March 28, 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 16.10.1, 16.9.3 and 16.8.5
- GitLab Enterprise Edition (EE) – versions prior to 16.10.1, 16.9.3 and 16.8.5

Technical Details

An issue has been discovered in GitLab CE/EE affecting all versions before 16.8.5, all versions starting from 16.9 before 16.9.3, all versions starting from 16.10 before 16.10.1. A wiki page with a crafted payload may lead to a Stored XSS, allowing attackers to perform arbitrary actions on behalf of victims. This is a high severity issue (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N, 8.7). It is now mitigated in the latest release and is assigned CVE-2023-6371..

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-2023-6371 CVE-2024-2818
- GitLab Security Advisory
- GitLab Releases