



CVE-2021-31407

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2021-31407 |
| State | PUBLIC |
| Assigner | security@vaadin.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-04-23 16:15:00 UTC |
| Updated | 2022-08-12 18:02:00 UTC |
| Description | Vulnerability in OSGi integration in com.vaadin:flow-server versions 1.2.0 through 2.4.7 (Vaadin 12.0.0 through 14.4.9), and |

Risk And Classification

Problem Types: CWE-668

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Vaadin | Flow | All | All | All | All |
| Application | Vaadin | Vaadin | All | All | All | All |
| Application | Vaadin | Vaadin | 19.0.0 | - | All | All |

References

| Reference |
|---|
| Vaadin OSGi applications should not expose relevant classpath content as static resources · Issue #50 · vaadin/osgi · GitHub |
| fix: avoid exposing ServletContext resources via StaticFileServer (#10261) by denis-anisimov · Pull Request #10269 · vaadin/flow · GitHub |
| CVE-2021-31407: Server classes and resources exposure in OSGi applications using Vaadin 12-14 and 19 |
| refactor: use StaticFileHandler as a service by denis-anisimov · Pull Request #10229 · vaadin/flow · GitHub |
| CVE Program record |
| NVD vulnerability detail |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[982669](#) Java (maven) Security Update for com.vaadin:flow-server (GHSA-25xc-jwfg-39jw)

© [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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)