contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

OSGeo GeoServer exploited

CVE-2026-120705 · on CISA's exploited list since 27 November 2026

Analysis Report

Anyone running GeoServer must act by 30 November 2026 — CISA's deadline is three days from the listing date. Check whether WFS is reachable from untrusted networks and update to the vendor's latest ...

PREPARED BY	NamiQ	DATE	27 November 2026
FACTS AS OF	27 November 2026	VERSION	1.0
SEVERITY	**Not scored yet**	STATUS	On CISA's exploited list; due 30 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/osgeo-geoserver-cve-2026-120705

The bottom line

> *Anyone running GeoServer must act by 30 November 2026 — CISA's deadline is three days from the listing date. Check whether WFS is reachable from untrusted networks and update to the vendor's latest release; if GeoServer is not in your estate, nothing to do.*

At a glance

Fact	Detail
Product	OSGeo GeoServer (CVE-2026-120705)
Severity	Not scored when we read it
CISA	On its exploited list since 27 November 2026. Deadline for US federal agencies: 30 November 2026.
Chance of exploitation (EPSS)	Not available yet
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	The vendor's November 2026 advisory announces GeoServer 3.0.2, 2.28.6, and 2.27.7 as current releases; it does not explicitly state which release first fixed this CVE.
Who looks first	Anyone running OSGeo GeoServer with the WFS service accessible from untrusted networks. No authentication is required, so any host that can reach the endpoint is a potential source of exploitation.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run OSGeo GeoServer anywhere in your environment?	Nothing to do for this CVE.	Check whether WFS 2.0 is enabled on that instance.
Is WFS 2.0 enabled on your GeoServer instance?	Lower direct risk; still patch to cover the other flaws in the same release.	Check who can reach the WFS endpoint.
Can untrusted users or internet traffic reach your GeoServer WFS endpoint?	Lower urgency; patch within CISA's window of 30 November 2026 regardless.	Patch immediately — no authentication is needed to exploit this.

What it is

An unauthenticated attacker reaching the WFS 2.0 GetFeatureById endpoint can make GeoServer read local text files the server process can access, or force it to fetch attacker-chosen HTTP or HTTPS URLs via a crafted ID parameter. No login is needed. The CISA record notes this chains with four other flaws to reach unauthenticated remote code execution.

Why it matters

No authentication is needed: any network path to the WFS endpoint is enough. The CISA record states the flaw chains with CVE-2026-129244, CVE-2026-129243, CVE-2026-129245, and CVE-2026-129242 to reach unauthenticated remote code execution; the vendor's advisory calls this CVE step 4 of that chain. Used alone it still enables reading server-side files and making the server fetch internal URLs — useful for credential theft or pivoting to internal services. CISA's deadline of 30 November 2026 is three days from the listing date, which is unusually tight.

What the vendor's advisory says

We read one page on geoserver.org. In short:

- The same advisory addresses CVE-2026-129245 (Critical): predictable remember-me key allows administrator session forgery — also part of the RCE chain alongside this CVE.
- CVE-2026-129242 (High): deserialization in JDBC user and role services allows administrator code execution — the advisory identifies this as a step in the same RCE chain.
- CVE-2026-120707 (High) and CVE-2026-120708 (High): source IP access rules bypassed via X-Forwarded-For header in the GeoFence extension and ACL plugin respectively.
- CVE-2026-120709 (Medium): unauthenticated SSRF and file read via printing legend icon URL in the printing extension — a separate unauthenticated file-read path.
- Earlier releases addressed CVE-2025-53607 (High, unauthenticated XXE via OWS xsi:schemaLocation) in 3.0.0/2.28.4/2.27.6, and CVE-2024-35233 (High, ImageMosaic RCE) in 3.0.0/2.28.5/2.27.6.

Things people will get wrong

- An attacker needs credentials to reach the WFS endpoint. The CISA description says unauthenticated — no login is needed. Any host that can send an HTTP request to the WFS endpoint can attempt this.
- If we don't store sensitive files in the GeoServer data directory, the file-read risk is low. The SSRF component lets an attacker reach internal services regardless of local file content. The chain also reaches code execution via the other four CVEs.
- Patching CVE-2026-120705 alone is sufficient. The CISA record identifies four other CVEs (129244, 129243, 129245, 129242) that chain with this one to reach unauthenticated RCE. All

should be patched in the same update.

How we would triage it

This is our judgement.

Step 1: Find which version of GeoServer you run

- Check the GeoServer admin web interface under About & Status → Server Information, or query the REST API, for the installed version number.
- Note whether the WFS service is listed as enabled under Services in the admin UI.
- Record whether the GeoServer admin port or WFS endpoint is reachable from outside your internal network.

Step 2: Reduce exposure while preparing the patch

- If WFS is enabled and reachable from untrusted networks, consider restricting access at the firewall or network layer until the patch is applied.
- In the GeoServer admin UI under Services, confirm whether WFS 2.0 is enabled; disable it only if your use case permits.

Step 3: Apply the vendor's November 2026 security update

- The vendor's advisory announces GeoServer 3.0.2, 2.28.6, and 2.27.7 as current releases; update to the release matching your current branch.
- The same update addresses the other chain CVEs (129244, 129243, 129245, 129242); apply all fixes in the same maintenance window.
- Follow the vendor's upgrading guide referenced in the advisory before applying.

Step 4: Confirm the updated version and review access logs

- After updating, verify the new version via the GeoServer admin UI or REST API.
- Review GeoServer access logs for WFS GetFeatureById requests with unusual ID values — paths, URL schemes, or XML special characters — before the patch date.
- If the instance was internet-facing before patching, check outbound connection logs from the GeoServer host for unexpected external HTTP or HTTPS requests.

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 run OSGeo GeoServer and need to understand our exposure to CVE-2026-120705, an unauthenticated XML injection flaw in the WFS 2.0 GetFeatureById endpoint that allows file reads and server-side request forgery. CISA has listed this with a deadline of 30 November 2026. The vendor's November 2026 advisory announces GeoServer 3.0.2, 2.28.6, and 2.27.7 as the current releases. Please confirm: whether and where we run GeoServer and which version; whether WFS 2.0 is enabled and reachable from outside our internal network; and whether the update has been applied or when it can be completed by 30 November 2026. Please send written confirmation of the installed version and fix status.*

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:

- Look for WFS GetFeatureById requests with unusual ID values — particularly those containing file paths, URL schemes, or XML special characters — in GeoServer access logs.
- Look for outbound HTTP or HTTPS connections from the GeoServer host to unexpected addresses, which would indicate SSRF was attempted.
- Look for file-not-found errors or accesses to paths outside the data directory in GeoServer application logs, which may indicate local file read attempts.

The weakness behind it

CISA's entry classes this as CWE-91 (XML Injection) and CWE-611 (Improper Restriction of XML External Entity Reference) and CWE-918 (Server-Side Request Forgery).

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	An unauthenticated crafted request to the public-facing WFS endpoint would likely be the initial access technique — network access alone is sufficient, no credentials needed.
File and Directory Discovery (T1083): Listing files and folders to find what is there.	Discovery: looking around	The local file read component would likely serve discovery — an attacker could read GeoServer config files to find paths, credentials, or map accessible resources.
Exploitation of Remote Services (T1210): Exploiting a flaw in a service on another machine to move to it.	Lateral Movement: moving to other machines	The SSRF component would likely be used to reach internal services the GeoServer host can access, making this a probable lateral movement technique alongside the initial access.

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:

> *OsGeo GeoServer contains an XML injection vulnerability that allows an unauthenticated remote attacker to cause the server to read local text files accessible to the GeoServer process or fetch attacker-specified HTTP or HTTPS URLs via a crafted ID parameter in the WFS 2.0 GetFeatureById stored query. This vulnerability can be chained with CVE-2026-129244, CVE-2026-129243, CVE-2026-129245, and CVE-2026-129242 to achieve unauthenticated remote code execution on an affected GeoServer instance.*

The CVE record for CVE-2026-120705 was not available when we read it on 27 November 2026. CISA's entry is the only primary text until it is.

Without the record we cannot give version ranges. Use the vendor's advisory for the affected versions.

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-2026-120705
```

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-2026-120705
```

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 CVSS base score is in the available record; the vendor's advisory calls this High severity but no numeric score is stated for this CVE.
- The available record does not list specific GeoServer version ranges affected — it describes an affected GeoServer instance without naming a floor or ceiling version.
- No workaround short of patching is described in the available sources.
- The CVE record was unavailable at the time of this listing; the CISA description and the vendor's advisory are the only sources for the technical details of this flaw.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 27 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. Timeline

Date	Event
27 November 2026	CISA added it to its list of exploited vulnerabilities.
30 November 2026	CISA's deadline for US federal agencies.

Appendix 2. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
GeoServer WFS 2.0 is accessible from the internet or any untrusted network.	High	Patch by 30 November 2026.
Any of CVE-2026-129244, 129243, 129245, or 129242 are also unpatched on the same instance.	High	Patch all five together; the chain reaches unauthenticated RCE.
GeoServer WFS is internal-only but reachable from other systems on the same network segment.	Medium	Patch this week.
GeoServer is running but WFS is disabled, or the instance is already on a patched version.	Low	Verify patch status and check the other flaws in the same release.
GeoServer is not present in the estate.	None	No action needed for this CVE.

Appendix 3. Definition of done

- Every OSGeo GeoServer 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-2026-120705: https://www.cve.org/CVERecord?id=CVE-2026-120705
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: geoserver.org/vulnerability/2026/11/23/cve-update.html: https://geoserver.org/vulnerability/2026/11/23/cve-update.html