

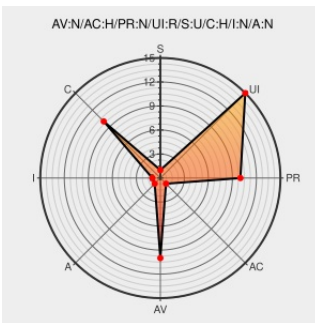


CVE-2022-1148

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

CVE-2022-1148

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

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

Improper authorization in GitLab Pages included with GitLab CE/EE affecting all versions from 11.5 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowed an attacker to steal a user's access token on an attacker-controlled private GitLab Pages website and reuse that token on the victim's other private websites

CVE-2022-1148 has been assigned by [cve@gitlab.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 11.5 , $< 14.7.7$

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 14.8 , $< 14.8.5$

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 14.9 , $< 14.9.2$

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References		
Description	Tags	Link
HackerOne	hackerone.com text/html	 MISC hackerone.com/reports/1439552
2022/CVE-2022-1148.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	 CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1148.json
Not Found	gitlab.com text/html Inactive Link Not Archived	 MISC gitlab.com/gitlab-org/gitlab/-/issues/350687
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	
690828	Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (8657eedd-b423-11ec-9559-001b217b3468)

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

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-1148 : Improper authorization in GitLab Pages included with GitLab CE/EE affecting all versions from 11.5... twitter.com/i/web/status/1...	2022-04-04 20:07:50
 @LinInfoSec	Gitlab - CVE-2022-1148: gitlab.com/gitlab-org/git...	2022-04-04 23:01:45

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](#)