Security Advisory 2024-096

Vulnerabilities in GitLab

2024-09-13 — v1.0

TLP:CLEAR

History:

- *13/09/2024 — v1.0 – Initial publication*

Summary

On September 11, 2024, GitLab released a security advisory addressing several vulnerabilities, one of which being critical, allowing an attacker to trigger pipelines as arbitrary users under certain conditions [1].

Technical Details

- The critical vulnerability **CVE-2024-6678**, with a CVSS score of 9.9, allows an attacker to trigger a pipeline as an arbitrary 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-2024-8640**, with a CVSS score of 8.5, allows an attacker to inject commands into a connected Cube server.
- The vulnerability **CVE-2024-8635**, with a CVSS score of 7.7, allows an attacker to make requests to internal resources using a custom Maven Dependency Proxy URL.
- The vulnerability **CVE-2024-8124**, with a CVSS score of 7.5, allows an attacker cause Denial of Service via sending a large `glm_source` parameter.

Affected Products

The following versions of GitLab CE/EE are affected:

- from 8.14 up to 17.1.7;
- from 17.2 prior to 17.2.5;
- from 17.3 prior to 17.3.2.

Recommendations

CERT-EU strongly recommends updating affected GitLab instances to the latest versions [1].

References

[1] https://about.gitlab.com/releases/2024/09/11/patch-release-gitlab-17-3-2-released/