GeoServer flaws CVE-2026-120705 and CVE-2026-129243 probed in attacks



WatchTowr has seen probing of two high-severity GeoServer flaws that can be chained for unauthenticated remote code execution. Patches exist; upgrade to 3.0.2, 2.28.6 or 2.27.7.

- WatchTowr observed attempts to exploit CVE-2026-120705 and CVE-2026-129243, apparently to find vulnerable servers.
- No successful remote code execution has been reported, and no other exploitation reports were seen at the time of writing.
- The flaws belong to a five-bug chain found by a Rapid7 researcher; technical details and PoC code were published this week.
- Eye Security demonstrated unauthenticated RCE on Linux and Windows and counted more than 3,000 internet-accessible instances.

> - Fixed versions are GeoServer 3.0.2, 2.28.6 and 2.27.7.

Threat actors are targeting two recently disclosed GeoServer vulnerabilities that can be combined with other flaws to achieve unauthenticated remote code execution (RCE). GeoServer is an open source application for publishing and sharing geospatial data, widely used by government agencies and utilities.

What is happening

WatchTowr has observed exploit attempts against CVE-2026-120705 and CVE-2026-129243, both rated high severity. The probes appear designed to identify vulnerable servers, using error-based requests that create and invoke stored queries. WatchTowr has not reported any successful remote code execution, and the source notes no other exploitation reports at the time of writing.

CVE-2026-120705 is an XML injection flaw that can let an unauthenticated attacker read sensitive files or carry out server-side request forgery (SSRF). CVE-2026-129243 allows access controls to be bypassed so that administrator-level operations can be performed.

Why it matters

Both flaws are part of a five-bug chain reported to GeoServer developers in early August by Rapid7 researcher Jonah Burgess. The chain also includes CVE-2026-129244, CVE-2026-129245 and CVE-2026-129242, and shows how an attacker can gain admin access and run commands with the GeoServer process's privileges. Technical details and PoC exploit code were published this week. Eye Security independently demonstrated unauthenticated RCE on Linux and Windows by combining CVE-2026-120705, CVE-2026-129245 and CVE-2026-120704, and has identified more than 3,000 internet-accessible instances.

What to do

GeoServer released patches several weeks ago and has published advisories in recent days. Organizations should upgrade to GeoServer 3.0.2, 2.28.6 or 2.27.7. With public PoC code available, internet-facing instances should be treated as a priority.

What to do now

1. Inventory all GeoServer instances, including those run by business units or third parties, and note which are internet-facing.
2. Upgrade to GeoServer 3.0.2, 2.28.6 or 2.27.7, starting with internet-exposed instances.
3. Review web and application logs for error-based requests that create or invoke stored queries, and escalate any hits to incident response.
4. Check GeoServer for unexpected administrative changes and confirm the service runs with least privilege.
5. Where patching cannot be immediate, restrict access to GeoServer to trusted networks until the upgrade

is done.