مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

# Critical Vulnerability in GitLab Products

Tracking #:432316000

Date:01-07-2024

## 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 could allow unauthenticated attackers to execute pipelines as any user within the GitLab instance.

## TECHNICAL DETAILS:

- **CVE ID: CVE-2024-5655**
- **CVSS Score: CNA: GitLab Inc,9.6 Critical**
- An attacker can potentially exploit a vulnerability within GitLab to execute pipelines as any user on the platform. While the specific circumstances for exploitation are not currently disclosed by GitLab, the potential impact is severe. A successful attack could allow unauthorized access to sensitive data, deployment of malicious code, or disruption of critical workflows.
- **Affected Versions**: GitLab CE/EE versions from 15.8 through 16.11.4, 17.0.0 to 17.0.2, and 17.1.0 to 17.1.0.,
- **Updated Versions**: 17.1.1, 17.0.3, and 16.11.5

## 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://nvd.nist.gov/vuln/detail/CVE-2024-5655