



CVE-2020-13330

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-13330
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-30 18:15:00 UTC
Updated	2020-10-02 16:58:00 UTC
Description	An issue has been discovered in GitLab affecting versions prior to 12.10.13. GitLab was vulnerable to a stored XSS in impo

Risk And Classification

Problem Types: CWE-79

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	All	All	All	All

References

Reference	Source	Link	Tags
2020/CVE-2020-13330.json · master · GitLab.org / cves · GitLab	CONFIRM	gitlab.com	Vendor Advisory
Cross-Site Scripting In BitbucketServer Import (#30017) · Issues · GitLab.org / GitLab · GitLab	MISC	gitlab.com	Exploit, Vendor /
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

Vendor Comments And Credit

Discovery Credit

LEGACY: Thanks [[@saltyyolk](#) of Chaitin Tech](<https://hackerone.com/saltyyolk>) for responsibly reporting this vulnerability to us.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)