

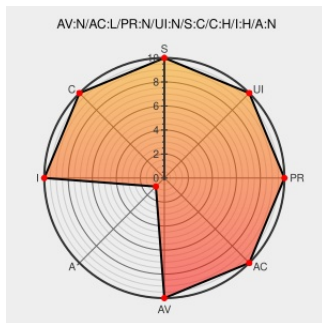


CVE-2023-2825

Published on: Not Yet Published

Last Modified on: 05/29/2023 03:52:00 AM UTC

CVE-2023-2825

[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 CE/EE affecting only version 16.0.0. An unauthenticated malicious user can use a path traversal vulnerability to read arbitrary files on the server when an attachment exists in a public project nested within at least five groups.

CVE-2023-2825 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **16.0.0**

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
2023/CVE-2023-2825.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2825.json
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1994725
Not Found	gitlab.com text/html Inactive Link Not Archived	MISC gitlab.com/gitlab-org/gitlab/-/issues/412371

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

Related QID Numbers

[378519](#) GitLab Path Traversal Vulnerability (CVE-2023-2825)

Exploit/POC from Github

On May 23, 2023 GitLab released version 16.0.1 which fixed a critical vulnerability, CVE-2023-2825, affecting the Com...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gitlab	Gitlab	16.0.0	All	All	All
Application	Gitlab	Gitlab	16.0.0	All	All	All
cpe:2.3:a:gitlab:gitlab:16.0.0:*:*:*:community:*:*:						
cpe:2.3:a:gitlab:gitlab:16.0.0:*:*:*:enterprise:*:*:						

Discovery Credit

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

Social Mentions

Source	Title	Posted (UTC)
 @benhabing	.@KrollWire is tracking CVE-2023-2825, vulnerability discovered in #GitLab Community and Enterprise Edition that al... twitter.com/i/web/status/1...	2023-06-15 22:47:11
 @CyberAlliance	Thank you @JuniperNetworks @Mounirhahad for the Early Share with @CyberAlliance Members: CVE-2023-2825: Gitlab Arbi... twitter.com/i/web/status/1...	2023-06-30 13:02:37
 /r/Action1	June 2023 Patch Tuesday	2023-06-13 17:30:55

[← Previous ID](#)[Next ID →](#)