

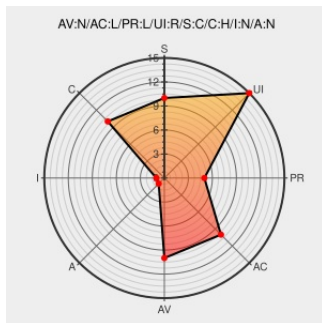


CVE-2021-22238

Published on: 08/20/2021 12:00:00 AM UTC

Last Modified on: 08/26/2021 02:40:00 AM UTC

CVE-2021-22238

[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 with 13.3. GitLab was vulnerable to a stored XSS by using the design feature in issues.

CVE-2021-22238 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.1, <14.1.2**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.0, <14.0.7**

Affected Vendor/Software: **GitLab** - **GitLab** version **>13.3, <13.12.9**

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	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
Not Found	gitlab.com text/html Inactive Link Not Archived	 MISC gitlab.com/gitlab-org/gitlab/-/issues/332420
HackerOne	hackerone.com text/html	 MISC hackerone.com/reports/1212067
2021/CVE-2021-22238.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	 CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22238.json
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-13-12-9, 14-0-7, and 14-1-2)

[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

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

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-22238 : An issue has been discovered in GitLab affecting all versions starting with 13.3. GitLab was vulne... twitter.com/i/web/status/1...	2021-08-20 18:04:57
 @LinInfoSec	Gitlab - CVE-2021-22238: hackerone.com/reports/1212067	2021-08-20 21:10:07
 @threatmeter	CVE-2021-22238 An issue has been discovered in GitLab affecting all versions starting with 13.3. GitLab was vulnera... twitter.com/i/web/status/1...	2021-08-21 07:09:56

[← Previous ID](#)

[Next ID →](#)

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](#)