مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerability in GitLab Products

Tracking #:432316046

Date:12-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in GitLab Community and Enterprise Edition (CE/EE) products that which allows an attacker to trigger a pipeline as another user under certain circumstances.

TECHNICAL DETAILS:

- **CVE ID: CVE-2024-6385**
- **CVSS Score: CNA: GitLab Inc,9.6 Critical**
- An issue was discovered in GitLab CE/EE affecting all versions starting from 15.8 prior to 16.11.6, starting from 17.0 prior to 17.0.4, and starting from 17.1 prior to 17.1.2, which allows an attacker to trigger a pipeline as another user under certain circumstances.
- **Affected Versions**: GitLab CE/EE versions from versions 15.8 prior to 16.11.6, 17.0 prior to 17.0.4, and 17.1 prior to 17.1.2
- **Updated Versions:** GitLab Community Edition (CE) and Enterprise Edition (EE) 17.1.2, 17.0.4, 16.11.6

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade to fixed version at the earliest.

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/2024/07/10/patch-release-gitlab-17-1-2-released/