contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Apache Software Foundation Apache JSPWiki: new CVE

CVE-2026-78114 · record published 25 November 2026

Analysis Report

Anyone running Apache JSPWiki version 2.10 through 3.0.0 should upgrade now; the record carries a CVSS 4.0 score of 10, the maximum. The first step is to upgrade to 3.0.1 (3.x) or 2.12.6 (2.x) as the …

PREPARED BY	NamiQ	DATE	26 November 2026
FACTS AS OF	26 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 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/apache-software-foundation-apache-jspwiki-cve-2026-78114

The bottom line

> *Anyone running Apache JSPWiki version 2.10 through 3.0.0 should upgrade now; the record carries a CVSS 4.0 score of 10, the maximum. The first step is to upgrade to 3.0.1 (3.x) or 2.12.6 (2.x) as the record states.*

At a glance

Fact	Detail
Product	Apache Software Foundation Apache JSPWiki (CVE-2026-78114)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by Apache on 25 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 26 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	3.0.1 for 3.x users, or 2.12.6 for 2.x users. The record names both as the fix.
Who looks first	Anyone running Apache JSPWiki on versions 2.10 through 3.0.0 on any platform. The flaw is in the login flow, so it affects any installation where users authenticate.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Apache JSPWiki anywhere on your network?	Nothing to do for this CVE.	Check the version (next question).
Is the version between 2.10 and 3.0.0 (inclusive)?	Nothing to do for this CVE.	Plan an upgrade to 3.0.1 (3.x) or 2.12.6 (2.x).
Is the JSPWiki login page reachable from outside your organisation?	Lower urgency; upgrade at the next opportunity.	Upgrade promptly; external access raises the risk of session fixation attempts.

What it is

The session identifier was not replaced when a user logged in. An attacker who had placed a known session identifier in the victim's browser beforehand could use that same identifier after login to access whatever the authenticated account can reach.

Why it matters

Session fixation lets an attacker piggyback on a legitimate user's login without knowing their password. The attacker plants a session token they control in the victim's browser before the victim authenticates; once the victim logs in, that token becomes valid for the authenticated session. The record scores this 10 on CVSS 4.0, the maximum possible. Our reading is that the practical difficulty depends on how the attacker delivers a crafted session identifier to the victim's browser; the record does not describe the delivery method, so that step remains uncertain and is worth factoring into your priority assessment.

Things people will get wrong

- Any upgrade within the 3.x line is sufficient. The record names 3.0.1 specifically. Version 3.0.0 is listed as affected; only 3.0.1 is named as the fix for 3.x users.
- This flaw only matters if the attacker already has credentials. The attacker needs no credentials. The risk is to any user who logs in while an attacker can influence their session identifier before that login occurs.

The wording includes conditions the score may not show: authenticated. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

Step 1: Find the version you run

- Look at the JSPWiki admin panel or the About page inside the wiki; the version number is shown there.
- If you have server access, check the deployed WAR or JAR filename, or the deployment manifest for the version string.

Step 2: Assess who can reach the login page

- Confirm whether the login endpoint is reachable from outside your organisation; this affects how urgently the upgrade should be prioritised.

Step 3: Upgrade to the fixed version

- The record states the fix is in 3.0.1 for 3.x installations or 2.12.6 for 2.x installations; deploy the appropriate release.
- Confirm the updated version appears in the admin panel before allowing users to resume logins.

Step 4: Invalidate existing sessions after upgrade

- After patching, ask the wiki administrator to invalidate all active sessions so any session identifiers planted before the upgrade cannot be used.

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 have been made aware of CVE-2026-78114, a session fixation flaw in Apache JSPWiki affecting versions 2.10 through 3.0.0. The CVE record carries a CVSS 4.0 score of 10. We would like to know whether we run JSPWiki anywhere, which version is installed, and whether the login page is reachable from outside our network. The record names version 3.0.1 (for 3.x) or 2.12.6 (for 2.x) as the fix. Please confirm in writing which version we run, whether the upgrade has been applied or is scheduled, and provide an expected completion date.*

The weakness behind it

The record classes this as CWE-384.

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	Session fixation exploits the login flow of a web application. If JSPWiki is internet-facing, this would likely be the initial access technique used to gain authenticated entry without valid credentials.
Use Alternate Authentication Material (T1550): Using a stolen token or hash instead of a password to log in.	Defense Evasion: avoiding detection	After the victim authenticates, the attacker holds a valid session token they planted beforehand. Using that token to access authenticated pages would likely follow, in place of a normal credential-based login.

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:

> *Session Fixation in the login flow of Apache JSPWiki versions 2.10 through 3.0.0 on all platforms. The session identifier was not replaced when a user authenticated, so an attacker who could set a known session identifier in the browser of a victim could use the same identifier after the victim logged in. Users are recommended to upgrade to version 3.0.1 (3.x) or 2.12.6 (2.x), which fix this issue.*

Versions of Apache Software Foundation Apache JSPWiki the record lists as affected:

- 2.10.0 through 3.0.0

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-2026-78114
```

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-2026-78114
```

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 describe how an attacker delivers a fixed session identifier to a victim's browser; whether that step requires a second vulnerability or is straightforward is not stated.
- No workaround short of upgrading is mentioned in the record; patching appears to be the only stated remedy.
- The record does not say whether any configuration option or server-side session setting mitigates the flaw on versions that cannot be immediately upgraded.
- 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 26 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", "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-2026-78114: score 10, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA: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.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
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
25 November 2026	CVE record published by Apache.

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
JSPWiki 2.10–3.0.0 with the login page reachable from the internet	Medium	This week
JSPWiki 2.10–3.0.0 on an internal network accessible to untrusted users	Medium	Next patch cycle

JSPWiki 2.10–3.0.0 on a tightly controlled internal network with trusted users only	Low	Next patch cycle
JSPWiki on any version outside 2.10–3.0.0	None	none for this CVE

Appendix 4. Definition of done

- Every Apache Software Foundation Apache JSPWiki 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-2026-78114: https://www.cve.org/CVERecord?id=CVE-2026-78114
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: lists.apache.org: https://lists.apache.org/thread.html/n43zhkpnphlksm12w7ndx4d87s7wdffv