February 21, 2024

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 that GitLab published a security advisory to address vulnerabilities in the following products:

- GitLab Community Edition (CE) – versions prior to 16.9.1, 16.8.3 and 16.7.6
- GitLab Enterprise Edition (EE) – versions prior to 16.9.1, 16.8.3 and 16.7.6

Technical Details

GitLab releases patches for vulnerabilities in dedicated security releases. There are two types of security releases: a monthly, scheduled security release, released a week after the feature release (which deploys on the 3rd Thursday of each month), and ad-hoc security releases for critical vulnerabilities. For more information, you can visit our security FAQ. You can see all of our regular and security release blog posts here. In addition, the issues detailing each vulnerability are made public on our issue tracker 30 days after the release in which they were patched.

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-2024-1451 CVE-2023-6477 CVE-2023-6736 CVE-2024-1525 CVE-2023-4895 CVE-2024-0861 CVE-2023-3509 CVE-2024-0410
- GitLab Security Advisory
- GitLab Releases