مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Security Patch-GitLab

Tracking #:432316966

Date:13-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that GitLab has issued a critical patch release for its Community Edition (CE) and Enterprise Edition (EE). These updates address multiple vulnerabilities, including critical issues in third-party libraries such as ruby-saml and graphql, which could lead to authentication bypasses and remote code execution (RCE).

TECHNICAL DETAILS:

GitLab has issued a critical patch release for versions 17.9.2, 17.8.5, and 17.7.7 of its Community Edition (CE) and Enterprise Edition (EE). These updates address multiple vulnerabilities, including critical issues in third-party libraries such as ruby-saml and graphql, which could lead to authentication bypasses and remote code execution (RCE).

Key Vulnerabilities Addressed

1. **Critical Vulnerabilities**:
    - **CVE-2025-25291 & CVE-2025-25292**:
        - Found in the ruby-saml library used for SAML SSO authentication.
        - Exploitation could allow an attacker with a valid signed SAML document to impersonate another user.
    - **CVE-2025-27407**:
        - Found in the graphql library.
        - Exploitation could result in RCE through maliciously crafted project transfers.

Other Vulnerabilities:

- Denial of Service (DoS) due to inefficient processing of untrusted input.
- Credentials disclosure during repository mirroring failures.
- DoS vulnerability in approval rules caused by unbounded fields.
- Low-severity vulnerabilities such as shell code injection in Google integrations and improper permissions for guest users.

Fixed Versions:

- GitLab CE/EE to versions 17.9.2, 17.8.5, or 17.7.7

Mitigations (if upgrade is not immediately possible):

- For ruby-saml vulnerabilities:
    - Enable two-factor authentication (2FA) for all users.
    - Disable the SAML two-factor bypass option.
    - Require admin approval for auto-created users (gitlab_rails['omniauth_block_auto_created_users'] = true).
- For graphql vulnerability:
    - Disable the Direct Transfer feature if enabled (disabled by default).

RECOMMENDATIONS:

- Upgrade GitLab CE/EE to fixed versions immediately, if upgrading is not immediately possible, apply the mitigations.

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/2025/03/12/patch-release-gitlab-17-9-2-released/