مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

# Critical Security Updates-GitLab

Tracking #:432316387

Date:11-10-2024



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed GitLab has released critical security updates to address several vulnerabilities, including a critical -severity flaw that allows attackers to execute pipelines on arbitrary branches.

## TECHNICAL DETAILS:

GitLab released critical security updates addressing multiple vulnerabilities, notably CVE-2024-9164, which has a CVSS score of 9.6. This vulnerability permits attackers to run pipelines on arbitrary branches, posing significant risks of unauthorized access to sensitive data.

**Critical Severity Vulnerability:**

- CVE ID:CVE-2024-9164
- Severity: Critical (CVSS 9.6)
- Description: Allows attackers to execute pipelines on arbitrary branches.
- Affected Versions: All GitLab EE versions from 12.5 prior to 17.4.2.
- Fixed Versions: 17.4.2, 17.3.5, 17.2.9 for GitLab Community Edition (CE) and Enterprise Edition (EE).

## RECOMMENDATIONS:

- Upgrade all GitLab installations to the latest versions as soon as possible.
- Implement logging and monitoring solutions to detect any unauthorized access attempts or unusual activities related to GitLab instances.
- Regularly review and audit your GitLab configurations and user permissions to minimize potential attack surfaces.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://about.gitlab.com/releases/2024/10/09/patch-release-gitlab-17-4-2-released/