

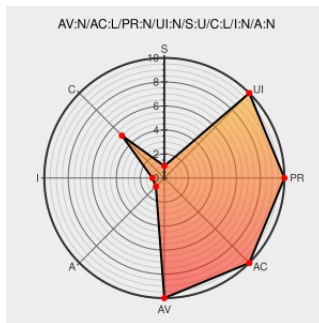


CVE-2022-1352

Published on: Not Yet Published

Last Modified on: 05/19/2022 08:41:00 PM UTC

CVE-2022-1352

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

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

Due to an insecure direct object reference vulnerability in Gitlab EE/CE affecting all versions from 11.0 prior to 14.8.6, 14.9 prior to 14.9.4, and 14.10 prior to 14.10.1, an endpoint may reveal the issue title to a user who crafted an API call with the ID of the issue from a public project that restricts access to issue only to project members.

CVE-2022-1352 has been assigned by [cve@gitlab.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 11.0 , $< 14.8.6$

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 14.9 , $< 14.9.4$

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 14.10 , $< 14.10.1$

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
2022/CVE-2022-1352.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	 CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1352.json
HackerOne	hackerone.com text/html	 MISC hackerone.com/reports/1450306
Not Found	gitlab.com text/html Inactive Link Not Archived	 MISC gitlab.com/gitlab-org/gitlab/-/issues/350691
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	
376605	GitLab Multiple Security Vulnerabilities (gitlab- 14.8.6, 14.9.4, 14.10.1)

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
Application	Gitlab	Gitlab	14.10.0	All	All	All
Application	Gitlab	Gitlab	14.10.0	All	All	All
cpe:2.3:a:gitlab:gitlab:*:*:*:community:*:*:						
cpe:2.3:a:gitlab:gitlab:*:*:*:enterprise:*:*:						
cpe:2.3:a:gitlab:gitlab:14.10.0:*:*:community:*:*:						
cpe:2.3:a:gitlab:gitlab:14.10.0:*:*:enterprise:*:*:						

Discovery Credit	
Thanks [shells3c](https://hackerone.com/shells3c) for reporting this vulnerability through our HackerOne bug bounty program	

Social Mentions		
Source	Title	Posted (UTC)
 @LinInfoSec	Gitlab - CVE-2022-1352: hackerone.com/reports/1450306	2022-05-11 17:06:55
 /r/netcve	CVE-2022-1352	2022-05-11 16:38:34

© [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](#)