March 6, 2024

Overall Rating - High

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 16.9.2, 16.8.4 and 16.7.7
- GitLab Enterprise Edition (EE) – versions prior to 16.9.2, 16.8.4 and 16.7.7

Technical Details

An authorization bypass vulnerability was discovered in GitLab affecting versions 11.3 prior to 16.7.7, 16.7.6 prior to 16.8.4, and 16.8.3 prior to 16.9.2. An attacker could bypass CODEOWNERS by utilizing a crafted payload in an old feature branch to perform malicious actions. This is a high severity issue.

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-2024-0199 CVE-2024-1299.
- .GitLab Security Advisory
- GitLab Releases