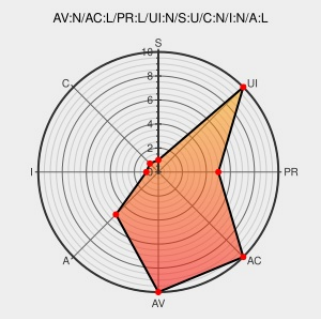
CVE-2020-26409

Published on: 12/10/2020 12:00:00 AM UTC

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

CVE-2020-26409

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Gitlab from Gitlab contain the following vulnerability:

A DOS vulnerability exists in Gitlab CE/EE >=10.3, <13.4.7,>=13.5, <13.5.5,>=13.6, <13.6.2 that allows an attacker to trigger uncontrolled resource by bypassing input validation in markdown fields.

CVE-2020-26409 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Uncontrolled Resource Consumption in any Markdown field using Mermaid (#259626) · Issues · GitLab.org / GitLab · GitLab	Broken Link, gitlab.com, text/html	MISC gitlab.com/gitlab-org/gitlab/-/issues/259626
2020/CVE-2020-26409.json · master · GitLab.org / cves · GitLab	Vendor Advisory	CONFIRM gitlab.com/gitlab-

	gitlab.com text/html	org/cves/-/blob/master/2020/CVE-2020-26409.json
HackerOne	Permissions Required hackerone.com text/html	MISC hackerone.com/reports/990461

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

690365 Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (5d5e5cda-38e6-11eb-bbbf-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
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:*:*:*:

Discovery Credit

Thanks [misha98857](https://hackerone.com/misha98857) for reporting this vulnerability through our HackerOne bug bounty program

← Previous ID

Next ID→