

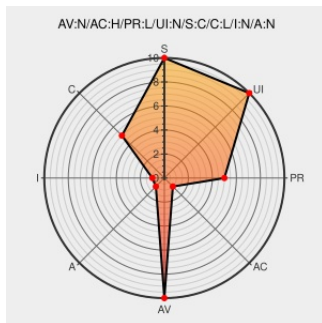


CVE-2022-3331

Published on: Not Yet Published

Last Modified on: 10/20/2022 02:30:00 PM UTC

CVE-2022-3331

[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 EE affecting all versions starting from 14.5 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. GitLab's Zentao integration has an insecure direct object reference vulnerability that may be exploited by an attacker to leak Zentao project issues.

CVE-2022-3331 has been assigned by [cve@gitlab.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [GitLab](#) - **GitLab** version **>=14.5, <15.1.6**

Affected Vendor/Software: [GitLab](#) - **GitLab** version **>=15.2, <15.2.4**

Affected Vendor/Software: [GitLab](#) - **GitLab** version **>=15.3, <15.3.2**

CVSS3 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
HackerOne	hackerone.com text/html	hackerone.com/reports/1542834
IDOR in Zentao integration leaks details of issues from a users other "products" (#360372) · Issues · GitLab.org / GitLab · GitLab	gitlab.com text/html	gitlab.com/gitlab-org/gitlab/-/issues/360372
2022/CVE-2022-3331.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3331.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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gitlab	Gitlab	All	All	All	All
cpe:2.3:a:gitlab:gitlab:*:*:*:enterprise:*:*:						

Discovery Credit

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

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-3331 : An issue has been discovered in GitLab EE affecting all versions starting from 14.5 before 15.1.6,... twitter.com/i/web/status/1...	2022-10-17 16:10:05
 /r/netcve	CVE-2022-3331	2022-10-17 17:38:32

[← Previous ID](#)

[Next ID →](#)

© 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