



# GitLab Community and Enterprise Editions Improper Access Control Vulnerability

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

## Summary

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

## Risk And Classification

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

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

## CISA Known Exploited Vulnerability

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

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 | <a href="https://www.cve.org">www.cve.org</a>   | canonical           |
| NVD vulnerability detail                     | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a> | canonical, analysis |
| CISA Known Exploited Vulnerabilities catalog | CISA    | <a href="https://www.cisa.gov">www.cisa.gov</a> | 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)

© [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](#)