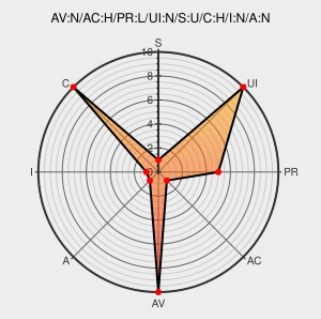
CVE-2021-39947

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:22:00 PM UTC

CVE-2021-39947

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Gitlab Runner from Gitlab contain the following vulnerability:

In specific circumstances, trace file buffers in GitLab Runner versions up to 14.3.4, 14.4 to 14.4.2, and 14.5 to 14.5.2 would re-use the file descriptor 0 for multiple traces and mix the output of several jobs

CVE-2021-39947 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **GitLab** - **GitLab Runner** version **<14.3.4**

Affected Vendor/Software: **GitLab** - **GitLab Runner** version **>=14.4, <14.4.2**

Affected Vendor/Software: **GitLab** - **GitLab Runner** version **>=14.5, <14.5.2**

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	NONE	HIGH	NONE

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
2021/CVE-2021-39947.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39947.json
Not Found	gitlab.com text/html Inactive Link Not Archived	MISC gitlab.com/gitlab-org/gitlab-runner/-/issues/28732

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 Runner	All	All	All	All

cpe:2.3:a:gitlab:gitlab_runner:*:*:*:*:*:*:*:*:

Discovery Credit

This vulnerability has been discovered internally by the GitLab team

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-39947 : In specific circumstances, trace file buffers in GitLab Runner versions up to 14.3.4, 14.4 to 14.4… twitter.com/i/web/status/1…	2022-06-06 17:09:47
@wvdsteen	New vulnerability on the NVD: CVE-2021-39947 ift.tt/g0ITLUQ June 07, 2022 at 05:15AM	2022-06-06 18:16:55
@WesUncensored	New vulnerability on the NVD: CVE-2021-39947 ift.tt/g0ITLUQ	2022-06-06 18:33:08
/r/netcve	CVE-2021-39947	2022-06-06 18:38:27

← Previous ID Next ID→