УДК 4.56.52

Разработка методики безопасного автоматизированного обновления серверных приложений на платформе GitLab

Груздев Я.В. (ИТМО), **Щукин А.И.** (ИТМО)
Научный руководитель – кандидат технических наук, доцент Ищенко А.П. (ИТМО)

Введение. В современном мире разработки программного обеспечения инструменты автоматизации, такие как GitLab, играют ключевую роль в ускорении процессов CI/CD. Однако по умолчанию GitLab предоставляет разработчикам обширные привилегии, что открывает потенциальные векторы атак, особенно в контексте автоматизированных систем обновления серверных приложений.

Основная часть. Разработка и деплоймент приложений в среде GitLab сопряжены с рядом задач, направленных на повышение безопасности и управления привилегиями:

1) Предотвращение несанкционированного доступа и эскалации привилегий. Учитывая, что разработчики обладают обширными привилегиями в среде GitLab, повышается угроза безопасности. Это влечёт за собой риск использования этих привилегий для выполнения произвольных скриптов и доступа к хост-серверу, что может быть использовано для атак на системы автоматизированного обновления серверных приложений. [1].
2) Улучшение механизмов развертывания приложений. При стандартной конфигурации GitLab, отсутствие специализированного демона с повышенными привилегиями и широкие возможности для запуска пайплайнов могут привести к риску запуска вредоносного кода на этапе развертывания.
3) Разграничение прав доступа с использованием технологии мультипайплайнов. Так мы обеспечиваем возможность строгого разграничения привилегий и защиты кода пайплайна от неавторизованных изменений, позволяя тем самым улучшить безопасность процессов CI/CD [2]
4) Использование подхода downstream-pipelines для безопасного развертывания, при котором код размещается в отдельном репозитории с ограниченным доступом. При этом минимизируются риски безопасности, связанные с развертыванием, и исключается возможность выполнения произвольного кода.

Выводы. Использование расширенных привилегий в GitLab без должного контроля представляет существенный риск для безопасности. Мультипайплайны и стратегии безопасного развертывания, такие как использование downstream-pipeline, предлагают эффективные подходы к минимизации этих рисков, обеспечивая безопасность и гибкость процессов разработки. Эти меры позволяют компаниям лучше защитить свои системы и данные от потенциальных атак.

Список использованных источников:

1. Cowell C., Lotz N., Timberlake C. "Automating DevOps with GitLab CI/CD Pipelines: Build efficient CI/CD pipelines to verify, secure, and deploy your code using real-life examples." – Packt Publishing, 2023. – ISBN: 978-1-80323-300-0.
2. GitLab Docs. URL: https://docs.gitlab.com (дата обращения: 24.09.2023)