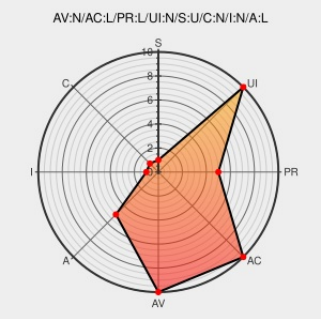
CVE-2020-26411

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

Last Modified on: 03/23/2021 11:23:55 PM UTC

CVE-2020-26411

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



Certain versions of Gitlab from Gitlab contain the following vulnerability:

A potential DOS vulnerability was discovered in all versions of Gitlab starting from 13.4.x (>=13.4 to <13.4.7, >=13.5 to <13.5.5, and >=13.6 to <13.6.2). Using a specific query name for a project search can cause statement timeouts that can lead to a potential DOS if abused.

CVE-2020-26411 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.4, <13.4.7**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.5, <13.5.5**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.6, <13.6.2**

CVSS3 Score: 4.3 - MEDIUM

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

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
2020/CVE-2020-26411.json · master · GitLab.org / cves · GitLab	Third Party Advisory gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-26411.json
A query for name=%13 on the explore causes statement timeouts (#260330) · Issues · GitLab.org / GitLab · GitLab	Broken Link Third Party Advisory gitlab.com text/html	MISC gitlab.com/gitlab-org/gitlab/-/issues/260330

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

cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:*:

cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:*:

Discovery Credit

This vulnerability has been discovered internally by the GitLab team

← Previous ID

Next ID→