contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Oracle Corporation Oracle Platform Security for Java: new CVE

CVE-2026-114824 · record published 17 November 2026

Analysis Report

If you run Oracle Fusion Middleware, find out this week whether Oracle Platform Security for Java is installed and which version it is. The record lists 12.2.1.4.0 and

PREPARED BY	NamiQ	DATE	17 November 2026
FACTS AS OF	17 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/oracle-corporation-oracle-platform-security-cve-2026-114824

The bottom line

> *If you run Oracle Fusion Middleware, find out this week whether Oracle Platform Security for Java is installed and which version it is. The record lists 12.2.1.4.0 and 14.1.2.0.0. If you do not run it, you can stop reading.*

At a glance

Fact	Detail
Product	Oracle Corporation Oracle Platform Security for Java (CVE-2026-114824)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by Oracle on 17 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 17 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No source we read names a fixed version
Who looks first	Anyone running Oracle Fusion Middleware, and the IT provider who manages it. The record names the Centralized Thirdparty Jars component of Oracle Platform Security for Java.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Oracle Fusion Middleware, or does your IT provider run it for you?	Nothing to do for this CVE.	Check whether Oracle Platform Security for Java is installed (next question).
Is Oracle Platform Security for Java at 12.2.1.4.0 or 14.1.2.0.0?	The record does not list your version. Note it and ask Oracle's support to confirm.	Check whether anyone can reach it over HTTP (next question).
Can that server be reached over HTTP from the internet or from untrusted networks?	Lower urgency, but still patch. The record says no login is needed.	Treat as urgent. Restrict access now and ask for the vendor's fix.

What it is

An attacker with no login and network access over HTTP can take over Oracle Platform Security for Java. The record says the damage can spread to other products that depend on it (a scope change).

Why it matters

Our reading is that this is a rare combination: no login, no user action, a network path, and a score of 10.0. The record says a successful attack means takeover of the component, and that other products may be affected too. The record gives no sign of exploitation yet, so there is time to look before anyone attacks. Do not leave it for the next patch cycle.

Things people will get wrong

- "It is not on CISA's exploited list, so we can wait." The record only says it was new when read. It also says no login is needed and the attack is easy over a network, so waiting is a risk.
- "It is only a component library, so the impact is small." The record says attacks may significantly impact additional products (scope change), and that takeover of the component is possible.
- "A fixed version is out, so we just update." No source we could read names a fixed version. Ask Oracle or your provider for the patch information.

How we would triage it

This is our judgement.

Step 1: Find where it is installed

- List Oracle Fusion Middleware installations on your servers, or ask your provider for the list.
- Check whether Oracle Platform Security for Java is present and which version it reports.

Step 2: Reduce exposure

- The record says the attack comes over HTTP, so close that path to untrusted networks where you can.
- Put the server behind a firewall or VPN rule while no fix is confirmed.

Step 3: Get the fix

- No source we could read names a fixed version. Ask Oracle support or your provider which patch covers this CVE.

- Apply it only once the vendor confirms it covers this CVE and your version.

Step 4: Check afterwards

- Ask for written confirmation of the version and the fix.
- Review web server logs for unusual requests from before the fix.

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 have read CVE-2026-114824 in Oracle Platform Security for Java (Oracle Fusion Middleware, Centralized Thirdparty Jars). The record lists versions 12.2.1.4.0 and 14.1.2.0.0 and says an unauthenticated attacker can take over the component over HTTP. Please tell us whether we run it, where, and at which version, and whether it can be reached from outside. No fixed version is named in the record, so please tell us which patch Oracle recommends. Please confirm the version and the fix to us in writing by the end of this week.*

The weakness behind it

The listing classes this as Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Platform Security for Java. While the vulnerability is in Oracle Platform Security for Java, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Platform Security for Java..

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 says an unauthenticated attacker can reach the component over HTTP. That likely makes it an exploit against a public-facing application.

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:

> *Vulnerability in the Oracle Platform Security for Java product of Oracle Fusion Middleware (component: Centralized Thirdparty Jars). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Platform Security for Java. While the vulnerability is in Oracle Platform Security for Java, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Platform Security for Java. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector ...*

Versions of Oracle Corporation Oracle Platform Security for Java the record lists as affected:

- 12.2.1.4.0
- 14.1.2.0.0

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-2026-114824
```

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-2026-114824
```

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

- Which version fixes it. No vendor page could be read.
- Whether it is being exploited. It was not on CISA's list when read.
- What the vulnerable code or request looks like. The record does not say.
- Whether any workaround exists. No source says.
- 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 17 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-2026-114824: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/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	Changed	Damage reaches beyond 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
17 November 2026	CVE record published by Oracle.

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, reachable over HTTP from the internet	High	Immediately: restrict access, then patch when a fix is available
Affected version, reachable only from the internal network	Medium	This week
Fusion Middleware in use, version not yet known	Medium	This week: find the version first
Version outside the two listed	Low	Next patch cycle; ask the vendor to confirm
No Oracle Fusion Middleware at all	None	None for this CVE

Appendix 4. Definition of done

- Every Oracle Corporation Oracle Platform Security for Java 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-2026-114824: https://www.cve.org/CVERecord?id=CVE-2026-114824
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: www.oracle.com: https://www.oracle.com/security-alerts/cspunov2026.html