مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Gitlab Security Updates
Tracking #:432316510
Date:14-11-2024

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

GitLab has released critical patches for versions **17.5.2**, **17.4.4**, and **17.3.7** of both the **Community Edition (CE)** and **Enterprise Edition (EE)** to address multiple security vulnerabilities, including **CVE-2024-9693**, which affects the **Kubernetes agent** in GitLab-managed Kubernetes clusters. These versions also address several other vulnerabilities, including issues with **Device OAuth flow**, **Denial of Service (DoS)**, **Stored XSS** in analytics dashboards, **HTML injection**, and **information disclosure** via API endpoints.

Vulnerability Details:
- Unauthorized Access to Kubernetes Cluster Agent (CVE-2024-9693)
  - Severity: High (CVSS 8.5)
- Device OAuth Flow Allows Cross-Window Forgery (CVE-2024-7404)
  - Severity: Medium (CVSS 6.8)
- Denial of Service via Malicious FogBugz Import Payload (No CVE Assigned)
  - Severity: Medium (CVSS 6.5)
- Stored XSS via JavaScript URL in Analytics Dashboards (CVE-2024-8648)
  - Severity: Medium (CVSS 6.1)
- HTML Injection in Vulnerability Code Flow (CVE-2024-8180)
  - Severity: Medium (CVSS 5.4)
- Information Disclosure via API Endpoint (CVE-2024-10240)
  - Severity: Medium (CVSS 5.3)

Fixed Versions:
- GitLab Patch Release: 17.5.2, 17.4.4, 17.3.7 for GitLab Community Edition (CE) and Enterprise Edition (EE).

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade GitLab Version to the latest version at the earliest.

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/2024/11/13/patch-release-gitlab-17-5-2-released/