مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – GitLab Community Edition and Enterprise Edition

Tracking #:432318657

Date:25-03-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

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 to address multiple vulnerabilities, including several high-severity issues, affecting GitLab Community Edition (CE) and Enterprise Edition (EE). Successful exploitation of these vulnerabilities could result in authentication bypass, unauthorized actions, exposure of sensitive data, execution of malicious scripts, or denial-of-service conditions.

Vulnerability Details
High Severity

- **CVE-2026-2370** – Improper Handling of Parameters in Jira Connect installations (CVSS 8.1)
- **CVE-2026-3857** – Cross-Site Request Forgery (CSRF) in GraphQL API (CVSS 8.1)
- **CVE-2026-2995** – HTML Injection in vulnerability report *(EE only)* (CVSS 7.7)
- **CVE-2026-3988** – Denial of Service in GraphQL API (CVSS 7.5)

Medium Severity

- **CVE-2026-2745** – Improper Access Control in WebAuthn 2FA (CVSS 6.8)
- **CVE-2026-1724** – Improper Access Control in GraphQL query *(EE only)* (CVSS 6.8)
- **CVE-2025-13436** – Denial of Service in CI configuration processing (CVSS 6.5)
- **CVE-2025-13078** – Denial of Service in webhook configuration (CVSS 6.5)
- **CVE-2026-2973** – Cross-site Scripting (XSS) in Mermaid renderer (CVSS 5.4)
- **CVE-2026-2726** – Improper Access Control in Merge Requests (CVSS 4.3)
- **CVE-2025-14595** – Access Control issue in GraphQL API *(EE only)* (CVSS 4.3)

Low Severity

- **CVE-2026-4363 –** Incorrect Authorization in authorization caching *(EE only)* (CVSS 3.7)

Fixed Versions

- GitLab Community Edition (CE) and Enterprise Edition (EE) 18.10.1, 18.9.3, 18.8.7

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/2026/03/25/patch-release-gitlab-18-10-1-released/