

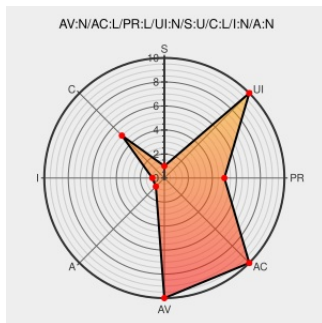


CVE-2020-13357

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

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

CVE-2020-13357

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

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

An issue was discovered in Gitlab CE/EE versions ≥ 13.1 to $<13.4.7$, ≥ 13.5 to $<13.5.5$, and ≥ 13.6 to $<13.6.2$ allowed an unauthorized user to access the user list corresponding to a feature flag in a project.

CVE-2020-13357 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **GitLab** - **GitLab CE/EE** version ≥ 13.1 to $<13.4.7$

Affected Vendor/Software: **GitLab** - **GitLab CE/EE** version ≥ 13.5 to $<13.5.5$

Affected Vendor/Software: **GitLab** - **GitLab CE/EE** version ≥ 13.6 to $<13.6.2$

CVSS3 Score: **4.3 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
HackerOne	Press/Media Coverage hackerone.com text/html	 MISC hackerone.com/reports/962408
2020/CVE-2020-13357.json · master · GitLab.org / cves · GitLab	Vendor Advisory gitlab.com text/html	 CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13357.json
IDOR-Get feature flag user list (including user IDs) of any private/public projects (#241132) · Issues · GitLab.org / GitLab · GitLab	Broken Link gitlab.com text/html	 MISC gitlab.com/gitlab-org/gitlab/-/issues/241132

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.

Related QID Numbers

[690365](#) Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (5d5e5cda-38e6-11eb-bbbf-001b217b3468)

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

[← Previous ID](#)

[Next ID →](#)

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](#)