contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Apache Axis exploited

CVE-2026-90436 · on CISA's exploited list since 18 November 2026

Analysis Report

If you run Apache Axis 1.x, treat it as urgent: CISA's date is 21 November 2026, three days away. Find where Axis 1.x runs and cut off its network exposure first, because no fixed version is recorded.

PREPARED BY	NamiQ	DATE	18 November 2026
FACTS AS OF	18 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	STATUS	On CISA's exploited list; due 21 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-axis-cve-2026-90436

The bottom line

> *If you run Apache Axis 1.x, treat it as urgent: CISA's date is 21 November 2026, three days away. Find where Axis 1.x runs and cut off its network exposure first, because no fixed version is recorded.*

At a glance

Fact	Detail
Product	Apache Axis (CVE-2026-90436)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 18 November 2026. Deadline for US federal agencies: 21 November 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 18 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	The record's affected ranges end before 41f3b4e8d04e310ca81f86b92630ab2c11d608bd
Who looks first	Anyone running Apache Axis 1.x, version 1.4 or earlier, in a Java application that receives SOAP messages. Old web services and bundled libraries are the likely places.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run any Java application that uses Apache Axis 1.x?	Nothing to do for this CVE.	Check the version (next question).
Is the Axis version 1.4 or earlier?	Not in the record's affected range; confirm the version in writing.	Affected. Go to the next question.
Can untrusted networks reach the service, or does it parse SOAP replies from outside?	Lower urgency, but still plan to migrate.	Restrict access now, then plan migration.

What it is

A crafted SOAP fault message makes Axis load and create a class the attacker names. If a suitable class is on the application's classpath, the attacker can run code on the server without logging in.

Why it matters

Our reading is that this flaw matters because it needs no login and the record scores it 9.8 on CVSS 3.1. The record says authentication handlers on a service do not help, as the fault is parsed before they run. The record also says Axis 1 is unsupported, so a patch may never come.

Things people will get wrong

- "We have authentication on our service, so we are safe." The record says the fault is parsed while Axis resolves the target service, before any per-service handler chain runs, so those handlers do not protect against it.
- "Nothing happens unless a class is already present." The record says loading a class runs its static initializer, and code execution needs a suitable class on the classpath. Most applications' classpaths are hard to rule out.
- "Updating to the latest Axis 1.x fixes it." The record lists all versions up to and including 1.4 as affected and names no fixed version.

How we would triage it

This is our judgement.

Step 1: Find where Axis 1.x runs

- List Java applications and servers, and look for Axis 1.x libraries inside them.
- Check the version. The record says all versions up to and including 1.4 are affected.

Step 2: Reduce exposure

- Block or restrict network access to Axis services from untrusted networks.
- The record says per-service authentication does not protect, so restrict at the network level.

Step 3: Plan the migration

- The record recommends moving to a different SOAP engine and names Apache Axis 2/Java as an example.

- The record mentions an alternative build, but its text is cut off. Ask the vendor or your provider what it is.

Step 4: Check and record the result

- Confirm in writing which applications used Axis 1.x and what was done about each.
- Look in logs for unusual SOAP faults, as listed below.

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 need to know whether any of our systems use Apache Axis 1.x, which CVE-2026-90436 affects (all versions up to and including 1.4). Please tell us where it runs and which version. No fixed version is recorded, so please say how you will cut off exposure or migrate. CISA's date is 21 November 2026. Please confirm in writing by 20 November 2026.*

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:

- Inbound SOAP messages containing a fault with an exception name and a data element.
- Unexpected child processes started by the Java application that runs Axis.
- Application errors about classes that cannot be loaded or created.

The weakness behind it

The record classes this as CWE-470 (Use of Externally-Controlled Input to Select Classes or Code).

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 a network without login, so it would likely be used to get into a public-facing service.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The record says it leads to remote code execution, so an attacker would typically then run commands on the host.

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 Axis contains an unsafe reflection vulnerability that could allow an unauthenticated remote attacker to execute arbitrary code via a crafted SOAP fault message that causes Axis to load and instantiate an attacker-specified class when a suitable class is available on the application classpath. The impacted product(s) could be end-of-life (EoL) and/or end-of-service (EoS). Users are advised to discontinue use and/or transition to a supported version.*

The CVE record, published by Apache on 6 November 2026:

> *** UNSUPPORTED WHEN ASSIGNED ** Deserialization of an inbound SOAP fault in Apache Axis 1.x allows unauthenticated remote class instantiation. When a SOAP <Fault> carries a <detail> <exceptionName> element, Axis loads the named class and, if a String <data> element is also present, instantiates it through its String constructor before checking that it is an AxisFault. Loading alone runs the class's static initializer. With a suitable class on the application's classpath this leads to remote code execution. The fault is parsed while the engine resolves the target service, before any per-service handler chain runs, so authentication handlers configured on a service do not protect against it. …*

Versions of Apache Software Foundation Apache Axis 1.x (EOL) the record lists as affected:

- all versions up to and including 1.4

Versions of Apache Software Foundation Apache Axis 1.x (EOL) the record lists as affected:

- all versions up to and including 1.4

Versions of Apache Software Foundation Apache Axis 1.x (EOL) the record lists as affected:

- aac718c6035435d96b39d6aebb9c078a13af7cc8 up to, but not including, 41f3b4e8d04e310ca81f86b92630ab2c11d608bd

The affected ranges end before 41f3b4e8d04e310ca81f86b92630ab2c11d608bd. 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-2026-90436
```

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-2026-90436
```

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

- No vendor page could be read, so no fixed version, build or workaround is confirmed.
- The record names no specific classes that make exploitation possible.
- The record text is cut off, so details of the alternative build it mentions are missing.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 18 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-2026-90436: 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
6 November 2026	CVE record published by Apache.
18 November 2026	CISA added it to its list of exploited vulnerabilities.
21 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
Axis 1.x service reachable from the internet	High	Within CISA's window
Axis 1.x reachable only from an internal network	Medium	This week
Axis 1.x client or library that parses SOAP replies from outside parties	Medium	This week
No Axis 1.x anywhere in your estate	None	None for this CVE

Appendix 4. Definition of done

- Every Apache Axis 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-2026-90436: https://www.cve.org/CVERecord?id=CVE-2026-90436
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: github.com: https://github.com/apache/axis-axis1-java/commit/41f3b4e8d04e310ca81f86b92630ab2c11d608bd
- Reference in the CVE record: lists.apache.org: https://lists.apache.org/thread.html/8slf0j9gz35z56t0glt5h0ncwlbn4bdz