

Audit

git : https://github.com/hakid29/Dex_solidity/blob/main/src/Dex.sol

commit : `0f49cc9c5179fd611c90028dc67f8a10378d23b8`

ID	요약	위험도
HAKID-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 교란하려면 상당한 자산이 필요할 수 있으며, 공격 비용이 높을 수 있습니다. 그러나 풀 비율을 충분히 교란시킬 수 있는 경우, 공격자는 큰 이익을 취할 수 있습니다.

또한 공격 자체가 단순하지 않지만, 성공했을 때 재정적 피해가 크고, 서비스 운영에 미치는 영향이 매우 큽니다.

Recommendation

- 유동성 풀 비율 검증 로직 추가