

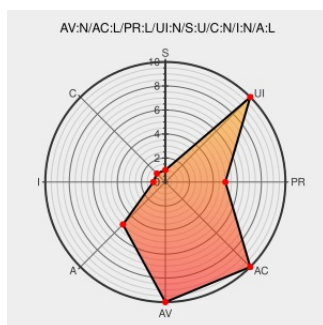


CVE-2022-1174

Published on: Not Yet Published

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

CVE-2022-1174

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

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

A potential DoS vulnerability was discovered in Gitlab CE/EE versions 13.7 before 14.7.7, all versions starting from 14.8 before 14.8.5, all versions starting from 14.9 before 14.9.2 allowed an attacker to trigger high CPU usage via a special crafted input added in Issues, Merge requests, Milestones, Snippets, Wiki pages, etc.

CVE-2022-1174 has been assigned by [cve@gitlab.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 13.7 , $< 14.7.7$

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 14.8 , $< 14.8.5$

Affected Vendor/Software: [GitLab](#) - **GitLab** version ≥ 14.9 , $< 14.9.2$

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	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Not Found	gitlab.com text/html Inactive Link Not Archived	 MISC gitlab.com/gitlab-org/gitlab/-/issues/338721
HackerOne	hackerone.com text/html	 MISC hackerone.com/reports/1305431
2022/CVE-2022-1174.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	 CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1174.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

690828 Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (8657eedd-b423-11ec-9559-001b217b3468)

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

cpe:2.3:a:gitlab:gitlab:*:*:*:community:*:*:

cpe:2.3:a:gitlab:gitlab:*:*:*:enterprise:*:*:

Discovery Credit

Thanks [scaramouche31](https://hackerone.com/scaramouche31) for reporting this vulnerability through our HackerOne bug bounty program

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-1174 : A potential #DoS vulnerability was discovered in Gitlab CE/EE versions 13.7 before 14.7.7, all vers... twitter.com/i/web/status/1...	2022-04-04 20:08:40
 @LinInfoSec	Gitlab - CVE-2022-1174: gitlab.com/gitlab-org/cve...	2022-04-04 23:01:45
 /r/netcve	CVE-2022-1174	2022-04-04 20:38:55

← Previous ID

Next ID →

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](#)