مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – GitLab Community Edition and Enterprise Edition

Tracking #:432318831

Date:23-04-2026

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 security updates addressing multiple vulnerabilities in GitLab Community Edition (CE) and Enterprise Edition (EE). The vulnerabilities include Cross-Site Request Forgery (CSRF), Cross-Site Scripting (XSS), Denial-of-Service (DoS), and access control issues.
Successful exploitation could allow attackers to perform unauthorized actions, access sensitive data, or disrupt services.

Vulnerability Details

High Severity Vulnerabilities

- **CVE-2026-4922** – Cross-Site Request Forgery (CSRF) in GraphQL API
- **CVE-2026-5816** – Improper Path Validation in Web IDE
- **CVE-2026-5262** – Cross-Site Scripting (XSS) in Storybook

Medium Severity Vulnerabilities

- **CVE-2025-0186** – Denial of Service in discussions endpoint
- **CVE-2026-1660** – Denial of Service in Jira import
- **CVE-2025-6016** – Denial of Service in notes endpoint
- **CVE-2025-3922** – Denial of Service in GraphQL API
- **CVE-2026-6515** – Insufficient session expiration in virtual registry credentials
- **CVE-2026-5377** – Improper access control in issue description renderer

Low Severity Vulnerabilities

- **CVE-2026-3254** – Improper restriction in Mermaid sandbox
- **CVE-2025-9957** – Improper access control in project fork relationship API

Fixed Versions

- GitLab Community Edition (CE) and Enterprise Edition (EE) 18.11.1, 18.10.4, 18.9.6

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://docs.gitlab.com/releases/patches/patch-release-gitlab-18-11-1-released/