CVE-2024-3303:

GITLAB IMPROPER NEUTRALIZATION OF INPUT USED FOR LLM PROMPTING

Vairav Advisory Report

Date: 2025-02-13

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: mail@vairavtech.com

EXECUTIVE SUMMARY

A vulnerability identified as CVE-2024-3303 has been discovered in GitLab Enterprise Edition (EE), affecting versions from 16.0 up to but not including 17.6.5, from 17.7 up to but not including 17.7.4, and from 17.8 up to but not including 17.8.2. This vulnerability allows an attacker to exfiltrate contents of a private issue using prompt injection. The severity of this vulnerability is rated as Medium, with a CVSS score of 6.4. Exploitation of this vulnerability could lead to unauthorized access and leakage of sensitive information contained within private issues.

VULNERABILITY DETAILS

CVE-2024-3303

- **Description:** This vulnerability arises from improper handling of user inputs within GitLab EE's issue tracking system. An attacker can exploit this flaw by crafting malicious inputs that, when processed, allow unauthorized access to the contents of private issues. The root cause is insufficient input validation, leading to prompt injection vulnerabilities.
- **Impact:** Successful exploitation enables attackers to access and exfiltrate sensitive information from private issues, potentially leading to information disclosure and unauthorized data access.
- **CVSS Score:** 6.4 (Medium)

AFFECTED VERSIONS

GitLab EE versions affected by this vulnerability include:

- 16.0 and later, prior to 17.6.5
- 17.7 and later, prior to 17.7.4
- 17.8 and later, prior to 17.8.2

EXPLOIT DETAILS

In environments where GitLab EE is utilized for issue tracking and project management, an attacker with access to the system can perform prompt injection attacks by submitting specially crafted inputs. These inputs exploit the vulnerability, allowing the attacker to retrieve and exfiltrate the contents of private issues without proper authorization. This poses significant risks, especially in scenarios where private issues contain confidential or sensitive information.

RECOMMENDED ACTIONS

Patch & Upgrade:

It is strongly recommended to upgrade to the latest versions of GitLab EE to mitigate this vulnerability:

- 17.6.5
- 17.7.4
- 17.8.2

ADDITIONAL SECURITY MEASURES

- **Input Validation**: Implement strict input validation to ensure that all user inputs are properly sanitized and validated before processing.
- **Access Controls**: Review and enforce access controls to ensure that only authorized users have access to private issues and sensitive information.
- **Monitoring and Logging**: Enable comprehensive logging and monitoring to detect and respond to unauthorized access attempts or suspicious activities promptly.

REFERENCES

- https://app.opencve.io/cve/CVE-2024-3303
- https://nvd.nist.gov/vuln/detail/CVE-2024-3303

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com