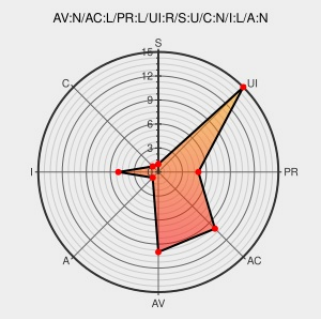
CVE-2021-39881

Published on: 10/05/2021 12:00:00 AM UTC

Last Modified on: 10/09/2021 03:31:00 AM UTC

CVE-2021-39881

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



Certain versions of Gitlab from Gitlab contain the following vulnerability:

In all versions of GitLab CE/EE since version 7.7, the application may let a malicious user create an OAuth client application with arbitrary scope names which may allow the malicious user to trick unsuspecting users to authorize the malicious client application using the spoofed scope name and description.

CVE-2021-39881 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=7.7, <14.1.7**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.2, <14.2.5**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.3, <14.3.1**

CVSS3 Score: 3.5 - LOW

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

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
HackerOne	hackerone.com text/html	MISC hackerone.com/reports/494530
Not Found	gitlab.com text/html Inactive Link Not Archived	MISC gitlab.com/gitlab-org/gitlab/-/issues/26695
2021/CVE-2021-39881.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-39881.json

Related QID Numbers

376097 GitLab Multiple Security Vulnerabilities (gitlab- 14.3.1, 14.2.5, 14.1.7)

690021 Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (1bdd4db6-2223-11ec-91be-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 @executor for reporting this vulnerability through our HackerOne bug bounty program

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-39881 : In all versions of GitLab CE/EE since version 7.7, the application may let a malicious user create… twitter.com/i/web/status/1…	2021-10-05 14:07:42
@LinInfoSec	Gitlab - CVE-2021-39881: hackerone.com/reports/494530	2021-10-05 17:06:20

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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