November 30, 2023

Overall Rating - High

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware GitLab published a security advisory to address vulnerabilities in the following products:

- GitLab Community Edition (CE) – multiple versions
- GitLab Enterprise Edition (EE) – multiple versions

Technical Details

Improper neutralization of input in Jira integration configuration in GitLab CE/EE, affecting all versions from 15.10 prior to 16.6.1, 16.5 prior to 16.5.3, and 16.4 prior to 16.4.3 allowed attacker to execute javascript in victim's browser.

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-2023-6033.

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-2023-6033, CVE-2023-6396
- GitLab Security Advisory