BRITISH COLUMBIA

**********************************************************************

**Number: AL24-002**
**Date: January 15, 2024**

## Audience

**This Alert is intended for IT professionals and managers.**

## Purpose

An Alert is used to raise awareness of a recently identified cyber threat that may impact cyber information assets, and to provide additional detection and mitigation advice to recipients. The Canadian Centre for Cyber Security ("Cyber Centre") is also available to provide additional assistance regarding the content of this Alert to recipients as requested.

## Details

On January 11, the Cyber Centre became aware of critical vulnerabilities impacting multiple versions of GitLab Community Edition (CE) and GitLab Enterprise Edition (EE). CVE-2023-7028, a vulnerability which permits account take over via password reset emails was rated the maximum CVSS (Common Vulnerability Scoring System) score of 10[Footnote1]. On January 12 the Cyber Centre published AV24-025 which highlighted the vulnerabilities and encouraged readers to patch at their earliest opportunity[Footnote2]. Later that day, the Cyber Centre became aware of multiple proof of concepts which look to exploit CVE-2023-7028. There is an elevated risk that targeted exploitation will soon impact self-managed GitLab services.

The following versions of GitLab self-managed instances are impacted:

- 16.1 to 16.1.5
- 16.2 to 16.2.8
- 16.3 to 16.3.6
- 16.4 to 16.4.4
- 16.5 to 16.5.5
- 16.6 to 16.6.3
- 16.7 to 16.7.1

## Suggested actions.

The Cyber Centre strongly recommends that:

- Any organizations using affected version of GitLab should ensure that the service is inaccessible until patches are installed.
    - GitLab encourages users to not skip upgrade stops as this could create instability, with 16.3.x being a required upgrade stop.
- While CVE-2023-7028 may still result in a successful password reset, the implementation of two factor authentication (2FA) will deny malicious actors access to compromised accounts. Enforcing 2FA will help to ensure that malicious actors cannot login with compromised credentials.

- Organizations should review and implement the Cyber Centre’s Top 10 IT Security Actions[Footnote3] with an emphasis on the following topics:
    - Consolidating, monitoring, and defending Internet gateways.
    - Patching operating systems and applications.
    - Segmenting and separating information.
    - Protecting information at the enterprise level.

If activity matching the content of this alert is discovered, recipients are encouraged to report via the My Cyber Portal, or email contact@cyber.gc.ca.

## References

**Footnote 1**

GitLab Critical Security Release: 16.7.2, 16.6.4, 16.5.6

**Footnote 2**

GitLab security advisory (AV24-025)

**Footnote 3**

Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)

*****************************************************************