GitLab Security Patch Release: Critical Fixes for XSS and Authorization Vulnerabilities

Vairav Advisory Report

Date: February 27, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

GitLab has released critical security patches for its Community Edition (CE) and Enterprise Edition (EE) in versions 17.9.1, 17.8.4, and 17.7.6. These updates address multiple vulnerabilities, including Cross-Site Scripting (XSS) issues, improper authorization, and HTML injection risks. Organizations using affected versions should upgrade immediately to prevent potential exploits. GitLab.com is already running the patched versions, and GitLab Dedicated customers do not need to take any action.

VULNERABILITY DETAILS

CVE-2025-0475: XSS in k8s Proxy Endpoint

Description: A proxy feature could allow unintended content rendering, leading to potential XSS attacks under specific conditions.

Impact: Unauthorized script execution, data exposure.

CVSS Score: 8.7 (Critical)

CVE-2025-0555: XSS Maven Dependency Proxy

Description: A Cross-Site Scripting (XSS) vulnerability in the Maven Dependency Proxy could allow an attacker to bypass security controls and execute arbitrary scripts in a user's browser.

Impact: Remote script execution, unauthorized access.

CVSS Score: 7.7 (High)

CVE-2024-8186: HTML Injection

Description: An attacker could inject HTML into the child item search, leading to potential XSS in certain situations.

Impact: Unauthorized script execution, user data compromise.

CVSS Score: 5.4 (Medium)

CVE-2024-10925: Improper Authorization Check

Description: A guest user could read the security policy YAML due to an improper authorization check.

Impact: Information disclosure, unauthorized access.

CVSS Score: 5.3 (Medium)

CVE-2025-0307

Description: Improper authorization allowed users with limited permissions to access potentially sensitive project analytics data.

Impact: Data leakage, unauthorized access.

CVSS Score: 4.3 (Medium)

AFFECTED VERSIONS

GitLab versions:

- 15.10 up to but not including 17.7.6
- 16.6 up to but not including 17.8.4
- 17.7 up to but not including 17.9.1

EXPLOIT DETAILS

Attackers can exploit these vulnerabilities by leveraging XSS and HTML injection techniques to execute malicious scripts, manipulate user sessions, and access unauthorized data. The improper authorization flaws allow unauthorized users to view sensitive security policies and project analytics. If chained together, these vulnerabilities could enable persistent access, data exfiltration, or privilege escalation.

RECOMMENDED ACTIONS

- GitLab urges users to upgrade to the latest secure versions: 17.9.1, 17.8.4, 17.7.6.

ADDITIONAL SECURITY MEASURES

- Restrict access to sensitive project resources.
- Enable security policies to mitigate XSS attacks.

REFERENCES

https://securityonline.info/cve-2025-0475-cve-2025-0555-gitlabs-high-risk-patch-now/

https://about.gitlab.com/releases/2025/02/26/patch-release-gitlab-17-9-1-released/

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