CVE-2020-26412

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-26412
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-11 04:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	Removed group members were able to use the To-Do functionality to retrieve updated information on confidential epics sta

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Lin
Removed group user can check confidential EPIC updates using TODOS (#228670) · Issues · GitLab.org / GitLab · GitLab	MISC	gitl
2020/CVE-2020-26412.json · master · GitLab.org / cves · GitLab	CONFIRM	gitl
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

Vendor Comments And Credit

Discovery Credit

LEGACY: This vulnerability has been discovered internally by the GitLab team

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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