



CVE-2020-13334

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

Summary

CVE	CVE-2020-13334
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-07 14:15:00 UTC
Updated	2020-10-15 16:17:00 UTC
Description	In GitLab versions prior to 13.2.10, 13.3.7 and 13.4.2, improper authorization checks allow a non-member of a project/group

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

- [Guest users can change the confidentiality attribute on those issues that have been assigned to them \(#195327\) · Issues · GitLab.org / GitLab](#)
- [2020/CVE-2020-13334.json · master · GitLab.org / cves · GitLab](#)
- [HackerOne](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

Vendor Comments And Credit

Discovery Credit

LEGACY: Thanks [0xwintermute](https://hackerone.com/0xwintermute) for reporting this vulnerability through our HackerOne bug bounty program

Legacy QID Mappings

690529 Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (a3495e61-047f-11eb-86ea-001b217b3468)

© [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](#).

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