CERT-EU

Security Advisory 2024-109

Critical vulnerabilities in Gitlab

2024-10-11 — v1.0

TLP:CLEAR

History:

- *11/10/2024 — v1.0 – Initial publication*

Summary

On October 9, 2024, GitLab released an advisory addressing several critical vulnerabilities in GitLab EE/CE affecting versions from 8.16 to 17.4.1.

It is recommended updating affected assets as soon as possible.

Technical Details

The vulnerability **CVE-2024-9164**, with a CVSS score of 9.6, allows unauthorised users to execute pipelines on branches without appropriate permission, leading to unauthorised code execution.

The vulnerability **CVE-2024-8970**, with a CVSS score of 8.2, allows an attacker to trigger a pipeline as another user under certain conditions, leading to potential unauthorised actions.

The vulnerability **CVE-2024-8977**, with a CVSS score of 8.2, is a Server-Side Request Forgery (SSRF) vulnerability in the Analytics Dashboard, allowing attackers to make unauthorised network requests.

Affected Products

GitLab CE/EE versions from 8.16 up to 17.4.1.

Recommendations

It is highly recommended updating affected assets to the latest version as soon as possible.

References

[1] https://about.gitlab.com/releases/2024/10/09/patch-release-gitlab-17-4-2-released/#run-pipelines-on-arbitrary-branches