

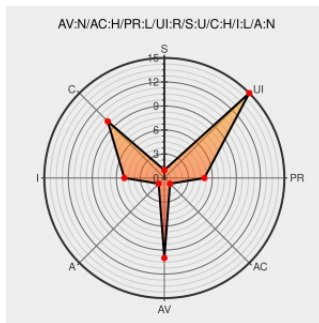


CVE-2022-1944

Published on: Not Yet Published

Last Modified on: 06/13/2022 06:37:00 PM UTC

CVE-2022-1944

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

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

When the feature is configured, improper authorization in the Interactive Web Terminal in GitLab CE/EE affecting all versions from 11.3 prior to 14.9.5, 14.10 prior to 14.10.4, and 15.0 prior to 15.0.1 allows users with the Developer role to open terminals on other Developers' running jobs

CVE-2022-1944 has been assigned by [cve@gitlab.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 11.3 , $< 14.9.5$

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 14.10 , $< 14.10.4$

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 15.0 , $< 15.0.1$

CVSS3 Score: **7.1 - HIGH**

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

CVSS2 Score: **4.9 - MEDIUM**

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

CVE References

Description	Tags	Link
Not Found	gitlab.com text/html Inactive Link Not Archived	 MISC gitlab.com/gitlab-org/gitlab/-/issues/349750
2022/CVE-2022-1944.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	 CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1944.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

[376655](#) GitLab Multiple Security Vulnerabilities (gitlab- 15.0.1, 14.10.4, and 14.9.5)

[690874](#) Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (f414d69f-e43d-11ec-9ea4-001b217b3468)

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	15.0.0	All	All	All
Application	Gitlab	Gitlab	15.0.0	All	All	All
cpe:2.3:a:gitlab:gitlab:*:*:*:community:*:*:						
cpe:2.3:a:gitlab:gitlab:*:*:*:enterprise:*:*:						
cpe:2.3:a:gitlab:gitlab:15.0.0:*:*:*:community:*:*:						
cpe:2.3:a:gitlab:gitlab:15.0.0:*:*:*:enterprise:*:*:						

Discovery Credit

This vulnerability has been discovered internally by the GitLab team

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-1944 : When the feature is configured, improper authorization in the Interactive Web Terminal in GitLab CE... twitter.com/i/web/status/1...	2022-06-06 17:06:36
 /r/netcve	CVE-2022-1944	2022-06-06 18:38:19

[← 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](#)