Multiple GitLab Vulnerabilities Allow Account Takeover and Stored XSS At

Data: 2025-08-13 13:11:48

Autor: Inteligência Against Invaders

GitLab has released critical security patches addressing multiple high-severity vulnerabilities that could enable attackers to execute account takeovers and stored cross-site scripting (XSS) attacks across both Community Edition (CE) and Enterprise Edition (EE) platforms.

The vulnerabilities, disclosed in patch releases 18.2.2, 18.1.4, and 18.0.6, represent serious security risks that require immediate attention from administrators.

Critical Security Flaws Enable Account Compromise

The most concerning vulnerabilities involve multiple cross-site scripting flaws that could allow authenticated attackers to execute malicious actions on behalf of other users.

CVE-2025-6186, rated with a CVSS score of 8.7, specifically enables account takeover by allowing authenticated users to inject malicious HTML content into work item names.

This vulnerability affects GitLab CE/EE versions 18.1 before 18.1.4 and 18.2 before 18.2.2.

CVE ID	Vulnerability Type	Severity	CVSS Score
CVE-2025-7734	Cross-site scripting in blob viewer	High	8.7
CVE-2025-7739	Cross-site scripting in labels	High	8.7
CVE-2025-6186	Cross-site scripting in Workitem	High	8.7
CVE-2025-8094	Improper permissions in project API	High	7.7
CVE-2024-12303	Incorrect privilege assignment	Medium	6.7
CVE-2025-2614	Resource allocation limits bypass	Medium	6.5
CVE-2024-10219	Incorrect authorization in jobs API	Medium	6.5
CVE-2025-8770	Merge request approval bypass	Medium	6.5
CVE-2025-2937	RegEx complexity in wiki	Medium	6.5
CVE-2025-1477	Resource limits in Mattermost integration	Medium	6.5
CVE-2025-5819	Permission assignment	Medium	5.0

CVE ID	Vulnerability Type	Severity	CVSS Score
	in ID token		
CVE-2025-2498	Access control in IP restrictions	Low	3.1

Two additional high-severity XSS vulnerabilities compound the security risks.CVE-2025-7734affects the blob viewer component and impacts all versions from 14.2 before the patched releases, whileCVE-2025-7739targets label descriptions in the most recent 18.2 branch.

Both vulnerabilities carry the same 8.7 CVSS rating and could enable stored cross-site scripting attacks. Beyond XSS vulnerabilities, the patch addresses significant permission handling flaws.

CVE-2025-8094allows authenticated users with maintainer privileges to manipulate shared infrastructure resources beyond their intended access level, potentially causing denial of service to other users' CI/CD pipelines.

This vulnerability affects versions 18.0 before 18.0.6, 18.1 before 18.1.4, and 18.2 before 18.2.2.

Several medium-severity vulnerabilities enable privilege escalation and unauthorized access.

CVE-2024-12303allows users to delete confidential issues through role manipulation, whileCVE-2024-10219permits bypassing access controls to download private artifacts.

Resource exhaustion vulnerabilitiesCVE-2025-2614andCVE-2025-1477could enable denial of service attacks through specially crafted content.

GitLab strongly recommends immediate upgrading to the latest patched versions, as GitLab.com is already running the secured release.

The vulnerabilities were primarily discovered through GitLab's HackerOne bug bounty program, with researchers including joaxcar, yvvdwf, and others contributing to the discoveries.

The comprehensive nature of these vulnerabilities underscores the critical importance of maintaining current GitLab installations and implementing regular security updates.