

CVE-2025-58360

OSGeo GeoServer Improper Restriction of XML External Entity Reference Vulnerability

CISA KEV since Dec 11, 2025

Actively exploited

Public exploit module (Metasploit)

GeoServer is an open source server that allows users to share and edit geospatial data. From version 2.26.0 to before 2.26.2 and before 2.25.6, an XML External Entity (XXE) vulnerability was identified. The application accepts XML input through a specific endpoint /geoserver/wms operation GetMap. However, this input is not sufficiently sanitized or restricted, allowing an attacker to define external entities within the XML request. This issue has been patched in GeoServer 2.25.6, GeoServer 2.26.3, and GeoServer 2.27.0.

EVRS 79/₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.600 99.13rd percentile · FIRST	CISA DEADLINE Jan 1, 2026 CISA federal deadline · Overdue by 10 months
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.600 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** This vulnerability affects an open-source component, third-party library, or a protocol used by different products.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
org.geoserver.web:gs-web-app	≥ 2.26.0, < 2.26.2	2.26.2	GitHub
org.geoserver.web:gs-web-app	< 2.25.6	2.25.6	GitHub
org.geoserver:gs-wms	≥ 2.26.0, < 2.26.2	2.26.2	GitHub
org.geoserver:gs-wms	< 2.25.6	2.25.6	GitHub
geoserver	< 2.25.6 ≥ 2.26.0 < 2.26.2	2.25.6 · 2.26.2	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-fjf5-xgmq-5525	Additional guidance	github.com/geoserver/geoserver/security/advisories/GHSA-fjf5-xgmq-5525
osgeo-org.atlassian.net	osgeo-org.atlassian.net/browse/GEOS-11922	NVD	nvd.nist.gov/vuln/detail/CVE-2025-58360
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-199606
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-58360		



Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.