Audit

git : https://github.com/55hnnn/DEX_solidity/blob/main/src/Dex.sol

commit : `8fdc0461ab492fbdf2edc2572c1492e30e312326`

ID	요약	위험도
KENNY-001	`addLiquidity` 함수에서 유동성 비율 계산 없이 유동성 풀에 추가됩니다.	High

Description

`addLiquidity` 함수는 사용자가 두 개의 토큰(`amountX` , `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
KENNY-002	실제 LP 토큰을 발행하거나 소각하는 과정이 존재하지 않습니다.	Critical

Description

이 컨트랙트에서는 LP 토큰을 발행하거나 소각하는 로직이 존재하지 않고 LP 토큰에 대한 수치만 증가합니다.

Impact

Critical

LP 토큰이 없으면 유동성 제공자의 지분은 DEX 내에서만 유효하며, 외부에서 거래나 양도가 불가능해집니다.

Recommendation

- `addLiquidity`와 `removeLiquidity` 에 각각 토큰을 발행하고 소각하는 로직을 구현

ID	요약	위험도
KENNY-003	`addLiquidity` 함수 호출 실패시 불필요한 가스비가 발생하게 됩니다.	Information

Description

`addLiquidity` 함수를 호출할 때, 복잡한 수학적 연산 후에 토큰의 `allowance`와 `balanceOf` 조건을 확인합니다. 이로 인해 조건에 부합하지 않는 경우 불필요한 가스비가 발생합니다.

Impact

Information

조건에 부합하지 않는 경우 불필요한 가스비가 발생합니다.

Recommendation

- `require` 문을 코드 앞쪽에 배치시켜 함수 호출시 바로 token에 대한 조건들을 확인하도록 구현