

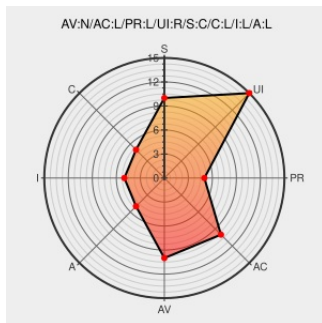


CVE-2020-13329

Published on: 09/29/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:42 PM UTC

CVE-2020-13329

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

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

An issue has been discovered in GitLab affecting versions from 12.6.2 prior to 12.10.13. GitLab was vulnerable to a stored XSS by in the blob view feature.

CVE-2020-13329 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=12.6.2, <12.10.13**

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	LOW

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Stored XSS in blob viewer (#208685) · Issues · GitLab.org / GitLab · GitLab	Exploit Vendor Advisory gitlab.com	MISC gitlab.com/gitlab-org/gitlab/-/issues/208685

