Two GeoServer Vulnerabilities Under Active Exploitation, Researchers Warn



watchTowr reports that attackers are actively exploiting two newly patched GeoServer flaws, CVE-2026-120705 and CVE-2026-129243. Researchers also warn of unauthenticated remote code execution chains.

- watchTowr says threat actors are actively exploiting two newly patched GeoServer vulnerabilities.
- The flaws are tracked as CVE-2026-120705 and CVE-2026-129243.
- CVE-2026-120705 has a CVSS score of 8.6 and is an arbitrary file read issue.
- It could expose local text files readable by the GeoServer process.
- Researchers warn the flaws can feature in unauthenticated remote code execution chains.

What has been reported

According to watchTowr, attackers are already exploiting two recently patched vulnerabilities in GeoServer. They are tracked as CVE-2026-120705 and CVE-2026-129243. Researchers also warn that such flaws can be combined into unauthenticated remote code execution chains.

What we know about the flaws

CVE-2026-120705 carries a CVSS score of 8.6. It is an **arbitrary file read** vulnerability that could let an attacker access local text files readable by the GeoServer process. The source excerpt is truncated, so it does not give full details of the second flaw or of the complete exploitation chains. We recommend reading the vendor and watchTowr advisories directly for technical detail.

Why it matters

Because exploitation is reported as active and fixes are already available, the window between patch release and attack is short. Any GeoServer instance reachable from untrusted networks and not yet updated should be treated as a priority exposure.

Organisations that use GeoServer for mapping or geospatial services, including in internal applications, should confirm where it runs and which version is deployed.

What to do now

1. Inventory all GeoServer instances, including internal and test environments, and record versions.
2. Apply the vendor's patches for CVE-2026-120705 and CVE-2026-129243 as a priority.
3. Restrict internet exposure of GeoServer administrative and service endpoints until patched.
4. Review web and application logs for unusual file-read requests or unexpected process activity.
5. Rotate credentials or secrets stored in files readable by the GeoServer process if compromise is suspected.