مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – GitLab CE and EE

Tracking #:432317018

Date:27-03-2025

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:

Vulnerabilities Addressed:

1. High-Severity Cross-Site Scripting (XSS) Vulnerabilities

- **CVE-2025-2255 (CVSS 8.7):** XSS via merge-request error messages. Attackers could inject malicious scripts via crafted error messages.
  - Affected Versions: 13.5.0 before 17.8.6, 17.9 before 17.9.3, and 17.10 before 17.10.1.
- **CVE-2025-0811 (CVSS 8.7):** XSS via improper rendering of certain file types. Malicious code could execute within the user's browser.
  - Affected Versions: 17.7 before 17.8.6, 17.9 before 17.9.3, and 17.10 before 17.10.1.

2. Privilege Escalation Vulnerability

- **CVE-2025-2242 (CVSS 7.5):** Improper access control allows a former instance admin—now a regular user—to retain elevated privileges to groups and projects.
  - Affected Versions: 17.4 before 17.8.6, 17.9 before 17.9.3, and 17.10 before 17.10.1.

3. Unauthorized Access to Internal Projects

- **CVE-2024-12619 (CVSS 5.2):** Internal users could gain unauthorized access to internal projects.
  - Affected Versions: 16.0 before 17.8.6, 17.9 before 17.9.3, and 17.10 before 17.10.1.

4. Additional Vulnerabilities:

- **CVE-2024-10307:** Uncontrolled resource consumption via malicious Terraform files in merge requests.
- **CVE-2024-9773:** Shell code injection in Harbor project name configuration using helper scripts.
- **Prompt Injection Vulnerability:** In GitLab Duo with Amazon Q integration.

Fixed Versions:

- GitLab Community Edition (CE) and Enterprise Edition (EE) versions: 17.10.1, 17.9.3, and 17.8.6.

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/2025/03/26/patch-release-gitlab-17-10-1-released/