AL2024_14 GitLab: Critical Vulnerability Allows Attackers to Run Pipelines as Other Users (11th July 2024)

Description

GitLab has recently disclosed a critical security vulnerability affecting its Community and Enterprise editions, posing significant risks to organizations using the platform. The vulnerability, identified as CVE-2024-6385, allows attackers to run pipeline jobs as any user, compromising the integrity and security of the CI/CD processes. With a CVSS base score of 9.6 out of 10, this flaw necessitates immediate attention and action from GitLab administrators.

Attack Details

The vulnerability impacts all GitLab CE/EE versions from 15.8 to 16.11.6, 17.0 to 17.0.4, and 17.1 to 17.1.2. Under undisclosed circumstances, attackers can exploit this flaw to trigger new pipelines as arbitrary users. GitLab pipelines, essential for Continuous Integration/Continuous Deployment (CI/CD) systems, enable the automated running of processes to build, test, or deploy code changes. Exploiting this vulnerability could allow malicious actors to manipulate these processes, leading to potential data breaches and integrity issues.

This critical vulnerability follows the patching of a similar flaw (CVE-2024-5655) in late June and another high-severity vulnerability (CVE-2024-4835) in May, which enabled unauthenticated threat actors to take over accounts through cross-site scripting (XSS) attacks. A zero-click GitLab vulnerability (CVE-2023-7028), actively exploited earlier this year, allowed account hijacking via password resets.

Indicators of Compromise (IOCs)

- Unusual or unexpected pipeline jobs being triggered
- Pipeline jobs being run under different user accounts without proper authorization
- Unauthorized changes in CI/CD environments
- Increased log entries indicating failed or successful exploitation attempts

Recommendations

GitLab has released updates to address this critical security flaw. Administrators are strongly advised to upgrade their installations to the latest versions:

- GitLab Community and Enterprise editions 17.1.2
- GitLab Community and Enterprise editions 17.0.4
- GitLab Community and Enterprise editions 16.11.6

GitLab has emphasized the urgency of these updates: "We strongly recommend that all installations running a version affected by the issues described below are upgraded to the latest version as soon as possible."

In addition to applying the updates, organizations should:

1. **Review and Monitor Pipelines:** Regularly audit pipeline activities for unusual or unauthorized actions.
2. **Enhance Access Controls:** Ensure that user permissions and access controls are appropriately configured to minimize the risk of unauthorized actions.
3. **Implement Multi-Factor Authentication (MFA)**: Strengthen account security by enabling MFA for all user accounts.
4. **Regularly Update Software:** Maintain up-to-date software installations to protect against known vulnerabilities.

Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Gatlan, S. (2024, July 10). GitLab: Critical bug lets attackers run pipelines as other users. Retrieved from *BleepingComputer*. https://www.bleepingcomputer.com/news/security/gitlab-warns-of-critical-bug-that-lets-attackers-run-pipelines-as-an-arbitrary-user/
- The Hacker News. (n.d.). GitLab patches critical flaw allowing unauthorized pipeline jobs. Retrieved from Hackers news. https://thehackernews.com/2024/07/gitlab-patches-critical-flaw-allowing.html