



CVE-2023-35042

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-35042
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-12 15:15:00 UTC
Updated	2023-11-07 04:15:00 UTC
Description	** DISPUTED ** GeoServer 2, in some configurations, allows remote attackers to execute arbitrary code via java.lang.Runti

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Geoserver	Geoserver	All	All	All	All

References

Reference	Source	Link	Tags
InfoSec Handlers Diary Blog - SANS Internet Storm Center	MISC	isc.sans.edu	
WPS Operations — GeoServer 2.21.x User Manual	MISC	docs.geoserver.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

995306 Java (Maven) Security Update for org.geoserver:gs-wfs (GHSA-59x6-g4jr-4hxc)

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report