

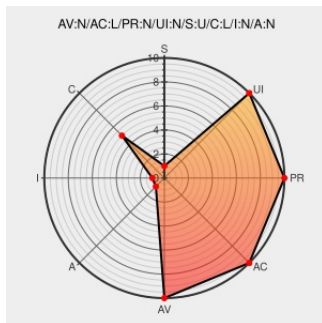


CVE-2021-22257

Published on: 10/05/2021 12:00:00 AM UTC

Last Modified on: 10/09/2021 03:34:00 AM UTC

CVE-2021-22257

[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 14.0 before 14.0.9, all versions starting from 14.1 before 14.1.4, all versions starting from 14.2 before 14.2.2. The route for /user.keys is not restricted on instances with public visibility disabled. This allows user enumeration on such instances.

CVE-2021-22257 has been assigned by [cve@gitlab.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 14.0 , $< 14.0.9$

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 14.1 , $< 14.1.4$

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 14.2 , $< 14.2.2$

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
2021/CVE-2021-22257.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	 CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22257.json
Not Found	gitlab.com text/html Inactive Link Not Archived	 MISC gitlab.com/gitlab-org/gitlab/-/issues/23832

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

375864 GitLab Arbitrary File Read Vulnerability (gitlab-14-2-2, 14-1-4, and 14-0-9)

690050 Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (6c22bb39-0a9a-11ec-a265-001b217b3468)

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

cpe:2.3:a:gitlab:gitlab:*:*:*:community:*:*:

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

Discovery Credit

GitLab would like to thank a customer who reported this issue.

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-22257 : An issue has been discovered in GitLab affecting all versions starting from 14.0 before 14.0.9, al... twitter.com/i/web/status/1...	2021-10-05 14:05:22
 @WesUncensored	New vulnerability on the NVD: CVE-2021-22257 ift.tt/3FhXM87	2021-10-05 16:33:53
 @workentin	New vulnerability on the NVD: CVE-2021-22257 ift.tt/3FhXM87	2021-10-05 16:40:50
 @xanadulinux	CVE-2021-22257 ift.tt/3FhXM87	2021-10-05 16:52:11
 @LinInfoSec	Gitlab - CVE-2021-22257: gitlab.com/gitlab-org/git...	2021-10-05 17:06:18
 @threatmeter	CVE-2021-22257 An issue has been discovered in GitLab affecting all versions starting from 14.0 before 14.0.9, all... twitter.com/i/web/status/1...	2021-10-06 07:09:51

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)