on a separate network or port. If that isolation is real, the exposure is small. If the port is reachable from wherever the main API is, it is not.

Things people will get wrong

- "We have authentication on Connect." On the main listener. The admin listener, if separate, did not inherit it.
- "It is only log levels." Cluster-wide, unauthenticated, and one of the effects is that your logs stop.
- "We use Kafka, so we are affected." Only Kafka Connect, and only if admin.listeners is set.

How we would triage it

This is our judgement. The facts are from the CVE record.

- Check the setting first. It takes a minute per worker and the answer decides everything.
- If it is set, the quick fix is to remove it, with the effect that the admin API moves back to the main listener and its authentication. Decide whether that is acceptable, then upgrade and consider restoring the separation.
- Whatever the answer, confirm the admin port is not reachable from places it does not need to be.

Step 1: is admin.listeners set

```
# In each Connect worker's configuration
grep -rn 'admin.listeners' /etc/kafka /opt/kafka/config 2>/dev/null

# Which Kafka version does the worker run
kafka-topics.sh --version 2>/dev/null || ls /opt/kafka/libs | grep -E '^kafka_.*\.jar'
```

Also check how your container or orchestration platform passes configuration, because the setting may come from environment variables or a manifest, not a file.

Step 2: test it from a place you should not be able to reach it from

```
# From a host that should NOT be able to use the admin API
curl -s -m 5 http://CONNECT-HOST:ADMIN-PORT/admin/loggers | head -c 300
```

If you get logger names back without presenting credentials, the endpoint is open to that host. Run this only against systems you operate.

Step 3: upgrade or mitigate

- Upgrade to Kafka 4.2.2, 4.3.2 or 4.4.0 or later in your line. From those releases the REST extensions apply to admin.listeners too.
- If you cannot upgrade, remove the admin.listeners setting and restart the workers.
- Restrict the admin port with a network rule so that only operations hosts can reach it.

Step 4: look backwards

- Look for changes to logger levels, particularly cluster-scoped, that no one on your team made, and for gaps in Connect logs.
- Review network logs for connections to the admin port from unexpected hosts.
- If you find a gap or a change you cannot explain, treat it as a sign someone looked around, and review what the connectors can reach.

Check your own servers and projects

The facts above are as of 28 October 2026. To compare your own estate with this CVE, the open-source lattice-scan command line checks the parts it can see. Naming the CVEs needs no key, only the CVE ids leave your machine, and a match is a candidate for a person to confirm, not a finding.

On a server: run it on the server itself, not on the laptop or CI runner that deploys to it. It reads installed packages (dpkg, rpm or apk), snaps, the names of running container images and the kernel

version, compares them on the machine, and keeps the inventory there. A distribution can fix a CVE under an unchanged version number, so on Debian-family hosts read the changelog line the report shows.

```
lattice-scan --cve CVE-2026-115644
```

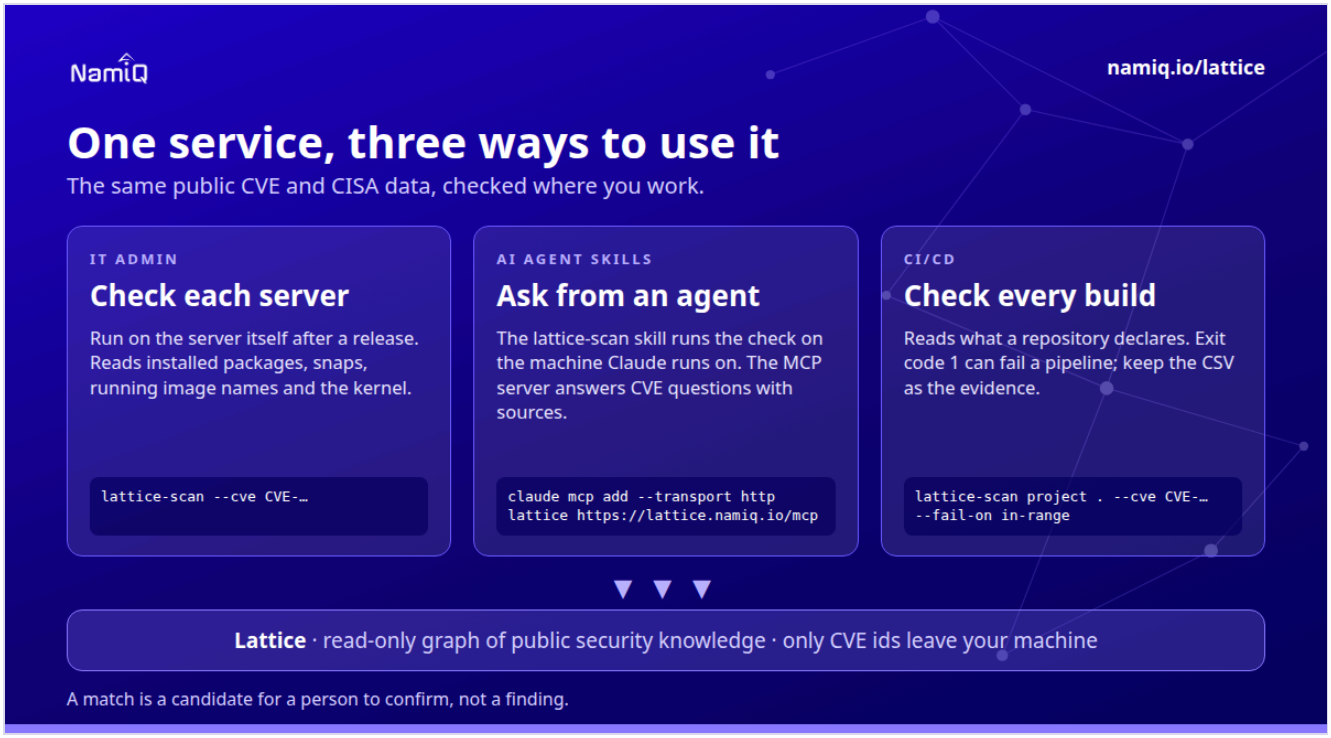
On a repository: the project check reads what it declares, in Python, JavaScript, Java, Rust, C and C++, Make, and Docker and compose files. It installs and runs nothing. A declared range or a tag without a patch number cannot show whether a fix is in, so such a row is undetermined and needs a person.

```
lattice-scan project . --cve CVE-2026-115644
```

Connector plugins, and a Kafka Connect shipped inside a vendor distribution, are not read by either check. The host check sees packages a distribution installed and the names of running images.

Who can use it, and how

For	What to do	Command
IT admin	Run the host check on each server after a release, and again when a new entry lands.	lattice-scan --cve CVE-2026-115644
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
CI/CD	Check the repository on every pull request. Exit code 1 fails the pipeline; keep the CSV as the evidence.	lattice-scan project . --cve CVE-2026-115644 --fail-on in-range



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

- A severity score. Apache has not published one with the record.
- Whether anyone is exploiting it. The record does not say.
- Whether managed services that run Connect for you are affected, and when they patch.

If you take one thing from this: when you separate an interface to protect it, test that the protection followed it. A control that works on the front door and not on the side door is how most of these start.

Appendix 1. Timeline

Date	Event
28 October 2026	Apache publishes the CVE record for CVE-2026-115644 and the fixed releases are listed as 4.2.2, 4.3.2 and 4.4.0.

Appendix 2. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
admin.listeners is set to a separate listener and the admin port is reachable by anyone who should not change logging	High	Remove the setting or upgrade this week
admin.listeners is set, admin port reachable only from a few operations hosts	Medium	Upgrade in the next window
admin.listeners is not set	None for this CVE	Confirm, then upgrade in the normal cycle
Kafka Connect not used	None	None

Appendix 3. Definition of done

- Every Kafka Connect worker's configuration has been read for admin.listeners.
- Where it is set, either it has been removed or the worker runs a fixed release.
- Connect workers are on 4.2.2, 4.3.2, 4.4.0 or later in their line.
- The admin port is reachable only from operations hosts.
- Changes to logging levels are monitored.

Sources

- CVE-2026-115644 record (Apache CNA): https://www.cve.org/CVERecord?id=CVE-2026-115644
- Apache Kafka CVE list: https://kafka.apache.org/cve-list