Audit

git : https://github.com/gloomydumber/DEX_solidity/blob/master/src/Dex.sol

commit : `1671f2f3a6a272387b4a884e92f9724563d9cb15`

ID	요약	위험도
Damon-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
Damon-002	유동성 공급없이 LP 토큰을 발급할 수 있습니다.	Critical

Description

`update` , `mint` 함수를 외부에서 누구나 호출할 수 있습니다.

`update` 함수를 호출해서 `reserveX` , `reserveY` 값을 조작하고 `mint` 함수를 호출하여 `addLiquidity` 함수 호출 없이 LP 토큰을 발급 받을 수 있게됩니다.

Impact

Critical

공격자가 공격 비용 없이 원하는 만큼 LP 토큰을 발급받을 수 있습니다.

Recommendation

- `update` , `mint` 함수를 `internal` 또는 `private` 으로 수정