ADV2024_332 GitLab Security Advisory (October 1st, 2024)

GitLab has published a security advisory highlighting vulnerabilities in the following products on September 25th, 2024. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- GitLab Community Edition (CE) – versions prior to 4.1, 17.3.4, 17.2.8, 16.10.10, 16.9.11, 16.8.10, 16.7.10, 16.6.10, 16.5.10, 16.4.7, 16.3.9, 16.2.11, 16.1.8 and 16.0.10
- GitLab Enterprise Edition (EE) – versions prior to 17.4.1, 17.3.4, 17.2.8, 16.10.10, 16.9.11, 16.8.10, 16.7.10, 16.6.10, 16.5.10, 16.4.7, 16.3.9, 16.2.11, 16.1.8 and 16.0.10

For more information on these updates, you can follow these URLs:

- GitLab Critical Patch Release: 16.10.10, 16.9.11, 16.8.10, 16.7.10, 16.6.10, 16.5.10, 16.4.7, 16.3.9, 16.2.11, 16.1.8, 16.0.10
- GitLab Patch Release: 17.4.1, 17.3.4, 17.2.8

The Guyana National CIRT recommends that users and administrators review this update and apply it where necessary.

References

- GitLab Releases. (September 25th, 2024). Retrieved from GitLab. https://about.gitlab.com/releases/categories/releases/
- GitLab Security Advisory. (September 26th, 2024). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/gitlab-security-advisory-av24-543