



CVE-2021-22171

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

Summary

CVE	CVE-2021-22171
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-15 16:15:00 UTC
Updated	2021-01-22 16:04:00 UTC
Description	Insufficient validation of authentication parameters in GitLab Pages for GitLab 11.5+ allows an attacker to steal a victim's AI

Risk And Classification

Problem Types: CWE-287

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
Application	Gitlab	Gitlab	All	All	All	All

References

Reference
2021/CVE-2021-22171.json · master · GitLab.org / cves · GitLab
HackerOne
[Gitlab Pages Auth Bypass] Able to steal a user's Authentication Code For Gitlab Pages (#262) · Issues · GitLab.org / gitlab-pages · GitLab
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Thanks [[@ngalog](https://hackerone.com/ngalog)](<https://hackerone.com/ngalog>) for reporting this vulnerability through our HackerOne bug bounty program

Legacy QID Mappings

[375379](#) GitLab Multiple Security Vulnerabilities(gitlab-13-7-2)

© [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](#).

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