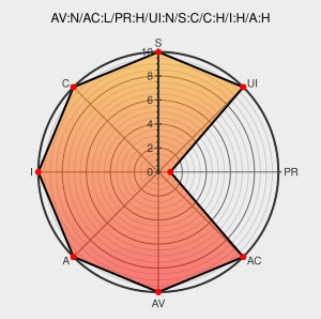
CVE-2020-13347

Published on: 10/07/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-13347

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Gitlab from Gitlab contain the following vulnerability:

A command injection vulnerability was discovered in Gitlab runner versions prior to 13.2.4, 13.3.2 and 13.4.1. When the runner is configured on a Windows system with a docker executor, which allows the attacker to run arbitrary commands on Windows host, via DOCKER_AUTH_CONFIG build variable.

CVE-2020-13347 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **GitLab** - **GitLab Runner** version **>=12.0.0, <13.2.4**

Affected Vendor/Software: **GitLab** - **GitLab Runner** version **>=13.3.0, <13.3.2**

Affected Vendor/Software: **GitLab** - **GitLab Runner** version **>=13.4.0, <13.4.1**

CVSS3 Score: 9.1 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
HackerOne	Permissions Required Third Party Advisory hackerone.com text/html	MISC hackerone.com/reports/955016
2020/CVE-2020-13347.json · master · GitLab.org / cves · GitLab	Vendor Advisory gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13347.json
GitLab-Runner on Windows `DOCKER_AUTH_CONFIG` container host Command Injection (#26725) · Issues · GitLab.org / gitlab-runner · GitLab	Broken Link Vendor Advisory gitlab.com text/html	MISC gitlab.com/gitlab-org/gitlab-runner/-/issues/26725

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:*:

cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*:

cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:*:

cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*:

Discovery Credit

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

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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