مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in GitLab

Tracking #:432316287

Date:16-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Gitlab released security advisory to address multiple vulnerabilities affecting its Community Edition (CE) and Enterprise Edition (EE) products.

TECHNICAL DETAILS:

GitLab has identified and patched a critical vulnerability (**CVE-2024-6678**) along with three high-severity vulnerabilities in its Community Edition (CE) and Enterprise Edition (EE) products. The critical flaw allows attackers to trigger pipeline jobs as arbitrary users, posing significant risks of unauthorized access and privilege escalation. Organizations using affected versions are urged to apply the latest updates immediately to mitigate these vulnerabilities.

- **CVE-2024-6678 (CVSS: 9.9)**: This critical vulnerability allows an attacker to trigger a pipeline as an arbitrary user under specific conditions, potentially leading to unauthorized access and privilege escalation. It affects all GitLab CE/EE versions starting from 8.14 up to 17.1.7, 17.2 prior to 17.2.5, and 17.3 prior to 17.3.2.
- **CVE-2024-8640 (CVSS: 8.5)**: A code injection vulnerability due to incomplete input filtering that allows attackers to inject commands into a connected Cube server. This affects GitLab EE from version 16.11.
- **CVE-2024-8635 (CVSS: 7.7)**: A Server-Side Request Forgery (SSRF) vulnerability that enables attackers to make requests to internal resources via a custom Maven Dependency Proxy URL, affecting GitLab EE from version 16.8.
- **CVE-2024-8124 (CVSS: 7.5)**: This vulnerability could lead to a Denial of Service (DoS) by sending a large parameter, impacting GitLab CE/EE from version 16.4

- **Fixed Versions:**
  - 17.3.2, 17.2.5, 17.1.7 for GitLab Community Edition (CE) and Enterprise Edition (EE).

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade to the latest version as soon as possible.

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/2024/09/11/patch-release-gitlab-17-3-2-released/