

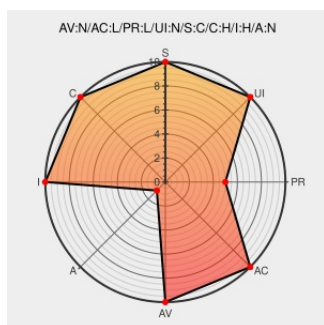


CVE-2020-13292

Published on: 08/10/2020 12:00:00 AM UTC

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

CVE-2020-13292

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

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

In GitLab before 13.0.12, 13.1.6 and 13.2.3, it is possible to bypass E-mail verification which is required for OAuth Flow.

CVE-2020-13292 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=12.3, <13.0.12**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.1, <13.1.6**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.2, <13.2.3**

CVSS3 Score: **9.6 - CRITICAL**

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

CVSS2 Score: **5.5 - MEDIUM**

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

CVE References

Description

HackerOne

Tags

Permissions Required

Third Party Advisory

hackerone.com

text/html

Link

 MISC

hackerone.com/reports/922456

Description

2020/CVE-2020-13292.json · master · GitLab.org / cves · GitLab

Tags

Third Party Advisory

gitlab.com

text/html

Link

 CONFIRM

gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13292.json

Description

Ability to bypass email verification for OAuth grants results in accounts takeovers on 3rd parties (#228629) · Issues · GitLab.org / GitLab · GitLab

Tags

Broken Link

gitlab.com

text/html

Link

 MISC

gitlab.com/gitlab-org/gitlab/-/issues/228629

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

← Previous ID

Next ID →