



CVE-2020-13295

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

Summary

CVE	CVE-2020-13295
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-10 14:15:00 UTC
Updated	2020-08-12 15:16:00 UTC
Description	For GitLab Runner before 13.0.12, 13.1.6, 13.2.3, by replacing dockerd with a malicious server, the Shared Runner is suscep

Risk And Classification

Problem Types: CWE-918

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	Source
2020/CVE-2020-13295.json · master · GitLab.org / cves · GitLab	CONFID
SSRF into Shared Runner, by replacing dockerd with malicious server in Executor (#209096) · Issues · GitLab.org / GitLab · GitLab	MISC
HackerOne	MISC
CVE Program record	CVE.OP
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Thanks [[@lucash-dev](#)](<https://hackerone.com/lucash-dev>) for reporting this vulnerability through our HackerOne bug bounty program

There are currently no legacy QID mappings associated with this CVE.

© [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](#)