

# Audit

git : [https://github.com/dokpark21/DEX\\_Lending\\_solidity/blob/main/src/Dex.sol](https://github.com/dokpark21/DEX_Lending_solidity/blob/main/src/Dex.sol)

commit : `e6034a6abd48ef304d449807c73c05721046fbcd`

ID	요약	위험도
KYRIE-001	<code>addLiquidity</code> 함수에서 유동성 비율 계산 없이 유동성 풀에 추가됩니다.	High

## Description

`addLiquidity` 함수는 사용자가 두 개의 토큰( `amountX` 와 `amountY` )을 제공하여 유동성 풀에 추가할 때, 현재 유동성 풀의 비율에 따라 `amountX` 와 `amountY` 를 계산하지 않고 바로 추가합니다. 이는 유동성 풀의 균형을 고려하지 않은 방식입니다.

## Impact

### High

공격자가 풀의 비율을 조작하려면 **상당한 자산이 필요**하며, 이로 인해 공격 비용이 높을 수 있습니다.

하지만 풀 비율을 충분히 조작시킬 수 있다면, 공격자는 막대한 이익을 얻을 수 있습니다.

## Recommendation

- 유동성 풀 비율 검증 로직 추가

ID	요약	위험도
KYRIE-002	<code>removeLiquidity</code> 함수는 유동성 공급자 개인의 LP 토큰량을 검증하지 않고 전체 LP 토큰량만 검증합니다.	information

## Description

`removeLiquidity` 함수는 유동성 공급자 개인의 LP 토큰량을 검증하지 않고 전체 LP 토큰량만 검증합니다.

이로 인해 사용자가 개인의 LP 토큰량을 초과하여 함수 호출을 시도할 경우, 불필요한 가스비를 추가로 소모하게 됩니다.

## Impact

### information

함수 호출을 실패하는 경우 불필요한 가스비를 소모합니다.

## Recommendation

- 유동성 풀에서 제거하려는 개인 LP 토큰량에 대한 검증 로직을 구현