

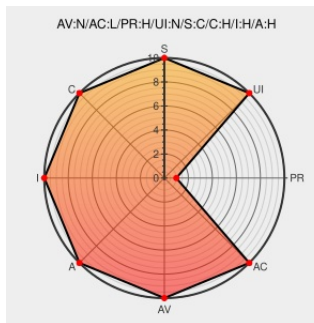


# CVE-2020-13347

Published on: 10/07/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

## CVE-2020-13347

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

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

A command injection vulnerability was discovered in Gitlab runner versions prior to 13.2.4, 13.3.2 and 13.4.1. When the runner is configured on a Windows system with a docker executor, which allows the attacker to run arbitrary commands on Windows host, via DOCKER\_AUTH\_CONFIG build variable.

CVE-2020-13347 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **GitLab - GitLab Runner** version **>=12.0.0, <13.2.4**

Affected Vendor/Software: **GitLab - GitLab Runner** version **>=13.3.0, <13.3.2**

Affected Vendor/Software: **GitLab - GitLab Runner** version **>=13.4.0, <13.4.1**

CVSS3 Score: **9.1 - CRITICAL**

| Attack Vector  | Attack Complexity      | Privileges Required | User Interaction    |
|----------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b> | <b>LOW</b>             | <b>HIGH</b>         | <b>NONE</b>         |
| Scope          | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>CHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **9 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>SINGLE</b>       |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>COMPLETE</b>        | <b>COMPLETE</b>   | <b>COMPLETE</b>     |

## CVE References

| Description                                                                                                                            | Tags                                                                                                                                       | Link                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HackerOne                                                                                                                              | <a href="#">Permissions Required</a><br><a href="#">Third Party Advisory</a><br><a href="#">hackerone.com</a><br><a href="#">text/html</a> |  MISC<br><a href="https://hackerone.com/reports/955016">hackerone.com/reports/955016</a>                                                                           |
| 2020/CVE-2020-13347.json · master · GitLab.org / cves · GitLab                                                                         | <a href="#">Vendor Advisory</a><br><a href="#">gitlab.com</a><br><a href="#">text/html</a>                                                 |  CONFIRM <a href="https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13347.json">gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13347.json</a> |
| GitLab-Runner on Windows `DOCKER_AUTH_CONFIG` container host Command Injection (#26725) · Issues · GitLab.org / gitlab-runner · GitLab | <a href="#">Broken Link</a><br><a href="#">Vendor Advisory</a><br><a href="#">gitlab.com</a><br><a href="#">text/html</a>                  |  MISC <a href="https://gitlab.com/gitlab-org/gitlab-runner/-/issues/26725">gitlab.com/gitlab-org/gitlab-runner/-/issues/26725</a>                                  |

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</a> | All     | All    | All     | All      |
| Application                                   | <a href="#">Gitlab</a> | <a href="#">Gitlab</a> | All     | All    | All     | All      |
| Application                                   | <a href="#">Gitlab</a> | <a href="#">Gitlab</a> | All     | All    | All     | All      |
| Application                                   | <a href="#">Gitlab</a> | <a href="#">Gitlab</a> | All     | All    | All     | All      |
| cpe:2.3:a:gitlab:gitlab:*:*:*:community:*:*:  |                        |                        |         |        |         |          |
| cpe:2.3:a:gitlab:gitlab:*:*:*:enterprise:*:*: |                        |                        |         |        |         |          |
| cpe:2.3:a:gitlab:gitlab:*:*:*:community:*:*:  |                        |                        |         |        |         |          |
| cpe:2.3:a:gitlab:gitlab:*:*:*:enterprise:*:*: |                        |                        |         |        |         |          |

## Discovery Credit

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

[← Previous ID](#)

[Next ID →](#)

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](#)