مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates- GitLab CE/EE Versions

Tracking #:432317847

Date:24-10-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that GitLab has released security updates for GitLab Community Edition (CE) and Enterprise Edition (EE) addressing multiple high-severity vulnerabilities that may allow unauthorized access, denial of service (DoS), and privilege escalation in self-managed instances.

TECHNICAL DETAILS:

GitLab has released security updates for GitLab Community Edition (CE) and Enterprise Edition (EE) addressing multiple high-severity vulnerabilities that may allow unauthorized access, denial of service (DoS), and privilege escalation in self-managed instances. These vulnerabilities affect a wide range of GitLab versions and could be exploited by both authenticated and unauthenticated attackers to disrupt services, hijack runners, or gain unauthorized access.

GitLab.com and GitLab Dedicated customers are already protected, but all self-managed GitLab users are strongly advised to upgrade immediately to the latest patched versions to prevent potential exploitation.

High and medium Severity Vulnerability Details:

CVE ID	Title / Description	Affected Versions	Severity (CVSS 3.1)
CVE-2025-11702	Improper Access Control in Runner API (GitLab EE) — Authenticated users with specific permissions could hijack project runners from other projects.	EE: 17.1 → before 18.3.5, 18.4 → before 18.4.3, 18.5 → before 18.5.1	High (8.5)
CVE-2025-10497	Denial of Service in Event Collection (GitLab CE/EE) — Unauthenticated users could cause service disruption via crafted payloads.	CE/EE: 17.10 → before 18.3.5, 18.4 → before 18.4.3, 18.5 → before 18.5.1	High (7.5)
CVE-2025-11447	Denial of Service in JSON Validation (GitLab CE/EE) — Unauthenticated attackers could send malicious GraphQL JSON payloads to exhaust system resources.	CE/EE: 11.0 → before 18.3.5, 18.4 → before 18.4.3, 18.5 → before 18.5.1	High (7.5)
CVE-2025-11974	Denial of Service in Upload Function (GitLab CE/EE) — Attackers could trigger DoS via large file uploads.	CE/EE: 11.7 → before 18.3.5, 18.4 → before 18.4.3, 18.5 → before 18.5.1	Medium (6.5)
CVE-2025-11971	Incorrect Authorization in Pipeline Builds (GitLab CE) — Authenticated users could trigger unauthorized pipelines through commit manipulation.	CE: 10.6 → before 18.3.5, 18.4 → before 18.4.3, 18.5 → before 18.5.1	Medium (6.5)

Patched Versions:

- 18.5.1
- 18.4.3
- 18.3.5

RECOMMENDATIONS:

- Immediate Upgrade: Upgrade GitLab CE/EE installations to one of the patched versions.

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/2025/10/22/patch-release-gitlab-18-5-1-released/