contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Apache Roller exploited

CVE-2026-129448 · on CISA's exploited list since 20 November 2026

Analysis Report

Anyone running Apache Roller 4.0.0 to 6.1.4 must act now: the CISA deadline of 23 November 2026 has passed and the record says active exploitation is under way. Upgrade to 6.1.6 first; if that is not ...

PREPARED BY	NamiQ	DATE	25 November 2026
FACTS AS OF	25 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	STATUS	On CISA's exploited list; due 23 November 2026

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-roller-cve-2026-129448

The bottom line

> *Anyone running Apache Roller 4.0.0 to 6.1.4 must act now: the CISA deadline of 23 November 2026 has passed and the record says active exploitation is under way. Upgrade to 6.1.6 first; if that is not yet possible, apply the web.xml workaround and restart before anything else.*

At a glance

Fact	Detail
Product	Apache Roller (CVE-2026-129448)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 20 November 2026. Deadline for US federal agencies: 23 November 2026.
Chance of exploitation (EPSS)	0.24, the estimated chance in the next 30 days, as at 25 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Apache Roller 6.1.6 or later, as stated in the record.
Who looks first	Anyone hosting Apache Roller versions 4.0.0 through 6.1.4. Exposure is highest if the XML-RPC endpoint is internet-facing, but the flaw also applies on networks where untrusted users can reach the application.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Apache Roller on any server?	Nothing to do for this CVE.	Check the installed version.
Is your version between 4.0.0 and 6.1.4 inclusive?	Not affected by this CVE. If you run 6.1.5, see CVE-2026-82384.	Assess whether the XML-RPC endpoint is reachable.
Is /roller-services/xmlrpc reachable from outside your network?	Risk is lower; still upgrade at the next opportunity.	Patch or apply the workaround today.

What it is

An unauthenticated attacker who can reach the XML-RPC endpoint sends a crafted request that the server deserialises before checking any credentials, allowing the attacker to run arbitrary code on the server.

Why it matters

The flaw requires no credentials: any network request to the XML-RPC endpoint triggers deserialisation before authentication runs. A CVSS score of 9.8 reflects that combination. The record states that active exploitation is occurring. The related CVE-2026-82384 covered only version 6.1.5; this CVE covers the wider range from 4.0.0, meaning the same flaw was present in older releases. Both carry CWE-502 and the same attack path. Our reading is that an internet-facing instance should be treated as already at risk.

Things people will get wrong

- Disabling XML-RPC in the administration UI is enough The record states it is not: older versions deserialise the XML-RPC request before checking the administration UI setting, so the endpoint remains exploitable even when the UI shows it as disabled.
- Only version 6.1.5 is affected Version 6.1.5 is covered by CVE-2026-82384, a separate record for the same underlying flaw. This CVE covers versions 4.0.0 through 6.1.4. Neither record lists the other's version range.

How we would triage it

This is our judgement.

Step 1: Find the Roller version you run

- Check the version in the Roller administration UI, or in the web application's manifest or build artefacts.
- The affected range is 4.0.0 to 6.1.4; if you are in that range, continue to the next step.

Step 2: Apply the workaround if you cannot upgrade immediately

- The record says to set 'enabledForExtensions' to 'false' in WEB-INF/web.xml, or to remove the '/roller-services/xmlrpc' servlet mapping, then restart Roller.
- The record warns that disabling XML-RPC from the administration UI alone is not sufficient.

Step 3: Upgrade to Apache Roller 6.1.6 or later

- The record recommends upgrading to 6.1.6 or later, which disables the extension types and rejects XML-RPC requests when the XML-RPC feature is disabled.
- The CISA deadline of 23 November 2026 has already passed; treat this as urgent.

Step 4: Verify the endpoint no longer accepts XML-RPC requests

- After patching or applying the workaround, confirm that requests to /roller-services/xmlrpc are rejected.
- Review web server and application logs for unusual POST requests to that path before the fix was applied.

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. CISA's wording adds that you should stop using the product if no mitigation is available.

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 writing about CVE-2026-129448, a remote code execution flaw in Apache Roller versions 4.0.0 through 6.1.4. The CISA remediation deadline was 23 November 2026 and the record states active exploitation is occurring. Please check whether we run Apache Roller on any server, and if so, which version. The fix is to upgrade to Apache Roller 6.1.6 or later. If immediate upgrade is not possible, the record describes a workaround: set 'enabledForExtensions' to false in WEB-INF/web.xml, or remove the XML-RPC servlet mapping, and restart. Please confirm in writing the version installed, whether the workaround or upgrade has been applied, and when full remediation will be complete.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unusual POST requests to /roller-services/xmlrpc in web server access logs, particularly from unfamiliar source addresses.
- Unexpected processes spawned by the application server process, or unusual outbound network connections from the host running Roller.

The weakness behind it

The record classes this as CWE-502 (Deserialization of Untrusted Data).

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 flaw is reachable over the network without credentials via a public-facing web endpoint; exploiting it would likely be the initial access step into the host.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	Deserialisation exploits typically achieve code execution by invoking a command interpreter on the host; the record confirms arbitrary code execution is possible.

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

CISA's catalogue entry:

> *Apache Roller contains a deserialization of untrusted data vulnerability that allows an unauthenticated remote attacker to execute arbitrary code via the XML-RPC endpoint, which accepts and deserializes vendor extension types before authentication. This CVE covers the same underlying vulnerability as CVE-2026-82384 but applies to a broader range of affected versions.*

The CVE record, published by Apache on 17 November 2026:

> *Deserialization of Untrusted Data in Apache Roller versions 4.0.0 through 6.1.4 allows an unauthenticated remote attacker to execute arbitrary code. The XML-RPC endpoint accepts vendor extension types and deserializes them before authenticating the requester. This is the same vulnerability as CVE-2026-82384, which listed only Apache Roller 6.1.5 as affected. This issue is being actively exploited. Users are recommended to upgrade to Apache Roller 6.1.6 or later, which disables the extension types and rejects XML-RPC requests when the XML-RPC feature is disabled. Users who cannot upgrade right away should set "enabledForExtensions" to "false" in WEB-INF/web.xml, or remove the ...*

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

- 4.0.0 up to, but not including, 6.1.5

The affected ranges end before 6.1.5. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

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-2026-129448
```

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-2026-129448
```

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 the XML-RPC endpoint is enabled by default in all affected versions from 4.0.0 onwards is not stated in the record.
- No vendor advisory page could be read; the workaround and fix details come from the CVE record alone.
- Which specific vendor extension types trigger exploitation is not described in the record.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 25 November 2026; the vendor's advisory wins where it differs.
- 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-2026-129448: 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. The record's own score can differ from the base score on the NVD record.

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
17 November 2026	CVE record published by Apache.
20 November 2026	CISA added it to its list of exploited vulnerabilities.
23 November 2026	CISA's deadline for US federal agencies.

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
Running Apache Roller 4.0.0–6.1.4 with the XML-RPC endpoint internet-facing	High	Now — patch or apply the workaround today
Running Apache Roller 4.0.0–6.1.4, upgrade not yet possible	High	Apply the web.xml workaround and restart today
Running Apache Roller 4.0.0–6.1.4 on an internal network only	Medium	Upgrade to 6.1.6 this week

Running Apache Roller 6.1.5 (not affected by this CVE)	Low	Review CVE-2026-82384 for that version
Running Apache Roller 6.1.6 or later	None	No action needed for this CVE

Appendix 4. Definition of done

- Every Apache Roller you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-129448: https://www.cve.org/CVERecord?id=CVE-2026-129448
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: github.com: https://github.com/apache/roller/pull/171
- Reference in the CVE record: lists.apache.org: https://lists.apache.org/thread/cc0jck13nb9vvcmzxzwotr6n16mx28z9
- Reference in the CVE record: www.cve.org: https://www.cve.org/CVERecord?id=CVE-2026-82384
- Reference in the CVE record: lists.apache.org: https://lists.apache.org/thread.html/lnz4s26tv6hdo03wngtdbpfj4hg4gtds