



CVE-2020-13327

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

Summary

CVE	CVE-2020-13327
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-22 21:15:00 UTC
Updated	2020-11-02 14:58:00 UTC
Description	An issue has been discovered in GitLab Runner affecting all versions starting from 13.4.0 before 13.4.2, all versions starting

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

- [Kubernetes Executor should block `CAP_NET_RAW` capability by default; allow configuration \(#26833\) · Issues · GitLab.org / gitlab-runner · CVE-2020-13327](#)
- [2020/CVE-2020-13327.json · master · GitLab.org / cves · GitLab](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

Vendor Comments And Credit

Discovery Credit

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

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](#)