مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – GitLab Community Edition and Enterprise Edition

Tracking #:432318005

Date:14-11-2025

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

GitLab has released important security updates for GitLab Community Edition (CE) and Enterprise Edition (EE), addressing multiple vulnerabilities across several components. The patched versions — 18.5.2, 18.4.4, and 18.3.6 — resolve issues that could allow cross-site scripting (XSS), authorization bypass, information disclosure, and denial of service.

Vulnerability Details

- **CVE-2025-11224**
  Severity: High (CVSS 7.7)
  Description: A stored cross-site scripting (XSS) vulnerability identified in the Kubernetes proxy component. Under certain conditions, an authenticated user could execute arbitrary JavaScript due to improper input validation in Kubernetes proxy requests.

- **CVE-2025-11865**
  Severity: Medium (CVSS 6.5)
  Description: An incorrect authorization issue in GitLab Duo workflows could allow a user to remove another user's Duo flows.

- **CVE-2025-2615**
  Severity: Medium (CVSS 4.3)
  Description: A vulnerability in GraphQL subscriptions could allow a blocked user to access sensitive data through WebSocket connections, resulting in unintended information disclosure.

- **CVE-2025-7000**
  Severity: Medium (CVSS 4.3)
  Description: An access control flaw could allow unauthorized users to view confidential branch names by accessing issues linked to related merge requests.

- **CVE-2025-6945**
  Severity: Low (CVSS 3.5)
  Description: A prompt injection issue in GitLab Duo review could allow an authenticated user to leak data from confidential issues by embedding malicious prompts in merge request comments.

- **CVE-2025-11990**
  Severity: Low (CVSS 3.1)
  Description: A client-side path traversal vulnerability in branch names could expose CSRF tokens due to improper input validation and weak redirect handling in repository references.

- **CVE-2025-6171**
  Severity: Low (CVSS 3.1)
  Description: An information disclosure issue in the packages API endpoint could allow authenticated users with limited access to view branch names and pipeline details even when repository access is restricted.

- **CVE-2025-7736**
  Severity: Low (CVSS 3.1)
  Description: An improper access control issue in GitLab Pages could allow an authenticated user to bypass page access restrictions and view content meant only for project members by authenticating via OAuth.

- **CVE-2025-12983**
  Severity: Low (CVSS 3.1)
  Description: A denial-of-service (DoS) vulnerability in markdown processing could allow an authenticated user to cause excessive resource consumption by submitting specially crafted markdown with nested formatting.

Fixed Versions

- GitLab **18.5.2**
- GitLab **18.4.4**
- GitLab **18.3.6**

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/2025/11/12/patch-release-gitlab-18-5-2-released/