CERT-EU

Security Advisory 2024-064

Vulnerabilities in GitLab

June 28, 2024 — v1.0

TLP:CLEAR

History:

- *28/06/2024 — v1.0 – Initial publication*

Summary

On June 26, 2024, GitLab released a security advisory addressing several vulnerabilities, one of which being critical, allowing an attacker to trigger a pipeline as another user under certain circumstances [1].

Technical Details

- The critical vulnerability `CVE-2024-5655`, with a CVSS score of 9.6, allows an attacker to trigger a pipeline as another user under certain circumstances. GitLab pipelines are a feature of the Continuous Integration/Continuous Deployment (CI/CD) system that enables users to automatically run processes and tasks, either in parallel or in sequence, to build, test, or deploy code changes.
- The vulnerability `CVE-2024-4901`, with a CVSS score of 8.7, is an issue where a stored XSS vulnerability could be imported from a project with malicious commit notes.
- The vulnerability `CVE-2024-4994`, with a CVSS score of 8.1, allows for a CSRF attack on GitLab's GraphQL API leading to the execution of arbitrary GraphQL mutations.
- The vulnerability `CVE-2024-6323`, with a CVSS score of 7.5, allows an attacker leak content of a private repository in a public project.

Affected Products

The following versions of GitLab CE/EE are affected:

- from 15.8 prior to 16.11.5
- from 17.0 prior to 17.0.3
- from 17.1 prior to 17.1.1.

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/2024/06/26/patch-release-gitlab-17-1-1-released/