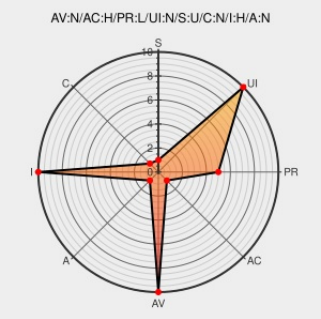
CVE-2021-39909

Published on: 11/04/2021 12:00:00 AM UTC

Last Modified on: 10/06/2022 07:55:00 PM UTC

CVE-2021-39909

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



Certain versions of Gitlab from Gitlab contain the following vulnerability:

Lack of email address ownership verification in the CODEOWNERS feature in all versions of GitLab EE starting from 11.3 before 14.2.6, all versions starting from 14.3 before 14.3.4, and all versions starting from 14.4 before 14.4.1 allows an attacker to bypass CODEOWNERS Merge Request approval requirement under rare circumstances

CVE-2021-39909 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=11.3, <14.2.6**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.3, <14.3.4**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.4, <14.4.1**

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1237750
2021/CVE-2021-39909.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39909.json
Not Found	gitlab.com text/html Inactive Link Not Archived	MISC gitlab.com/gitlab-org/gitlab/-/issues/335191

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

376040 GitLab Multiple Security Vulnerabilities (gitlab release-14.2.6,14.3.4,14.4.1)

690230 Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (33557582-3958-11ec-90ba-001b217b3468)

Exploit/POC from Github

Lack of email address ownership verification in the CODEOWNERS feature in all versions of GitLab EE starting from 11.…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gitlab	Gitlab	All	All	All	All
Application	Gitlab	Gitlab	14.4.0	All	All	All

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

cpe:2.3:a:gitlab:gitlab:14.4.0:*:*:*:enterprise:*:*:*:

Discovery Credit

Thanks vaib25vicky for reporting this vulnerability through our HackerOne bug bounty program

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-39909 : Lack of email address ownership verification in the CODEOWNERS feature in all versions of GitLab E… twitter.com/i/web/status/1…	2021-11-04 23:43:41
@LinInfoSec	Gitlab - CVE-2021-39909: hackerone.com/reports/1237750	2021-11-05 07:56:49

← Previous ID Next ID→

CVE.report and Source URL Uptime Status status.cve.report