

Contracts vulnerabilities

Vulnerabilities list:

Contracts vulnerabilities	1
Vulnerabilities list:	1
Involved contracts and level of the bugs	1
Vulnerabilities	1
1. Withdraw function	1

Involved contracts and level of the bugs

The present document aims to point out some vulnerabilities in the contracts.

Vulnerabilities

1. Withdraw function

Severity: Medium

The following method is implemented in the [liquidity_lockbox_v1](#) program:

```
withdraw(  
    ctx: Context<WithdrawLiquidityForTokens>,  
    id: u32,  
    amount: u64,  
    token_min_a: u64,  
    token_min_b: u64  
)
```

This method facilitates a liquidation process, enabling users to exchange a designated quantity of fungible tokens, which represent liquidity NFTs within the contract, for the corresponding liquidated assets tied to those liquidity NFTs. However, the current implementation of this method presents certain issues.

1. When attempting multiple withdrawals from either the same position or with the same identifier (id), the method encounters difficulties. Specifically, starting from

the second withdrawal, any subsequent attempt to withdraw a specified amount from the same position or with the same id, lacking sufficient liquidity to support multiple withdrawals, results in a failure.

2. Users retain the flexibility to choose both the position and identifier (id) from which they intend to withdraw. A crucial point to note is that a user may select a position with higher liquidity than required. This choice can force a user with a larger amount of fungible tokens to do multiple withdrawals.