



CVE-2022-3767

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

Summary

CVE	CVE-2022-3767
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-09 23:15:00 UTC
Updated	2023-03-15 16:41:00 UTC
Description	Missing validation in DAST analyzer affecting all versions from 1.11.0 prior to 3.0.32, allows custom request headers to be s

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gitlab	Dynamic Application Security Testing Analyzer	All	All	All	All

References

Reference	Source	Link	Tag
Restrict sending custom request headers to allowed hosts (#377473) · Issues · GitLab.org / GitLab · GitLab	MISC	gitlab.com	
2022/CVE-2022-3767.json · master · GitLab.org / cves · GitLab	CONFIRM	gitlab.com	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

Vendor Comments And Credit

Discovery Credit

LEGACY: This vulnerability has been discovered internally by the GitLab team

Legacy QID Mappings

690975 Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (16f7ec68-5cce-11ed-9be7-454b1dd82c64)

© [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](#)