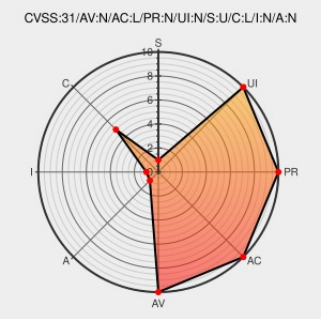
CVE-2020-10086

Published on: 03/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:33 PM UTC

CVE-2020-10086

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



Certain versions of Gitlab from Gitlab contain the following vulnerability:

GitLab 10.4 through 12.8.1 allows Directory Traversal. A particular endpoint was vulnerable to a directory traversal vulnerability, leading to arbitrary file read.

CVE-2020-10086 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
GitLab Security Release: 12.8.2, 12.7.7, and 12.6.8 | GitLab	Release Notes, Vendor Advisory, about.gitlab.com, text/html	CONFIRM about.gitlab.com/releases/2020/03/04/gitlab-12-dot-8-dot-2-released/index.html

GitLab Security Release: 12.8.2, 12.7.7, and 12.6.8 | GitLab	Release Notes Vendor Advisory about.gitlab.com text/html	MISC about.gitlab.com/releases/2020/03/04/gitlab-12-dot-8-dot-2-released/

There are currently no QIDs associated with this CVE

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

← Previous ID

Next ID→