May 23, 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 0.1, 16.11.3 and 16.10.6
- GitLab Enterprise Edition (EE) – versions prior to 17.0.1, 16.11.3 and 16.10.6

Technical Details

A XSS condition exists within GitLab in versions 15.11 before 16.10.6, 16.11 before 16.11.3, and 17.0 before 17.0.1. By leveraging this condition, an attacker can craft a malicious page to exfiltrate sensitive user information. This is a high severity issue (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N, 8.0) It is now mitigated in the latest release and is assigned CVE-2024-4835.

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-2024-4835 CVE-2024-2874 CVE-2023-7045 CVE-2023-6502 CVE-2024-1947
- GitLab Patch Release: 17.0.1, 16.11.3, 16.10.6
- GitLab Releases