



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



Security Updates- Multiple Vulnerabilities GitLab Community and Enterprise Edition  
Tracking #:432315738  
Date:29-03-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL



## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple Vulnerabilities in GitLab Community Edition (CE) and Enterprise Edition (EE) that could be exploited to gain unauthorized access to affected systems.

## TECHNICAL DETAILS:

### Vulnerabilities Details:

- **CVE-2023-6371- Stored-XSS injected in Wiki page via Banzai pipeline**
  - CVSS score 8.7 High
  - A vulnerability exists in GitLab CE/EE that allows attackers to inject malicious scripts into wiki pages via the Banzai pipeline. A crafted payload within a wiki page can lead to stored XSS, enabling attackers to execute arbitrary actions with the victim's privileges.
- **CVE-2024-2818- DOS using crafted emojis**
  - CVSS score 4.3 Medium
  - A vulnerability exists in GitLab CE/EE where a specially crafted emoji string used within the description parameter for labels can trigger a denial-of-service (DoS) attack. This vulnerability could potentially render the GitLab instance unavailable to legitimate users.

### Affected Versions:

- GitLab CE/EE affecting all versions before 16.8.5
- GitLab CE/EE affecting all versions starting from 16.9 before 16.9.3
- GitLab CE/EE affecting all versions starting from 16.10 before 16.10.1.

### Fixed Versions:

- GitLab CE/EE 16.10.1
- GitLab CE/EE 16.9.3
- GitLab CE/EE 16.8.5

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by GitLab.

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/2024/03/27/security-release-gitlab-16-10-1-released/#stored-xss-injected-in-wiki-page-via-banzai-pipeline>