contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Apache Struts exploited

CVE-2016-3081 · on CISA's exploited list since 8 October 2026

Analysis Report

If you run Apache Struts 2 with Dynamic Method Invocation enabled, you are already past CISA's date of 11 October 2026. Switch that feature off first, then move to 2.3.20.3, 2.3.24.3 or 2.3.28.1. If ...

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 8.1**	STATUS	On CISA's exploited list; due 11 October 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-struts-cve-2016-3081

The bottom line

> *If you run Apache Struts 2 with Dynamic Method Invocation enabled, you are already past CISA's date of 11 October 2026. Switch that feature off first, then move to 2.3.20.3, 2.3.24.3 or 2.3.28.1. If you do not run Struts, you can stop reading.*

At a glance

Fact	Detail
Product	Apache Struts (CVE-2016-3081)
Severity	High: 8.1 (CVSS 3.1)
CISA	On its exploited list since 8 October 2026. Deadline for US federal agencies: 11 October 2026.
Chance of exploitation (EPSS)	0.97, the estimated chance in the next 30 days, as at 1 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Struts 2.3.20.3, 2.3.24.3 or 2.3.28.1, according to the Apache Struts bulletin S2-032.
Who looks first	Anyone who runs a Java web application built on Struts 2, or whose IT provider or software supplier does. It only matters if Dynamic Method Invocation is on.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you, or a supplier, run a web application built on Apache Struts 2?	Nothing to do for this CVE.	Check the Struts version (next question).
Is it in the affected range, and not already one of the fixed releases?	The bulletin names no further action for this CVE.	Check whether Dynamic Method Invocation is on.
Is Dynamic Method Invocation enabled in the application's configuration?	The flaw needs it. Still plan the upgrade.	Turn it off now, then upgrade.
Can anyone outside your organisation reach the application over the network?	Lower exposure, but still fix it in this cycle.	Treat as urgent and check for signs of misuse.

What it is

A remote attacker can send a crafted request using the method: prefix and run their own code on the server. The record says this works when Dynamic Method Invocation is enabled.

Why it matters

Our reading is that this flaw is useful to an attacker as a way in: it gives code execution on the server through an ordinary web request, and the record names no login step. The record published it in April 2016 with a score of 8.1. A Struts application still affected has probably gone unpatched for a long time and may not have an owner who watches it.

What the vendor's advisory says

We read two pages on cwiki.apache.org. In short:

- The Apache bulletin S2-032 says remote code execution can be performed via the method: prefix when Dynamic Method Invocation is enabled.
- It rates the maximum security impact as Important.
- Its recommendation is to disable Dynamic Method Invocation if possible, or upgrade to 2.3.20.3, 2.3.24.3 or 2.3.28.1.
- Its workaround is to disable Dynamic Method Invocation, or write your own ActionMapper based on the source of the recommended versions.
- It expects no compatibility issues when upgrading to those three versions.

Things people will get wrong

- "Our Struts version isn't listed, so we're fine." The bulletin and the record give slightly different starting versions. Compare against the fixed releases, not only the lower bound.
- "It scores 8.1, so it can wait." The score does not capture that CISA lists it as exploited. The record also names no login step.
- "We never turned that feature on." Someone may have enabled it years ago. Check the configuration rather than relying on memory.

How we would triage it

This is our judgement.

Step 1: Find the Struts version you run

- Ask your IT provider and any software supplier whether any application uses Struts 2.

- Find the Struts core library on each server and read its version. Compare it with 2.3.20.3, 2.3.24.3 and 2.3.28.1.

Step 2: Check whether Dynamic Method Invocation is on

- Look in the Struts configuration for the Dynamic Method Invocation setting. The bulletin says the flaw needs it enabled.

Step 3: Reduce exposure, then upgrade

- Disable Dynamic Method Invocation if you can. The bulletin names this as its first recommendation and as a workaround.
- Upgrade to 2.3.20.3, 2.3.24.3 or 2.3.28.1, whichever matches your release line. The bulletin expects no compatibility issues.

Step 4: Check for signs of misuse and confirm the fix

- Review web server logs for requests that use the method: prefix.
- Ask for written confirmation of the version now running and that the setting is off.

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. CISA lists Apache Struts CVE-2016-3081 as exploited, and its date of 11 October 2026 has passed. Please tell us whether we run Struts 2 anywhere, directly or inside a supplier's product, and which version. Please also say whether Dynamic Method Invocation is enabled and whether the system is reachable from the internet. The Apache bulletin S2-032 names fixed versions 2.3.20.3, 2.3.24.3 and 2.3.28.1, and recommends disabling that feature. Please confirm in writing, by the end of this week, the version we run, whether the feature is off, and when the fix will be in place. Thank you.*

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:

- Web requests whose parameters or paths contain the method: prefix.

- Unexpected programs started by the Java application server process, or new files in its working folders.
- Any change to the Struts configuration that turned Dynamic Method Invocation on.

The weakness behind it

CISA's entry classes this as CWE-77 (Improper Neutralization of Special Elements used in a Command).

The sources, in their words

CISA's catalogue entry:

> *Apache Struts contains a command injection vulnerability that could allow remote attackers to execute arbitrary code via method:prefix when Dynamic Method Invocation is enabled.*

The CVE record, published by Redhat on 26 April 2016:

> *Apache Struts 2.3.19 to 2.3.20.2, 2.3.21 to 2.3.24.1, and 2.3.25 to 2.3.28, when Dynamic Method Invocation is enabled, allow remote attackers to execute arbitrary code via method: prefix, related to chained expressions.*

The record gives no version ranges. Use the vendor's advisory for the affected versions.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

What we do not know yet

- Whether the record's starting version of 2.3.19 or the bulletin's starting version of 2.3.20 is right. The two sources differ.
- Whether the attacks CISA lists need any particular configuration beyond Dynamic Method Invocation.
- Which products from other vendors bundle an affected Struts release. The sources do not list them.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 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", "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-2016-3081: score 8.1, `CVSS:3.1/AV:N/AC:H/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	High	Needs conditions outside the attacker's control.
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
26 April 2016	CVE record published by Redhat.
8 October 2026	CISA added it to its list of exploited vulnerabilities.
11 October 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
Struts 2 application on an affected version, Dynamic Method Invocation on, reachable from the internet	High	Now; CISA's date has passed
Same application, but reachable only from your internal network	Medium	This week
Affected version, but Dynamic Method Invocation is off	Low	Next patch cycle

Supplier-built product that bundles Struts, version unknown	Medium	Ask the supplier this week
You run no Struts application	None	None for this CVE

Appendix 4. Definition of done

- Every Apache Struts 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.
- 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-2016-3081: https://www.cve.org/CVERecord?id=CVE-2016-3081
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: cwiki.apache.org/confluence/spaces/WW/pages/62693266/S2-032: https://cwiki.apache.org/confluence/spaces/WW/pages/62693266/S2-032
- Advisory or release notes read: cwiki.apache.org/confluence/spaces/WW/pages/62693266/S2-032: https://cwiki.apache.org/confluence/spaces/WW/pages/62693266/S2-032
- Reference in the CVE record: struts.apache.org: https://struts.apache.org/docs/s2-032.html
- Reference in the CVE record: www.exploit-db.com: https://www.exploit-db.com/exploits/39756/