

CVE-2024-36401

OSGeo GeoServer GeoTools Eval Injection Vulnerability

Exigent

CISA KEV since Jul 15, 2024

Actively exploited

Public exploit module (Metasploit)

GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.22.6, 2.23.6, 2.24.4, and 2.25.2, multiple OGC request parameters allow Remote Code Execution (RCE) by unauthenticated users through specially crafted input against a default GeoServer installation due to unsafely evaluating property names as XPath expressions.

EVRS 87/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.998 99.96th percentile · FIRST	CISA DEADLINE Aug 5, 2024 KEV since 2024 · listed over a year
--	--	---	---

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	On the CISA KEV catalog for over two years
☒ EPSS	0.998 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions 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

The GeoTools library API that GeoServer calls evaluates property/attribute names for feature types in a way that unsafely passes them to the commons-jxpath library which can execute arbitrary code when evaluating XPath expressions. This XPath evaluation is intended to be used only by complex feature types (i.e., Application Schema data stores) but is incorrectly being applied to simple feature types as well which makes this vulnerability apply to **ALL** GeoServer instances. No public PoC is provided but this vulnerability has been confirmed to be exploitable through WFS GetFeature, WFS GetPropertyValue, WMS GetMap, WMS GetFeatureInfo, WMS GetLegendGraphic and WPS Execute requests. This vulnerability can lead to executing arbitrary code. Versions 2.22.6, 2.23.6, 2.24.4, and 2.25.2 contain a patch for the issue. A workaround exists by removing the `gt-complex-x.y.jar` file from the GeoServer where `x.y` is the GeoTools version (e.g., `gt-complex-31.1.jar` if running GeoServer 2.25.1). This will remove the vulnerable code from GeoServer but may break some GeoServer functionality or prevent GeoServer from deploying if the gt-complex module is needed.

Affected and fixed versions · GHSA-6jj6-gm7p-fcvv lists 4 more affected packages

PACKAGE	AFFECTED	FIXED IN	SOURCE
org.geoserver.web:gs-web-app	≥ 2.24.0, < 2.24.4	2.24.4	GitHub
org.geoserver.web:gs-web-app	≥ 2.25.0, < 2.25.2	2.25.2	GitHub
org.geoserver.web:gs-web-app	≥ 2.23.0, < 2.23.6	2.23.6	GitHub
org.geoserver:gs-wfs	≥ 2.24.0, < 2.24.4	2.24.4	GitHub
org.geoserver:gs-wfs	≥ 2.25.0, < 2.25.2	2.25.2	GitHub
org.geoserver:gs-wfs	≥ 2.23.0, < 2.23.6	2.23.6	GitHub

PACKAGE	AFFECTED	FIXED IN	SOURCE
org.geoserver:gs-wms	≥ 2.24.0, < 2.24.4	2.24.4	GitHub
org.geoserver:gs-wms	≥ 2.25.0, < 2.25.2	2.25.2	GitHub
geoserver	< 2.22.6 ≥ 2.23.0 < 2.23.6 ≥ 2.24.0 < 2.24.4 ≥ 2.25.0 < 2.25.2	2.22.6 · 2.23.6 · 2.24.4 · 2.25.2	NVD
geotools	< 29.6 ≥ 30.1 < 30.4 ≥ 31.1 < 31.2 30.0 31.0	29.6 · 30.4	NVD

Sources

Vendor guidance	github.com/geotools/geotools/pull/4797	Additional guidance	github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv
github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv , https://github.com/geotools/geotools/pull/4797	github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv , https://github.com/geotools/geotools/pull/4797	NVD	nvd.nist.gov/vuln/detail/CVE-2024-36401
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	GitHub advisory	github.com/advisories/GHSA-6jj6-gm7p-fcvv
ENISA EUVD	europa.eu/enisa/enisa/eu-vulnerability/EUVD-2024-2280	Current data	evulnabile.com/vulnerability-management/cve/CVE-2024-36401

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