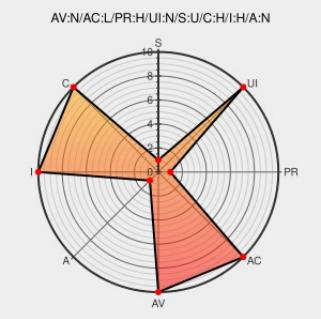
CVE-2022-1936

Published on: Not Yet Published

Last Modified on: 06/13/2022 06:27:00 PM UTC

CVE-2022-1936

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



Certain versions of Gitlab from Gitlab contain the following vulnerability:

Incorrect authorization in GitLab EE affecting all versions from 12.0 before 14.9.5, all versions starting from 14.10 before 14.10.4, all versions starting from 15.0 before 15.0.1 allowed an attacker already in possession of a valid Project Deploy Token to misuse it from any location even when IP address restrictions were configured

CVE-2022-1936 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=15.0.0, <15.0.1**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.10.0, <14.10.4**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=12.0.0, <14.9.5**

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	HIGH	NONE

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Not Found	gitlab.com text/html Inactive Link Not Archived	MISC gitlab.com/gitlab-org/gitlab/-/issues/363638
2022/CVE-2022-1936.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1936.json

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

376655 GitLab Multiple Security Vulnerabilities (gitlab- 15.0.1, 14.10.4, and 14.9.5)

690874 Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (f414d69f-e43d-11ec-9ea4-001b217b3468)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gitlab	Gitlab	All	All	All	All
Application	Gitlab	Gitlab	15.0.0	All	All	All

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

cpe:2.3:a:gitlab:gitlab:15.0.0:*:*:*:enterprise:*:*:*:

Discovery Credit

This was reported by a customer through our Responsible Vulnerability Disclosure process

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-1936 : Incorrect authorization in GitLab EE affecting all versions from 12.0 before 14.9.5, all versions s… twitter.com/i/web/status/1…	2022-06-06 17:05:40
@threatmeter	CVE-2022-1936 Incorrect authorization in GitLab EE affecting all versions from 12.0 before 14.9.5, all versions sta… twitter.com/i/web/status/1…	2022-06-07 07:09:16
@RemotelyAlerts	Severity: ?? | Incorrect authorization in GitLab EE aff... | CVE-2022-1936 | Link for more: alerts.remotelyrmm.com/CVE-2022-1936	2022-06-13 19:28:25
/r/netcve	CVE-2022-1936	2022-06-06 18:38:17

← Previous ID

Next ID→

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