contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

OSGeo GeoServer exploited

CVE-2026-129243 · on CISA's exploited list since 27 November 2026

Analysis Report

Anyone running GeoServer on a network reachable by untrusted users must act by 30 November 2026. The first step is to identify your GeoServer version and upgrade to 3.0.2, 2.28.6, or 2.27.7 as listed …

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-2026-129243

The bottom line

> *Anyone running GeoServer on a network reachable by untrusted users must act by 30 November 2026. The first step is to identify your GeoServer version and upgrade to 3.0.2, 2.28.6, or 2.27.7 as listed in the vendor's advisory.*

At a glance

Fact	Detail
Product	OSGeo GeoServer (CVE-2026-129243)
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	GeoServer 3.0.2, 2.28.6, and 2.27.7, as listed in the vendor's advisory release announcements.
Who looks first	Anyone who operates GeoServer and exposes it to users outside the organisation, or to any internal network where not all users are fully trusted. No login is required to trigger the bypass.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run GeoServer anywhere in your organisation?	Nothing to do for this CVE.	Check whether it is reachable by untrusted users (next question).
Is GeoServer reachable by users outside your organisation, or by internal users who are not fully trusted?	Risk is lower; still plan to patch at the next maintenance window.	Check the version running (next question).
Is the version earlier than 3.0.2 (3.x branch), 2.28.6 (2.28.x branch), or 2.27.7 (2.27.x branch)?	No upgrade needed for this CVE.	Upgrade to the fixed version before 30 November 2026.

Does GeoServer rely on service-level security rules as the primary access control?	Layered controls reduce exposure; still patch within the CISA window.	Any rule relying on service-level checks alone can be bypassed; treat this as urgent.

What it is

An unauthenticated attacker can bypass service-level access controls by adding a prefix to the service parameter in a request. The CISA description says this flaw can be chained with CVE-2026-129244, CVE-2026-120705, CVE-2026-129245, and CVE-2026-129242 to achieve unauthenticated remote code execution.

Why it matters

This flaw is the entry point of a chain the CISA description says reaches unauthenticated remote code execution. CWE-863 (Incorrect Authorization) means a protection decision is made on a name that can be crafted to pass the check while the protected action still runs. Our reading is that this makes the bypass low-effort: no credential and no special condition beyond network reach. The vendor's advisory scores CVE-2026-129245 (predictable remember-me key, also a step in this chain) as Critical.

What the vendor's advisory says

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

- The same release addresses CVE-2026-129245 (Critical): predictable remember-me key allows administrator session forgery — also named in the CISA-listed RCE chain.
- CVE-2026-129242 (High): deserialization in JDBC user and role services allows administrator code execution — the final RCE step. CVE-2026-120705 (High): unauthenticated WFS GetFeatureById XML injection — another step in the same chain.
- CVE-2026-120710 (High): arbitrary file write via GeoWebCache FileRasterFilter ZIP update. CVE-2026-120707 and CVE-2026-120708 (both High): source IP rule bypasses via X-Forwarded-For in GeoFence and ACL plugin respectively.
- CVE-2026-129294 (High, community module): unauthenticated style management in OGC API Styles. CVE-2026-129293 (High): stored XSS via style name in style editor Layer Preview — the advisory describes these two as a separate chain leading to XSS.
- The vendor's advisory states GeoServer 3.0.x is the current stable release and 2.28.x the current maintenance release, and recommends upgrading to a supported release at least once a year to receive security fixes.

Things people will get wrong

- Patching this CVE alone is enough to block the full RCE chain. The CISA description names four CVEs in the chain. The vendor's advisory addresses all of them in the same release; upgrading to the fixed release closes all steps at once.
- Only WFS requests are affected. The CISA description says any service protected by service-level role checks is affected; the advisory example uses a prefixed parameter such as 'x/WFS' but the bypass is not limited to WFS.
- Requiring a login to reach GeoServer prevents this attack. The CISA description explicitly says the attacker is unauthenticated; no login is required to send the prefixed request that triggers the bypass.

How we would triage it

This is our judgement.

Step 1: Find which GeoServer versions you run

- Check each server or container running GeoServer. The version appears on GeoServer's web administration interface under 'About GeoServer'.
- Note whether each instance is on the 3.0.x, 2.28.x, or 2.27.x branch; the vendor's advisory lists fixed releases for all three branches.

Step 2: Restrict network access while preparing to patch

- If GeoServer is internet-facing, consider whether a firewall rule or reverse-proxy restriction can limit access to known IP ranges until the upgrade is applied.
- The CISA description says the bypass requires only a network request; reducing who can reach GeoServer reduces exposure while the upgrade is prepared.

Step 3: Apply the vendor's upgrade

- Upgrade to GeoServer 3.0.2, 2.28.6, or 2.27.7, as listed in the vendor's advisory, whichever matches the branch you run.
- The vendor's advisory notes the upgrade path is described in the GeoServer User Guide under 'Upgrading existing versions'.

Step 4: Confirm service-level security rules are intact after upgrade

- After upgrading, review GeoServer's security settings to verify that service-level rules are configured as expected and have not been altered.
- Check access logs for requests containing prefixed service parameters that arrived before the upgrade was applied, as the CISA description identifies this as the trigger pattern.

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 have been alerted to CVE-2026-129243, an unauthenticated authorization bypass in GeoServer that CISA says can be chained with four other flaws in the same release to allow remote code execution. CISA's remediation deadline is 30 November 2026. Please confirm: whether we run GeoServer and where; which version is installed; and whether the fixed release (3.0.2, 2.28.6, or 2.27.7, as named in the vendor's advisory) has been applied. If not, please provide the planned upgrade date and confirm in writing the installed version and fix status by 30 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:

- Look in GeoServer's access logs for requests to service endpoints where the service parameter contains a prefix, such as 'x/WFS' or similar patterns, particularly from unexpected source addresses.
- Look for unexpected OGC service requests such as GetFeature or GetCapabilities arriving outside business hours or from addresses not in your known user base.
- Look for unexpected changes to GeoServer styles, layer configurations, or JDBC user and role service settings, which could indicate the full chain was used to reach administrator-level access.

The weakness behind it

CISA's entry classes this as CWE-863 (Incorrect Authorization).

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 description says an unauthenticated remote attacker sends a crafted request to GeoServer over a network; this would typically map to exploiting a public-facing application to gain initial access.
Exploitation for Privilege Escalation (T1068): Using a flaw to gain higher rights than the account had, such as administrator or root.	Privilege Escalation: gaining higher rights	The flaw bypasses service-level role checks and the CISA description says the chain progresses to administrator-level code execution; the bypass would likely be used to escalate from no access to privileged operations.
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 chain's final step per the CISA description achieves code execution; deserialization in JDBC services (CVE-2026-129242) would typically result in command or script execution 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:

> *GeoServer contains an incorrect authorization vulnerability that allows an unauthenticated remote attacker to bypass service-level role checks and invoke operations protected solely by those checks via a request with a prefixed service parameter. This vulnerability can be chained with CVE-2026-129244, CVE-2026-120705, CVE-2026-129245, and CVE-2026-129242 to achieve unauthenticated remote code execution on an affected GeoServer instance.*

The CVE record for CVE-2026-129243 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-2026-129243
```

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-2026-129243
```

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 numeric score is available in the record; the vendor's advisory describes the flaw as High severity but no score is published.
- The record does not define a lower version bound; it is not stated which older versions of GeoServer are affected.
- No workaround short of upgrading is described; CISA's required action says to follow vendor instructions but no specific mitigation is named.
- It is not stated whether the bypass affects GeoServer instances that restrict access via an external authentication proxy rather than GeoServer's own service-level rules.
- 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 is internet-facing and running a version earlier than 3.0.2, 2.28.6, or 2.27.7.	High	Before 30 November 2026
GeoServer is on an internal network reachable by any user who is not fully trusted, unpatched.	High	Before 30 November 2026
GeoServer is on an internal network with only trusted staff, but service-level rules are the primary access control.	Medium	This week
GeoServer is running but accessible only to fully trusted administrators, with no external exposure.	Low	Next patch cycle
GeoServer is not running in the organisation.	None	None 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-2026-129243: https://www.cve.org/CVERecord?id=CVE-2026-129243
- 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