مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in GitLab

Tracking #:432316300

Date:18-09-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

GitLab has identified and patched a critical vulnerability (**CVE-2024-45409**) in its Community Edition (CE) and Enterprise Edition (EE) products. The critical flaw would allow the attacker to log in as arbitrary user within the vulnerable system. Organizations using affected versions are urged to apply the latest updates immediately to mitigate these vulnerabilities.

- **CVE ID**: **CVE-2024-45409-**10.0 CRITICAL
- SAML authentication bypass-An unauthenticated attacker with access to any signed saml document (by the IdP) can thus forge a SAML Response/Assertion with arbitrary contents. This would allow the attacker to log in as arbitrary user within the vulnerable system.

- **Fixed Versions:**
  - 17.3.3, 17.2.7, 17.1.8, 17.0.8, 16.11.10 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/2024/09/17/patch-release-gitlab-17-3-3-released/