July 11, 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 of a recently released update by GitLab security advisory to address a critical vulnerability in the following products:

- GitLab Community Edition (CE) – versions prior to 17.1.2, 17.0.4 and 16.11.6
- GitLab Enterprise Edition (EE) – versions prior to 17.1.2, 17.0.4 and 16.11.6

Technical Details

GitLab warned today that a critical vulnerability in its product's GitLab Community and Enterprise editions allows attackers to run pipeline jobs as any other user.

The GitLab DevSecOps platform has over 30 million registered users and is used by over 50% of Fortune 100 companies, including T-Mobile, Goldman Sachs, Airbus, Lockheed Martin, Nvidia, and UBS.

The flaw patched in today's security update is tracked as CVE-2024-6385, and it received a CVSS base score severity rating of 9.6 out of 10.

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-2024-6397 CVE-2024-5257 CVE-2024-5470**
- GitLab Critical Patch Release: 17.1.2, 17.0.4, 16.11.6
- **GitLab: Critical bug lets attackers run pipelines as other users (bleepingcomputer.com)**