September 12, 2024

Overall Rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware GitLab published security advisories to address a critical vulnerability in the following products:

- GitLab Community Edition (CE) – versions prior to 17.3.2, 17.2.5, and 17.1.7
- GitLab Enterprise Edition (EE) – versions prior to 17.3.2, 17.2.5, and 17.1.7

Technical Details

An issue was discovered in GitLab CE/EE affecting all versions starting from 8.14 prior to 17.1.7, starting from 17.2 prior to 17.2.5, and starting from 17.3 prior to 17.3.2, which allows an attacker to trigger a pipeline as an arbitrary user under certain circumstances. This is a critical severity issue (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H, 9.9). It is now mitigated in the latest release and is assigned CVE-2024-6678.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

References

- CVE-2024-6678 CVE-2024-8640 CVE-2024-8635 CVE-2024-8124 CVE-2024-8641 CVE-2024-8311 CVE-2024-4660 CVE-2024-4283 CVE-2024-4612 CVE-2024-8631 CVE-2024-2743 CVE-2024-5435 CVE-2024-6389 CVE-2024-4472 CVE-2024-6446. CVE-2024-6685
- GitLab Critical Patch Release: 17.3.2, 17.2.4 and 17.1.7
- GitLab Releases