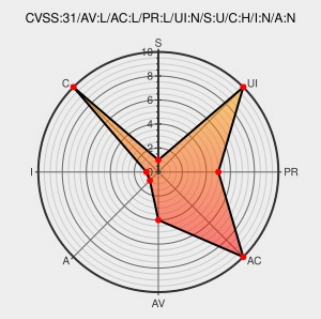
CVE-2020-10977

Published on: 04/08/2020 12:00:00 AM UTC

Last Modified on: 10/06/2022 08:51:00 PM UTC

CVE-2020-10977

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



Certain versions of Gitlab from Gitlab contain the following vulnerability:

GitLab EE/CE 8.5 to 12.9 is vulnerable to a an path traversal when moving an issue between projects.

CVE-2020-10977 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
GitLab Security Release: 12.9.1, 12.8.8, and 12.7.8 | GitLab	Vendor Advisory about.gitlab.com text/html	CONFIRM about.gitlab.com/releases/2020/03/26/security-release-12-dot-9-dot-1-released/
GitLab File Read Remote Code Execution ≈	packetstormsecurity.com	MISC packetstormsecurity.com/files/160441/GitLab-File-Read-

Packet Storm	text/html	Remote-Code-Execution.html
Releases | GitLab	Release Notes Vendor Advisory about.gitlab.com text/html	MISC about.gitlab.com/releases/categories/releases/

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.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

authenticated arbitrary file read for Gitlab (CVE-2020-10977)

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:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ? | GitLab EE/CE 8.5 to 12.9 is vulnerable t... | CVE-2020-10977 | Link for more: alerts.remotelyrmm.com/CVE-2020-10977	2022-10-06 22:31:39

← Previous ID

Next ID→