مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates - GitLab CE/EE

Tracking #:432317377

Date:13-06-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed GitLab has released security updates for its Community Edition (CE) and Enterprise Edition (EE) to address multiple vulnerabilities.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-4278 – HTML Injection (Account Takeover via Search Page)**
  Severity: High (CVSS 8.7)
  Improper input sanitization on the search page allowed malicious HTML injection, potentially leading to account takeover.
- **CVE-2025-2254 – Cross-Site Scripting (Snippet Viewer)**
  Severity: High (CVSS 8.7)
  Injected scripts in the snippet viewer could execute in the context of another user, enabling impersonation or data theft.
- **CVE-2025-5121 – Unauthorized CI/CD Pipeline Injection (Ultimate EE only)**
  Severity: High (CVSS 8.5)
  Authenticated users could tamper with CI/CD pipelines across all projects by injecting malicious jobs.
- **CVE-2025-0673 – Denial of Service (Infinite Redirect Loop)**
  Severity: High (CVSS 7.5)
  Memory exhaustion and DoS via redirect loops could cause total service disruption.
- **CVE-2025-1516 – DoS via Large Webhook Token Names**
  Severity: Medium (CVSS 6.5)
  Abuse of excessively large token names could lead to denial of service.
- **CVE-2025-1478 – DoS via Large Board Names**
  Severity: Medium (CVSS 6.5)
  Oversized board names caused performance degradation, risking denial of service.
- **CVE-2024-9512 – Information Disclosure (Secondary Node Repository Clone)**
  Severity: Medium (CVSS 5.3)
  Attackers could clone private repositories by exploiting sync delay vulnerabilities on secondary nodes.
- **CVE-2025-5996 – DoS via Uncontrolled HTTP Response Processing**
  Severity: Medium (CVSS 6.5)
  Third-party component misuse could lead to denial of service through malformed HTTP responses.
- **CVE-2025-5195 – Information Disclosure (Compliance Framework Access)**
  Severity: Medium (CVSS 4.3)
  Authenticated users could gain unauthorized access to compliance framework data.
- **CVE-2025-5982 – Group IP Restriction Bypass (EE Only)**
  Severity: Low (CVSS 3.7)
  IP-based access controls could be bypassed, allowing disclosure of sensitive group information.

Fixed Versions:

- GitLab Community Edition (CE) and Enterprise Edition (EE) Versions 18.0.2, 17.11.4, 17.10.8

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/2025/06/11/patch-release-gitlab-18-0-2-released/