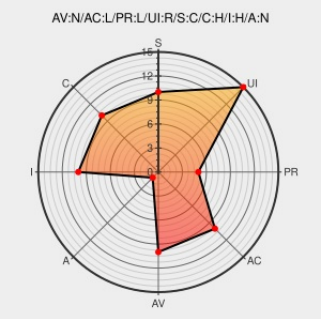
CVE-2021-39906

Published on: 11/04/2021 12:00:00 AM UTC

Last Modified on: 11/17/2021 09:38:19 PM UTC

CVE-2021-39906

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



Certain versions of Gitlab from Gitlab contain the following vulnerability:

Improper validation of ipynb files in GitLab CE/EE version 13.5 and above allows an attacker to execute arbitrary JavaScript code on the victim's behalf.

CVE-2021-39906 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=13.5, <14.2.6**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.3, <14.3.4**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.4, <14.4.1**

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
2021/CVE-2021-39906.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39906.json
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/1347600
Not Found	gitlab.com text/html Inactive Link Not Archived	MISC gitlab.com/gitlab-org/gitlab/-/issues/341566

Related QID Numbers

376040 GitLab Multiple Security Vulnerabilities (gitlab release-14.2.6,14.3.4,14.4.1)

690230 Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (33557582-3958-11ec-90ba-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:*:*:*:*:community:*:*:*:

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

Discovery Credit

Thanks @saleemrashid for reporting this vulnerability through our HackerOne bug bounty program

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-39906 : Improper validation of ipynb files in GitLab CE/EE version 13.5 and above allows an attacker to ex… twitter.com/i/web/status/1…	2021-11-04 23:43:11
@LinInfoSec	Gitlab - CVE-2021-39906: gitlab.com/gitlab-org/git…	2021-11-05 07:56:48
@circl_lu	CVE-2021-39901 CVE-2021-39902 CVE-2021-39903 CVE-2021-39904 CVE-2021-39905 CVE-2021-39906 CVE-2021-39907 CVE-2021-3… twitter.com/i/web/status/1…	2021-11-05 10:09:08

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report