Severity

Medium

Analysis Summary

CVE-2022-1413 CVSS:5.3

GitLab could allow a remote attacker to obtain sensitive information, caused by missing input masking. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to obtain sensitive integration properties from the web interface.

CVE-2022-1416 CVSS:4.3

GitLab is vulnerable to cross-site scripting, caused by improper validation of user-supplied input by the Pipeline error messages script. A remote authenticated attacker could exploit this vulnerability to execute script in a victim's Web browser within the security context of the hosting Web site. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.

CVE-2022-1423 CVSS:7.1

GitLab could allow a remote authenticated attacker to execute arbitrary code on the system, caused by improper access control in the CI/CD cache mechanism. By conducting a cache poisoning attack, an attacker could exploit this vulnerability to execute arbitrary code on the system.

Impact

- Information Disclosure
- Cross-Site Scripting
- Code Execution

Indicators Of Compromise

CVE

- CVE-2022-1413
- CVE-2022-1416
- CVE-2022-1423

Affected Vendors

- GitLab

Affected Products

- GitLab GitLab 14.10.0
- GitLab GitLab 14.8.5
- GitLab GitLab 14.9.3

Remediation

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

GitLab Web site