June 26, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of GitLab published a security advisory to address critical vulnerabilities in the following products::

- GitLab Community Edition (CE) – versions prior to 1.1, 17.0.3 and 16.11.5
- GitLab Enterprise Edition (EE) – versions prior to 1.1, 17.0.3 and 16.11.5

Technical Details

An issue has been discovered in GitLab CE/EE affecting all versions from 16.1.0 before 16.11.5, all versions starting from 17.0 before 17.0.3, all versions starting from 17.1.0 before 17.1.1 which allowed for a CSRF attack on GitLab's GraphQL API leading to the execution of arbitrary GraphQL mutations. This is a high severity issue

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at VulnerabilityandRiskManagement@gov.bc.ca

References

- CVE-2024-4901 CVE-2024-4994 CVE-2024-6323 CVE-2024-2177 CVE-2024-5430 CVE-2024-4025 CVE-2024-3959 CVE-2024-4557 CVE-2024-1493 CVE-2024-1816 CVE-2024-2191 CVE-2024-3115 CVE-2024-4011
- GitLab Critical Patch Release: 17.1.1, 17.0.3, 16.11.5
- GitLab Releases