

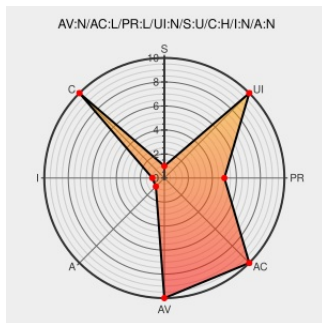


CVE-2020-13324

Published on: 09/29/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:43 PM UTC

CVE-2020-13324

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Gitlab](#) from [Gitlab](#) contain the following vulnerability:

A vulnerability was discovered in GitLab versions prior to 13.1. Under certain conditions the private activity of a user could be exposed via the API.

CVE-2020-13324 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=9.4, <12.10.13**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.0, <13.0.8**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.1, <13.1.2**

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description

Tags

Link

2020/CVE-2020-13324.json · master · GitLab.org / cves · GitLab

Vendor Advisory

gitlab.com

text/html

CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13324.json

User's activity-related personal information are exposed in API event response even enabled private profile (#24542) · Issues · GitLab.org / GitLab · GitLab

Exploit

Vendor Advisory

gitlab.com

text/html

MISC gitlab.com/gitlab-org/gitlab/-/issues/24542

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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

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

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

Discovery Credit

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

← Previous ID

Next ID →