



# CVE-2022-24816

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-24816
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-13 21:15:00 UTC
<b>Updated</b>	2023-02-16 19:08:00 UTC
<b>Description</b>	JAI-EXT is an open-source project which aims to extend the Java Advanced Imaging (JAI) API. Programs allowing Jiffle scr

## Risk And Classification

**EPSS:** 0.937140000 probability, percentile 0.998500000 (date 2026-04-22)

**CISA KEV:** Listed on 2024-06-26; due 2024-07-17; ransomware use Unknown

**Problem Types:** CWE-94

## CISA Known Exploited Vulnerability

<b>Vendor</b>	OSGeo
<b>Product</b>	JAI-EXT
<b>Name</b>	OSGeo GeoServer JAI-EXT Code Injection Vulnerability
<b>Required Action</b>	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
<b>Notes</b>	This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. The patched JAI-EXT is version 1.1.22: <a href="https://github.com/geosolutions-it/jai-ext/releases/tag/1.1.22">https://github.com/geosolutions-it/jai-ext/releases/tag/1.1.22</a> , <a href="https://github.com/geosolutions-it/jai-ext/security/advisories/GHSA-v92f-jx6p-73rx">https://github.com/geosolutions-it/jai-ext/security/advisories/GHSA-v92f-jx6p-73rx</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2022-24816">https://nvd.nist.gov/vuln/detail/CVE-2022-24816</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Geosolutionsgroup</a>	<a href="#">Jai-ext</a>	All	All	All	All
Application	<a href="#">Geosolutionsgroup</a>	<a href="#">Jai-ext</a>	All	All	All	All

## References

Reference	Source	Link
Improper Control of Generation of Code ('Code Injection') in jai-ext · Advisory · geosolutions-it/jai-ext · GitHub	CONFIRM	<a href="#">github.com</a>

validate Jiffle input variable names according to grammar, escape jav...	geosolutions-it/jai-ext@cb1d656 · GitHub	MISC	<a href="https://github.com">github.com</a>
CVE Program record		CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail		NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>
CISA Known Exploited Vulnerabilities catalog		CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [150667](#) GeoServer JAI-EXT Remote Code Execution (RCE) Vulnerability (CVE-2022-24816)
- [730744](#) jai-ext Remote Code Execution (RCE) Vulnerability (GHSA-v92f-jx6p-73rx)
- [995305](#) Java (Maven) Security Update for it.geosolutions.jaiext.jiffle:jt-jiffle (GHSA-v92f-jx6p-73rx)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)