Severity

Medium

Analysis Summary

CVE-2022-1417

GitLab could allow a remote authenticated attacker to obtain sensitive information, caused by improper access control. By sending a specially-crafted request using CI jobs, an attacker could exploit this vulnerability to access contents of Project Members-only Wikis, and use this information to launch further attacks against the affected system.

Impact

- Information Disclosure

Indicators Of Compromise

CVE

- CVE-2022-1417

Affected Vendors

- GitLab

Affected Products

- GitLab GitLab 8.12.0
- GitLab GitLab 14.8.0
- GitLab GitLab 14.10.0
- GitLab GitLab 14.9.0

Remediation

Refer to GitLab Web site for patch, upgrade or suggested workaround information.

GitLab Website