January 12, 2024

Overall rating: Critical

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a GitLab critical security release The vulnerabilities affect GitLab versions prior to 16.7.2, 16.6.4, 16.5.6 for GitLab Community Edition (CE) and Enterprise Edition (EE).

Technical Details

A critical issue has been discovered in GitLab CE/EE affecting all versions from 16.1 prior to 16.1.6, 16.2 prior to 16.2.9, 16.3 prior to 16.3.7, 16.4 prior to 16.4.5, 16.5 prior to 16.5.6, 16.6 prior to 16.6.4, and 16.7 prior to 16.7.2 in which user account password reset emails could be delivered to an unverified email address.

Additionally, a critical incorrect authorization checks in GitLab CE/EE from all versions starting from 8.13 before 16.5.6, all versions starting from 16.6 before 16.6.4, all versions starting from 16.7 before 16.7.2, allows a user to abuse Slack/Mattermost integrations to execute slash commands as another user.

A high-risk issue has been discovered in GitLab affecting all versions starting from 15.3 before 16.5.5, all versions starting from 16.6 before 16.6.4, all versions starting from 16.7 before 16.7.2. The required CODEOWNERS approval could be bypassed by adding changes to a previously approved merge request. This is a high severity issue.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

These vulnerabilities are rated as a **CRITICAL** 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.

References

- CVE-2023-7028, CVE-2023-5356, CVE-2023-4812, CVE-2023-6955, CVE-2023-2030
- GitLab Critical Security Release: 16.7.2, 16.6.4, 16.5.6
- VRM Vulnerability Reports