

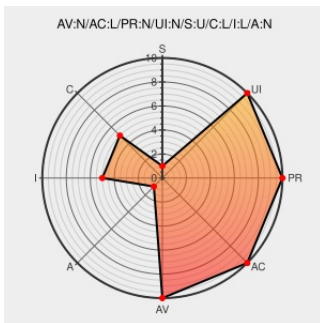


CVE-2020-13312

Published on: 09/14/2020 12:00:00 AM UTC

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

CVE-2020-13312

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

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

A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab OAuth endpoint was vulnerable to brute-force attacks through a specific parameter.

CVE-2020-13312 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=7.7, <13.1.10**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.2, <13.2.8**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.3, <13.3.4**

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link																																			
Not Found	Broken Link gitlab.com text/html Inactive Link Not Archived	 MISC gitlab.com/gitlab-org/gitlab/-/issues/29746																																			
2020/CVE-2020-13312.json · master · GitLab.org / cves · GitLab	Vendor Advisory gitlab.com text/html	 CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13312.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.																																					
There are currently no QIDs associated with this CVE																																					
Known Affected Configurations (CPE V2.3) <table><tr><th>Type</th><th>Vendor</th><th>Product</th><th>Version</th><th>Update</th><th>Edition</th><th>Language</th></tr><tr><td>Application</td><td>Gitlab</td><td>Gitlab</td><td>All</td><td>All</td><td>All</td><td>All</td></tr><tr><td>Application</td><td>Gitlab</td><td>Gitlab</td><td>All</td><td>All</td><td>All</td><td>All</td></tr><tr><td>Application</td><td>Gitlab</td><td>Gitlab</td><td>All</td><td>All</td><td>All</td><td>All</td></tr><tr><td>Application</td><td>Gitlab</td><td>Gitlab</td><td>All</td><td>All</td><td>All</td><td>All</td></tr></table> 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:*:*:			Type	Vendor	Product	Version	Update	Edition	Language	Application	Gitlab	Gitlab	All	All	All	All	Application	Gitlab	Gitlab	All	All	All	All	Application	Gitlab	Gitlab	All	All	All	All	Application	Gitlab	Gitlab	All	All	All	All
Type	Vendor	Product	Version	Update	Edition	Language																															
Application	Gitlab	Gitlab	All	All	All	All																															
Application	Gitlab	Gitlab	All	All	All	All																															
Application	Gitlab	Gitlab	All	All	All	All																															
Application	Gitlab	Gitlab	All	All	All	All																															
Discovery Credit This vulnerability has been discovered internally by the GitLab team																																					
← Previous ID Next ID →																																					