December 13, 2023

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware GitLab published a security advisory to address vulnerabilities in the following products:

- GitLab Community Edition (CE) – multiple versions
- GitLab Enterprise Edition (EE) – multiple versions

Technical Details

An improper certificate validation issue in Smartcard authentication in GitLab EE affecting all versions from 11.6 prior to 16.4.4, 16.5 prior to 16.5.4, and 16.6 prior to 16.6.2 allows an attacker to authenticate as another user given their public key if they use Smartcard authentication. Smartcard authentication is an experimental feature and must be manually enabled by an administrator.

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-6680, CVE-2023-6564, CVE-2023-6051, CVE-2023-3907, CVE-2023-5512, CVE-2023-3904, CVE-2023-5061
- GitLab Security Advisory
- GitLab Releases