



CVE-2019-10114

Published on: 05/16/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:39 PM UTC

CVE-2019-10114

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

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

An Information Exposure issue (issue 2 of 2) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. During the OAuth authentication process, the application attempts to validate a parameter in an insecure way, potentially exposing data.

CVE-2019-10114 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

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	HIGH	NONE	NONE

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
Releases GitLab	Release Notes Vendor Advisory about.gitlab.com	about.gitlab.com/blog/categories/releases/

GitLab Security Release: 11.9.4, 11.8.6, and 11.7.10 GitLab	text/html	
	Release Notes	MISC
	Vendor Advisory	about.gitlab.com/2019/04/01/security-release-gitlab-11-dot-9-dot-4-released/
	about.gitlab.com	
2019 Q1 Recurity Assessment: Information Exposure Through Timing Discrepancy (#9729) · Issues · GitLab.org / GitLab Enterprise Edition · GitLab	text/html	
	Exploit	MISC gitlab.com/gitlab-org/gitlab-ee/issues/9729
	Vendor Advisory	
	gitlab.com	
	text/html	

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)

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
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:*:*:						

No vendor comments have been submitted for this CVE