

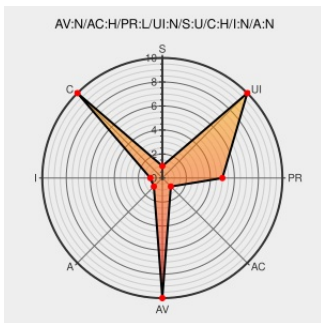


# CVE-2021-39947

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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>HIGH</b>         | <b>NONE</b>         |

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>PARTIAL</b>    | <b>NONE</b>         |

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](https://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](https://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](mailto: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                            | <a href="#">Gitlab</a> | <a href="#">Gitlab Runner</a> | 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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-06-06 17:09:47 |
|  @wvdsteen      | New vulnerability on the NVD: CVE-2021-39947 <a href="https://ift.tt/g0ITLUQ">ift.tt/g0ITLUQ</a> June 07, 2022 at 05:15AM                                                                                | 2022-06-06 18:16:55 |
|  @WesUncensored | New vulnerability on the NVD: CVE-2021-39947 <a href="https://ift.tt/g0ITLUQ">ift.tt/g0ITLUQ</a>                                                                                                         | 2022-06-06 18:33:08 |
|  /r/netcve      | <a href="#">CVE-2021-39947</a>                                                                                                                                                                           | 2022-06-06 18:38:27 |

← 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](#)