CVE-2020-13262

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

Summary

CVE	CVE-2020-13262
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-19 22:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	Client-Side code injection through Mermaid markup in GitLab CE/EE 12.9 and later through 13.0.1 allows a specially crafte

Risk And Classification

Problem Types: CWE-74

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
Application	Gitlab	Gitlab	13.0.0	All	All	All
Application	Gitlab	Gitlab	13.0.0	All	All	All
Application	Gitlab	Gitlab	All	All	All	All
Application	Gitlab	Gitlab	All	All	All	All
Application	Gitlab	Gitlab	13.0.0	All	All	All
Application	Gitlab	Gitlab	13.0.0	All	All	All

References

Reference	Source	Link	Tag
Send arbitrary PUT requests when user clicks on a link (#211949) · Issues · GitLab.org / GitLab · GitLab	MISC	gitlab.com	Brol
2020/CVE-2020-13262.json · master · GitLab.org / cves · GitLab	CONFIRM	gitlab.com	Ven
HackerOne	MISC	hackerone.com	Per
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

Vendor Comments And Credit

Discovery Credit

LEGACY: Thanks @yvvdwf for reporting this vulnerability through our HackerOne bug bounty program

Legacy QID Mappings

379222 GitLab Multiple Security Vulnerabilities (gitlab- 13.0.1, 12.10.7, 12.9.8)