Alert Bulletin

Bulletin N.: 2024-32
Publication Date: 12/09/2024
Subject: Alert 2024-32 Critical Vulnerability in GitLab
Traffic Light Protocol (TLP): White

GitLab has publicly disclosed several vulnerabilities affecting both the **Community Edition (CE)** and **Enterprise Edition (EE)** in their on-premise implementations, some of which are critical.

One of the most notable is **CVE-2024-6678**, a vulnerability in pipeline job execution. This flaw allows an attacker with low privileges to execute jobs as another user, potentially compromising private repositories and triggering supply chain issues. The vulnerability affects GitLab versions from **8.14** to those prior to **17.1.7**, **17.2.5**, and **17.3.2**, and has a **CVSS score of 9.9**, categorizing it as critical in severity.

For more details on the vulnerabilities and mitigations, visit: GitLab Security Releases.