مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – GitLab Community Edition and Enterprise Edition

Tracking #:432318764

Date:10-04-2026

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 for GitLab Community Edition (CE) and Enterprise Edition (EE) addressing multiple vulnerabilities affecting core components such as WebSockets, GraphQL APIs, Terraform state handling, CSV processing, analytics dashboards, and access control mechanisms. The issues include high-severity denial-of-service (DoS), information disclosure, cross-site scripting (XSS), code injection, and improper authorization flaws that could impact confidentiality, integrity, and availability of affected systems.

Vulnerability Details

High Severity

- **CVE-2026-5173** – WebSocket exposed method abuse (CVSS 8.5)
  Authenticated users may invoke unintended server-side methods due to improper access control.
- **CVE-2026-1092** – Terraform state lock API DoS (CVSS 7.5)
  Unauthenticated users can crash services via malformed JSON payloads.
- **CVE-2025-12664** – GraphQL API DoS (CVSS 7.5)
  Repeated GraphQL queries can degrade or disrupt service availability.

Medium Severity

- **CVE-2026-1403** – CSV import DoS affecting Sidekiq workers
- **CVE-2026-1101** – GraphQL SBOM API DoS (GitLab EE)
- **CVE-2026-1516** – Code Quality report injection leading to IP leakage (EE)
- **CVE-2026-4332** – XSS in analytics dashboards (EE)
- **CVE-2026-2619** – Incorrect authorization in vulnerability flag API (EE)
- **CVE-2025-9484** – GraphQL-based email address disclosure (EE)
- **CVE-2026-1752** – Improper environment API access control (EE)
- **CVE-2026-2104** – CSV export information disclosure (CE/EE)

Low Severity

- **CVE-2026-4916** – Custom role permission escalation (CE/EE)

Fixed Versions

- GitLab Community Edition (CE) and Enterprise Edition (EE) 18.10.3, 18.9.5, 18.8.9

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/2026/04/08/patch-release-gitlab-18-10-3-released/#cve-2026-5173---exposed-method-issue-in-websocket-connections-impacts-gitlab-ceee