



CVE-2019-25028

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

Summary

CVE	CVE-2019-25028
State	PUBLIC
Assigner	security@vaadin.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-23 16:15:00 UTC
Updated	2021-05-05 18:09:00 UTC
Description	Missing variable sanitization in Grid component in com.vaadin:vaadin-server versions 7.4.0 through 7.7.19 (Vaadin 7.4.0 through 7.7.19)

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
CVE-2019-25028: Stored cross-site scripting in Grid component in Vaadin 7 and 8	CONFIRM	vaadin.com	
Sanitize caption used in Grid header by ZheSun88 · Pull Request #11644 · vaadin/framework · GitHub	CONFIRM	github.com	
Sanitize caption used in Grid header by TatuLund · Pull Request #11645 · vaadin/framework · GitHub	CONFIRM	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was discovered and responsibly reported by MATE Marketing Technologie

Legacy QID Mappings

982667 Java (maven) Security Update for com.vaadin:vaadin-server (GHSA-q74r-4xw3-ppx9)

© [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](#)