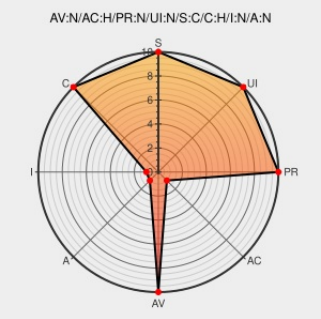
CVE-2021-22175

Published on: 06/11/2021 12:00:00 AM UTC

Last Modified on: 06/21/2021 06:44:00 PM UTC

CVE-2021-22175

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



Certain versions of Gitlab from Gitlab contain the following vulnerability:

When requests to the internal network for webhooks are enabled, a server-side request forgery vulnerability in GitLab affecting all versions starting from 10.5 was possible to exploit for an unauthenticated attacker even on a GitLab instance where registration is disabled

CVE-2021-22175 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=10.5, <13.6.7**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.7, <13.7.7**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.8, <13.8.4**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1059596
2021/CVE-2021-22175.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22175.json
Not Found	gitlab.com text/html Inactive Link Not Archived	MISC gitlab.com/gitlab-org/gitlab/-/issues/294178

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 [@myster](https://hackerone.com/myster?type=user) for reporting this vulnerability through our HackerOne bug bounty program

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Gitlab - CVE-2021-22175: gitlab.com/gitlab-org/git…	2021-06-11 18:15:23

← Previous ID

Next ID→