

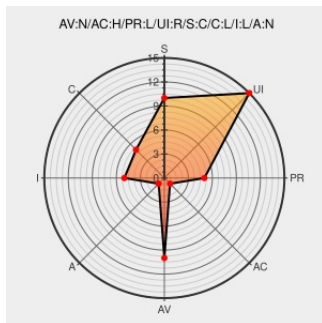


CVE-2022-2500

Published on: Not Yet Published

Last Modified on: 08/11/2022 03:19:00 PM UTC

CVE-2022-2500

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

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

A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions before 15.0.5, 15.1 prior to 15.1.4, and 15.2 prior to 15.2.1. A stored XSS flaw in job error messages allows attackers to perform arbitrary actions on behalf of victims at client side.

CVE-2022-2500 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **GitLab** - **GitLab** version ≥ 0.0 , $< 15.0.5$

Affected Vendor/Software: **GitLab** - **GitLab** version ≥ 15.1 , $< 15.1.4$

Affected Vendor/Software: **GitLab** - **GitLab** version ≥ 15.2 , $< 15.2.1$

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

CVE References

Description	Tags	Link
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1579645
2022/CVE-2022-2500.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-2500.json
Not Found	gitlab.com text/html Inactive Link Not Archived	MISC gitlab.com/gitlab-org/gitlab/-/issues/363725

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

[690905](#) Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (4c26f668-0fd2-11ed-a83d-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
Application	Gitlab	Gitlab	15.2	All	All	All
Application	Gitlab	Gitlab	15.2	All	All	All
cpe:2.3:a:gitlab:gitlab:*.~*.~*.community:~*.~*:						
cpe:2.3:a:gitlab:gitlab:*.~*.~*.enterprise:~*.~*:						
cpe:2.3:a:gitlab:gitlab:15.2.~*.~*.community:~*.~*:						
cpe:2.3:a:gitlab:gitlab:15.2.~*.~*.enterprise:~*.~*:						

Discovery Credit

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

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-2500 : A cross-site scripting issue has been discovered in GitLab CE/EE affecting all versions before 15.0... twitter.com/i/web/status/1...	2022-08-05 16:23:19

[← Previous ID](#)

[Next ID →](#)