GITLAB PATCH RELEASE 17.11.1 FIXES CRITICAL XSS, HEADER INJECTION, AND ACCESS CONTROL VULNERABILITIES

Vairav CVE Report

Date: April 24, 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 updates for GitLab Community and Enterprise Editions, addressing multiple high-severity vulnerabilities including XSS flaws and a Network Error Logging (NEL) injection that could lead to account takeover. Versions 17.11.1, 17.10.5, and 17.9.7 are now available and users are urged to upgrade immediately.

VULNERABILITY DETAILS

CVE-2025-1763: XSS in Maven Dependency Proxy

Description: GitLab EE failed to sanitize content security policy (CSP) directives properly in the Maven Dependency Proxy feature, allowing attackers to inject malicious scripts.

Impact: XSS and content security policy bypass under specific conditions.

CVSS Score: 8.7 (High)

CVE-2025-2443: XSS via Maven Dependency Proxy

Description: Improper validation of cache header values in the Maven Dependency Proxy allows malicious scripts to be injected in specific scenarios.

Impact: XSS that may compromise user sessions.

CVSS Score: 8.7 (High)

CVE-2025-1908: NEL Header Injection in Maven Dependency Proxy

Description: Missing input validation in NEL headers could allow attackers to insert malicious logging directives.

Impact: This could lead to a full account takeover through user tracking.

CVSS Score: 7.7 (High)

CVE-2025-0639: Denial of Service via Issue Preview

Description: A flaw in issue rendering logic can be exploited via malformed previews to trigger unavailability.

Impact: Temporary disruption of the GitLab instance due to a service crash.

CVSS Score: 6.5 (Medium)

CVE-2024-12244: Unauthorized Access to Branch Names

Description: GitLab CE/EE does not properly restrict access to branch names when repository assets are disabled

Impact: Unauthorized access to project metadata.

CVSS Score: 4.3 (Medium)

AFFECTED PRODUCTS/VERSIONS

- GitLab 16.6 < 17.9.7
- GitLab 17.10 < 17.10.5
- GitLab 17.11 < 17.11.1

EXPLOIT DETAILS

- **CVE-2025-1763 / CVE-2025-2443:** Exploitable via crafted dependency proxy responses.
- **CVE-2025-1908:** Injected NEL headers can monitor user browsing.
- **CVE-2025-0639:** Exploitable through malformed issue previews.
- **CVE-2024-12244:** Exploitable by querying repositories with disabled assets.

RECOMMENDATIONS

- Upgrade immediately to GitLab CE/EE versions 17.11.1, 17.10.5, or 17.9.7.
- Review access logs and user permissions to identify suspicious behavior.
- Sanitize input fields in custom integrations.
- Audit dependency proxy configurations and NEL settings.

Regular upgrades and monitoring are essential to maintaining the integrity of self-managed GitLab instances.

REFERENCES

https://about.gitlab.com/releases/2025/04/23/patch-release-gitlab-17-11-1-released/
https://securityonline.info/gitlab-releases-security-update-to-patch-xss-and-account-takeover-flaws/

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