Audit

git : https://github.com/Null0RM/DEX_solidity/blob/main/src/Dex.sol

commit : `abefae97824326faff03b0ba4d6358438766b0bb`

ID	요약	위험도
NULL-001	`transferFrom` 함수에서 다른 사용자의 LP 토큰을 소유자가 아닌 사람이 소각할 수 있습니다.	Critical

Description

`Dex` 컨트랙트에서 `transferFrom` 함수는 `to == address(this)` 조건만 확인하고 있어서 다른 사용자의 LP 토큰을 소유자가 아닌 사람이 소각할 수 있습니다.

Impact

Critical

공격자가 `Dex` 컨트랙트 유동성 공급자 주소를 알고 있다면 해당 공급자의 모든 LP 토큰을 제거할 수 있습니다.

Recommendation

- `transferFrom` 함수의 `from` 주소가 `msg.sender` 일 때만 호출 가능하도록 하는 조건을 추가

ID	요약	위험도
NULL-002	`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