GitLab Community and Enterprise Editions Improper Access Control Vulnerability

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

Summary

CVE	CVE-2023-7028
State	PUBLISHED
Assigner	Unknown
Source Priority	Enrichment-only fallback
Published	2024-05-01 00:00:00 UTC
Updated	2026-04-21 13:32:18 UTC
Description	GitLab Community and Enterprise Editions contain an improper access control vulnerability. This allows an attacker to trigg

Risk And Classification

EPSS: 0.935430000 probability, percentile 0.998310000 (date 2026-04-20)

CISA KEV: Listed on 2024-05-01; due 2024-05-22; ransomware use Unknown

CISA Known Exploited Vulnerability

Vendor	GitLab
Product	GitLab CE/EE
Name	GitLab Community and Enterprise Editions Improper Access Control Vulnerability
Required Action	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Notes	https://about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/ ; https://nvd.nist.gov/vuln/detail/CVE-2023-7028

There are no known software configurations currently associated with this CVE in NVD or the CVE Program record.

References

Reference	Source	Link	Tags
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

379244 GitLab EE/CE Improper Authorization Vulnerability (CVE-2023-7028)

691395 Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (4c8c2218-b120-11ee-90ec-001b217b3468)