contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

WSO2 API Manager: new CVE

CVE-2026-4052 · record published 3 November 2026

Analysis Report

Anyone running WSO2 API Manager 4.1.0–4.4.0 with WSO2 Identity Server as the Resident Key Manager and database sharing between them needs to act; if that configuration is not in place, this CVE does …

PREPARED BY	NamiQ	DATE	3 November 2026
FACTS AS OF	3 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	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/wso2-api-manager-cve-2026-4052

The bottom line

> *Anyone running WSO2 API Manager 4.1.0–4.4.0 with WSO2 Identity Server as the Resident Key Manager and database sharing between them needs to act; if that configuration is not in place, this CVE does not apply. Check whether that configuration is active before anything else.*

At a glance

Fact	Detail
Product	WSO2 API Manager (CVE-2026-4052)
Severity	Critical: 9.8 (CVSS 3.1)
Status	A new CVE record, published by WSO2 on 3 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 3 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	The record does not name a fixed version. No vendor advisory could be read at the time of writing.
Who looks first	Teams running WSO2 API Manager at version 4.1.0, 4.2.0, 4.3.0, or 4.4.0 where WSO2 Identity Server is configured as the Resident Key Manager and the two products share a database.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run WSO2 API Manager?	Nothing to do for this CVE.	Check the version next.
Is your version 4.1.0, 4.2.0, 4.3.0, or 4.4.0?	Nothing to do for this CVE.	Check the Resident Key Manager configuration next.
Is WSO2 Identity Server configured as the Resident Key Manager for API Manager?	Nothing to do for this CVE.	Check whether the two products share a database.
Do WSO2 API Manager and WSO2 Identity Server share a database?	Nothing to do for this CVE.	All conditions are met — act now.

What it is

A self-registered user can obtain a token from the WSO2 Identity Server token endpoint and use it to call the System REST APIs of WSO2 API Manager — interfaces that should require privileged access.

Why it matters

Our reading is that the 9.8 score reflects what an attacker can do once the condition is met: any self-registered user, with no elevated privileges, can reach the System REST APIs. The weakness, CWE-862, is a missing authorisation check — the API accepts a valid token without verifying the holder's entitlement to those resources. The specific configuration required limits who is at risk, but for those who are, the attacker needs only an account that anyone can create.

Things people will get wrong

- This affects any WSO2 API Manager deployment The record limits it to deployments where WSO2 Identity Server is the Resident Key Manager and shares a database with API Manager; without both conditions, the flaw does not apply.
- Blocking external access to the Identity Server token endpoint closes the risk The record does not state that network restriction alone is sufficient. No workaround is given; contact WSO2 for guidance.

How we would triage it

This is our judgement.

Step 1: Find which version of WSO2 API Manager you run

- Check the installed WSO2 API Manager version; versions 4.1.0, 4.2.0, 4.3.0, and 4.4.0 are listed as affected by the record.

Step 2: Check the Resident Key Manager configuration

- In the API Manager admin console, confirm whether WSO2 Identity Server is set as the Resident Key Manager; if it is not, this CVE does not apply to your deployment.

Step 3: Check whether the two products share a database

- Review the API Manager and Identity Server datasource configuration to confirm whether they use the same database; if they do not, this CVE does not apply.

Step 4: Contact WSO2 for the patch

- The record does not name a fixed version and no vendor advisory could be read. Contact WSO2 directly to obtain the patch or any available workaround.

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 are reviewing CVE-2026-4052, a critical vulnerability in WSO2 API Manager (CVSS 9.8). It affects versions 4.1.0, 4.2.0, 4.3.0, and 4.4.0 where WSO2 Identity Server is the Resident Key Manager and both products share a database. In that configuration, a self-registered user can access the System REST APIs without proper authorisation. Please confirm whether we run WSO2 API Manager, which version is installed, and whether the described configuration is in place. The record does not name a fixed version; please obtain the patch or workaround from WSO2 and provide written confirmation of the version and the fix by 10 November 2026.*

The weakness behind it

The record classes this as CWE-862.

The sources, in their words

The CVE record:

> *This issue only impacts deployments where WSO2 Identity Server is configured as a Resident Key Manager with database sharing. In such environments, a self-registered user may gain access to the System REST APIs of WSO2 API Manager by obtaining a token from the WSO2 Identity Server token endpoint.*

Versions of WSO2 API Manager the record lists as affected:

- 4.1.0
- 4.2.0
- 4.3.0
- 4.4.0

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-2026-4052
```

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 names of running container images 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-2026-4052
```

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. It reads the names of the running images, not what is 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

- No fixed version is named in the record, and no vendor advisory could be read; the patch version is not known.
- Whether disabling self-registration or restricting the Identity Server token endpoint serves as a workaround is not stated.
- Which specific System REST APIs become reachable and what actions they permit is not described in the record.
- Whether an external attacker who self-registers, or only an existing internal user, can exploit this is not stated.
- 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 3 November 2026. We have not read the vendor's advisory page and we have not tested it.
- 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", "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-2026-4052: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A: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.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
3 November 2026	CVE record published by WSO2.

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
Affected version, Identity Server as Resident Key Manager, shared database, and self-registration open	Medium	This week; no vendor fix is recorded yet
Affected version with that configuration but self-registration status unknown	Medium	Clarify self-registration status this week
Affected version installed but Resident Key Manager configuration not yet checked	Medium	Verify the configuration this week
WSO2 API Manager in use but Identity Server is not the Resident Key Manager	None	None for this CVE

Appendix 4. Definition of done

- Every WSO2 API Manager 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-2026-4052: https://www.cve.org/CVERecord?id=CVE-2026-4052
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: security.docs.wso2.com: https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2026-5212/