



CVE-2021-39892

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

Summary

CVE	CVE-2021-39892
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-18 17:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	In all versions of GitLab CE/EE since version 12.0, a lower privileged user can import users from projects that they don't have access to.

Risk And Classification

Problem Types: NVD-CWE-Other

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	14.3.0	All	All	All
Application	Gitlab	Gitlab	14.3.0	All	All	All

References

Reference	Source
HackerOne	MISC
2021/CVE-2021-39892.json · master · GitLab.org / cves · GitLab	CODE
Import pending members from public projects or private projects (if you have guest role) (#28440) · Issues · GitLab.org / GitLab · GitLab	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

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

Legacy QID Mappings

[376097](#) GitLab Multiple Security Vulnerabilities (gitlab- 14.3.1, 14.2.5, 14.1.7)

© [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](#)