



# GeoNetwork vulnerable to search end-point information disclosure in response headers

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2024-32037
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-02-11 22:15:27 UTC
<b>Updated</b>	2026-04-17 18:08:42 UTC
<b>Description</b>	GeoNetwork is a catalog application to manage spatially referenced resources. In versions prior to 4.2.10 and 4.4.5, the sear

## Risk And Classification

**Primary CVSS:** v3.1 5.3 MEDIUM from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

**EPSS:** 0.009400000 probability, percentile 0.762520000 (date 2026-04-21)

**Problem Types:** CWE-200 | NVD-CWE-noinfo | CWE-200 CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	security-advisories@github.com	Secondary	0	NONE	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
3.1	CNA	DECLARED	0	NONE	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Osgeo	Geonetwork	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Geonetwork	Core-geonetwork	affected < 4.2.10	Not specified
CNA	Geonetwork	Core-geonetwork	affected >= 4.4.0, < 4.4.5	Not specified

### References

Reference	Source	Link
github.com/geonetwork/core-geonetwork/releases/tag/4.2.10	security-advisories@github.com	github.com
github.com/geonetwork/core-geonetwork/security/advisories/GHSA-52rf-25hq...	security-advisories@github.com	github.com
github.com/geonetwork/core-geonetwork/releases/tag/4.4.5	security-advisories@github.com	github.com
docs.geonetwork-opensource.org/4.4/api/search	security-advisories@github.com	docs.geonetwork-opensc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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

