مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – GitLab Community Edition and Enterprise Edition

Tracking #:432316917

Date:28-02-2025

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:

High-Severity Cross-Site Scripting (XSS) vulnerabilities:

- CVE-2025-0475 (CVSS 8.7): A flaw in the Kubernetes proxy endpoint affecting all versions from 15.10 to 17.9.0. This vulnerability could allow attackers to inject malicious JavaScript payloads, leading to DOM-based XSS attacks.
- CVE-2025-0555 (CVSS 7.7): A vulnerability in the Maven Dependency Proxy affecting GitLab-EE versions 16.6 through 17.9.0. This flaw enables attackers to bypass Content Security Policy (CSP) restrictions using specially crafted dependency metadata files.

Medium-Severity vulnerabilities:

- CVE-2024-8186 (CVSS 5.4): HTML injection via child item search, enabling limited XSS in self-hosted instances.
- CVE-2024-10925 (CVSS 5.3): Guest user access to security policy YAML files, potentially exposing compliance rules.
- CVE-2025-0307 (CVSS 4.3): Planner role accessing code review analytics, revealing sensitive metrics.

Successful exploitation of this vulnerabilities could lead to session hijacking, credential theft, unauthorized system access, and other malicious actions.

Fixed Versions:

- GitLab Community Edition (CE) and Enterprise Edition (EE) 17.9.1, 17.8.4, 17.7.6

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/2025/02/26/patch-release-gitlab-17-9-1-released/