

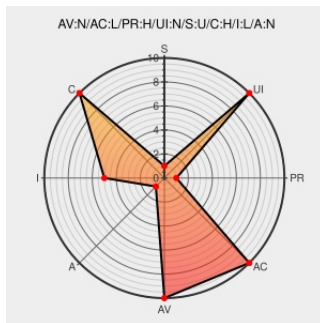


CVE-2021-22263

Published on: 10/11/2021 12:00:00 AM UTC

Last Modified on: 10/18/2021 07:37:00 PM UTC

CVE-2021-22263

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

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

An issue has been discovered in GitLab affecting all versions starting from 13.0 before 14.0.9, all versions starting from 14.1 before 14.1.4, all versions starting from 14.2 before 14.2.2. A user account with 'external' status which is granted 'Maintainer' role on any project on the GitLab instance where 'project tokens' are allowed may elevate its privilege to 'Internal' and access Internal projects.

CVE-2021-22263 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.0, <14.0.9**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.1, <14.1.4**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.2, <14.2.2**

CVSS3 Score: **6.5 - MEDIUM**

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

Privilege escalation of "external user" (with maintainer privilege) to internal access through project token (#331473) · Issues · GitLab.org / GitLab · GitLab

HackerOne

2021/CVE-2021-22263.json · master · GitLab.org / cves · GitLab

Tags

gitlab.com

text/html

hackerone.com

text/html

gitlab.com

text/html

Link

MISC

gitlab.com/gitlab-org/gitlab/-/issues/331473

MISC

hackerone.com/reports/1193062

CONFIRM

gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22263.json

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:*:*:*:community:*:*:

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

Discovery Credit

Thanks @joaxcar for reporting this vulnerability through our HackerOne bug bounty program.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-22263 : An issue has been discovered in GitLab affecting all versions starting from 13.0 before 14.0.9, al... twitter.com/i/web/status/1...	2021-10-11 17:02:53

← Previous ID

Next ID →

