مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - GitLab CE/EE

Tracking #:432317524

Date:24-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that GitLab has released important security updates for both Community Edition (CE) and Enterprise Edition (EE), addressing multiple vulnerabilities—including high-severity Cross-Site Scripting (XSS) flaws and data exposure risks.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-4700 – Cross-Site Scripting in Kubernetes Proxy (CVSS 8.7)**
  A high-severity vulnerability in GitLab's Kubernetes proxy could allow attackers to execute arbitrary JavaScript under certain conditions. This poses significant risks to the confidentiality and integrity of affected environments.
- **CVE-2025-4439 – XSS via Certain CDNs (CVSS 7.7)**
  An authenticated user could exploit this vulnerability in specific hosting environments using certain content delivery networks, potentially executing malicious scripts.
- **CVE-2025-7001 – Unauthorized API Access to Resource Groups (CVSS 4.3)**
  Privileged users could access resource_group data through the API beyond their intended scope, violating access control principles.
- **CVE-2025-4976 – Internal Notes Exposure via GitLab Duo (CVSS 4.3)** *(EE Only)*
  Under rare conditions, internal notes tied to GitLab Duo responses could be accessed without proper authorization, risking leakage of confidential information.
- **CVE-2025-0765 – Custom Service Desk Email Disclosure (CVSS 4.3)**
  This vulnerability could expose custom email addresses linked to the service desk functionality, potentially aiding in phishing or reconnaissance.
- **CVE-2025-1299 – Unauthorized Access to Deployment Job Logs (CVSS 4.3)**
  Improper access control allowed unauthorized users to retrieve sensitive deployment job logs through specially crafted requests.

Fixed Versions:

- GitLab Community Edition (CE) and Enterprise Edition (EE) Versions 18.2.1, 18.1.3, 18.0.5

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/2025/07/23/patch-release-gitlab-18-2-1-released/