

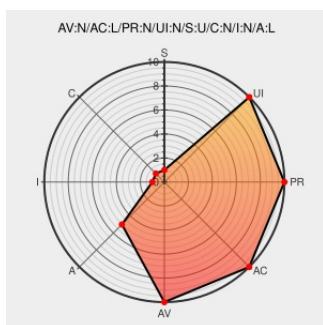


CVE-2022-3285

Published on: Not Yet Published

Last Modified on: 11/11/2022 01:06:00 AM UTC

CVE-2022-3285

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

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

Bypass of healthcheck endpoint allow list affecting all versions from 12.0 prior to 15.2.5, 15.3 prior to 15.3.4, and 15.4 prior to 15.4.1 allows an unauthorized attacker to prevent access to GitLab

CVE-2022-3285 has been assigned by [cve@gitlab.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [GitLab](#) - **GitLab** version **>=12.0, <15.2.5**

Affected Vendor/Software: [GitLab](#) - **GitLab** version **>=15.3, <15.3.4**

Affected Vendor/Software: [GitLab](#) - **GitLab** version **>=15.4, <15.4.1**

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

CVE References

Description	Tags	Link
Checking your Browser - GitLab	gitlab.com text/html Inactive Link Not Archived	MISC gitlab.com/gitlab-org/security/omnibus-gitlab/-/issues/64
2022/CVE-2022-3285.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3285.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 purposes. CVEreport does not necessarily endorse the views expressed, or agree with the facts presented on these sites. Further

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

690950 Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (04422df1-40d8-11ed-9be7-454b1dd82c64)

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	15.4.0	All	All	All
Application	Gitlab	Gitlab	15.4.0	All	All	All
cpe:2.3:a:gitlab:gitlab:*:*:*:community:*:*:						
cpe:2.3:a:gitlab:gitlab:*:*:*:enterprise:*:*:						
cpe:2.3:a:gitlab:gitlab:15.4.0:*:*:community:*:*:						
cpe:2.3:a:gitlab:gitlab:15.4.0:*:*:enterprise:*:*:						

Discovery Credit

This vulnerability has been discovered internally by the GitLab team

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-3285 : Bypass of healthcheck endpoint allow list affecting all versions from 12.0 prior to 15.2.5, 15.3 pr... twitter.com/i/web/status/1...	2022-11-09 23:04:36
 /r/netcve	CVE-2022-3285	2022-11-10 00:38:28

[← 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](#)