مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- GitLab Multiple Vulnerabilities

Tracking #:432315893

Date:27-05-2024

TLP: WHITE

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:

- **High Severity (CVE-2024-4835):** An XSS vulnerability in the VS Code editor (Web IDE) that could allow attackers to steal user credentials with a single click.
- **Medium Severity (CVE-2024-2874):** A Denial-of-Service (DoS) vulnerability in the runner description field.
- **Medium Severity (CVE-2023-7045):** A CSRF vulnerability via the Kubernetes Agent Server (KAS) that could allow attackers to steal anti-CSRF tokens.
- **Medium Severity (CVE-2024-5258):** An authorization bypass vulnerability related to the Set Pipeline Status of a Commit API.
- **Medium Severity (CVE-2023-6502):** A DoS vulnerability in the wiki render API/Page.
- **Medium Severity (CVE-2024-1947):** A DoS vulnerability related to test_report API calls.
- **Medium Severity (CVE-2024-5318):** An information disclosure vulnerability allowing guest users to view dependency lists of private projects.

Affected Versions:

- GitLab versions before 17.0.1, 16.11.3, and 16.10.6 (Community Edition and Enterprise Edition)

Fixed Versions:

- GitLab Community Edition (CE): 17.0.1, 16.11.3, or 16.10.6
- GitLab Enterprise Edition (EE): 17.0.1, 16.11.3, or 16.10.6

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/2024/05/22/patch-release-gitlab-17-0-1-released/