مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – GitLab Community Edition and Enterprise Edition

Tracking #:432317795

Date:10-10-2025

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 patch versions 18.4.2, 18.3.4, and 18.2.8 for GitLab Community Edition (CE) and Enterprise Edition (EE). These releases address multiple vulnerabilities that could allow unauthorized access, denial of service conditions, and exposure of sensitive data.

Vulnerability Details:

CVE-2025-11340: Incorrect Authorization in GraphQL Mutations (EE Only)

- Authenticated users with read-only API tokens could abuse incorrectly scoped GraphQL mutations to perform unauthorized write operations on vulnerability records.
- Severity: High (CVSS 7.7).

CVE-2025-10004: Denial of Service in GraphQL Blob Type (CE/EE)

- Crafted GraphQL queries requesting large repository blobs could render instances unresponsive or degraded.
- Severity: High (CVSS 7.5).

CVE-2025-9825: Missing Authorization in Manual Jobs (CE/EE)

- Authenticated users without project membership could view sensitive manual CI/CD variables via the GraphQL API.
- Severity: Medium (CVSS 5.0).

CVE-2025-2934: Denial of Service in Webhook Endpoints (CE/EE)

- Authenticated users could create webhook endpoints sending crafted HTTP responses that result in denial of service, due to an upstream Ruby Core library issue.
- Severity: Medium (CVSS 4.3).

Fixed Versions:

- GitLab 18.4.2, 18.3.4, 18.2.8 for GitLab Community Edition (CE) and Enterprise Edition (EE)

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/2025/10/08/patch-release-gitlab-18-4-2-released/