مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – GitLab

Tracking #:432316437

Date:25-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that GitLab has released security updates to address multiple vulnerabilities in GitLab Community Edition (CE) and Enterprise Edition (EE).

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-8312: High Severity Cross-Site Scripting (XSS) Vulnerability**
  - CVSS 3.1 score: 8.7
  - This vulnerability allows attackers to inject malicious HTML code into the Global Search field on a diff view, potentially leading to Cross-Site Scripting (XSS) attacks. Exploitation could result in: the theft of user data, session hijacking, or redirection to malicious websites.
  - Successful exploitation could compromise user accounts and sensitive information, potentially leading to further attacks within the GitLab environment.
  - **Affected versions:** GitLab CE/EE-All versions from 15.10 before 17.3.6, 17.4 before 17.4.3, and 17.5 before 17.5.1
- **CVE-2024-6826: Medium Severity Denial of Service (DoS) Vulnerability**
  - CVSS 3.1 score: 6.5
  - This vulnerability allows attackers to cause a Denial of Service (DoS) condition by importing a maliciously crafted XML manifest file
  - Successful exploitation could disrupt service availability for legitimate users, potentially affecting productivity and system reliability.
  - **Affected versions:** GitLab CE/EE-All versions from 11.2 before 17.3.6, 17.4 before 17.4.3, and 17.5 before 17.5.1

Fixed Versions:

- GitLab Community Edition (CE) and Enterprise Edition (EE) versions 17.5.1, 17.4.3, 17.3.6

RECOMMENDATIONS:

The UAE Cyber Security Council recommends upgrading the affected versions to the fixed versions 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/2024/10/23/patch-release-gitlab-17-5-1-released/#html-injection-in-global-search-may-lead-to-xss