مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – GitLab Community Edition and Enterprise Edition

Tracking #:432318389

Date:12-02-2026

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 for Community Edition (CE) and Enterprise Edition (EE) to address multiple vulnerabilities, including high-severity issues that could result in token theft, unauthorized actions, and denial of service.

High-Severity Vulnerabilities:

- **CVE-2025-7659 – Incomplete Validation in Web IDE:** May allow token theft and access to private repositories.
- **CVE-2025-8099 – GraphQL Introspection DoS:** Could allow unauthenticated DoS via repeated GraphQL queries.
- **CVE-2026-0958 – JSON Validation Middleware DoS:** Could allow CPU/memory exhaustion. CVSS 7.5
- **CVE-2025-14560 – Cross-Site Scripting in Code Flow:** Authenticated users may perform actions as other users.
- **CVE-2026-0595 – HTML Injection in Test Case Titles:** May allow unauthorized changes to user accounts.

Fixed Versions

- GitLab Community Edition (CE) and Enterprise Edition (EE) 18.8.4, 18.7.4, 18.6.6

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/2026/02/10/patch-release-gitlab-18-8-4-released/