Security Advisory 2024-026

Vulnerabilities in GitLab

March 8, 2024 — v1.0

TLP:CLEAR

History:

- *08/03/2024 — v1.0 – Initial publication*

Summary

On March 6, 2024, GitLab released a security advisory addressing several vulnerabilities that could lead to a security policy bypass and a breach of data confidentiality [1].

Technical Details

- The vulnerability `CVE-2024-0199`, with a CVSS score of 7.7, allows an attacker to bypass CODEOWNERS approval allowing stealing protected variables by utilising a crafted payload in an old feature branch to perform malicious actions.
- The vulnerability `CVE-2024-1299`, with a CVSS score of 6.5, allows a user with the custom role of `manage_group_access_tokens` to rotate group access tokens with owner privileges.

Affected Products

- GitLab Community Edition (CE) and Gitlab Enterprise Edition (EE) versions prior to 16.7.7;
- GitLab Community Edition (CE) and Gitlab Enterprise Edition (EE) versions 16.8.x prior to 16.8.4;
- GitLab Community Edition (CE) and Gitlab Enterprise Edition (EE) versions 16.9.x prior to 16.9.2.

Recommendations

CERT-EU strongly recommends updating software installations to the latest versions by following the instructions given by the vendor [1].

References

[1] https://about.gitlab.com/releases/2024/03/06/security-release-gitlab-16-9-2-released/