Smart contract security audit

Defibay

v.1.0

Table of Contents

1.0 Introduction

1.1 Project engagement

During November of 2021, Defibay engaged CTDSec to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. Defibay provided CTDSec with access to their code repository and whitepaper.

1.2 Disclaimer

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract, rather limited to an assessment of the logic and implementation. In order to ensure a secure contract that's able to withstand the network's fast-paced and rapidly changing environment, we at CTDSec recommend that Defibay team put in place a bug bounty program to encourage further and active analysis of the smart contract.

2.0 Coverage

2.1 Target Code and Revision

For this audit, we performed research, investigation, and review of the Defibay contract followed by issue reporting, along with mitigation and remediation instructions outlined in this report. The following code files are considered in-scope for the review:

Source:

https://bscscan.com/address/0xFC563895C1D5BB779685fB3d2ec09f5Fa5B6473c#code

2.2 Attacks made to the contract

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices.

№	Issue description.	Checking status
1	Compiler warnings.	PASSED
2	Race conditions and Reentrancy. Cross-function race conditions.	PASSED
3	Possible delays in data delivery.	PASSED
4	Oracle calls.	PASSED
5	Front running.	LOW ISSUES
6	Timestamp dependence.	PASSED
7	Integer Overflow and Underflow.	PASSED
8	DoS with Revert.	PASSED
9	DoS with block gas limit.	LOW ISSUES
10	Methods execution permissions.	PASSED
11	Economy model. If application logic is based on an incorrect economic model, the application would not function correctly and participants would incur financial losses. This type of issue is most often found in bonus rewards systems, Staking and Farming contracts, Vault and Vesting contracts, etc.	PASSED
12	The impact of the exchange rate on the logic.	PASSED
13	Private user data leaks.	PASSED
14	Malicious Event log.	PASSED
15	Scoping and Declarations.	PASSED
16	Uninitialized storage pointers.	PASSED
17	Arithmetic accuracy.	PASSED

18	Design Logic.	PASSED
19	Cross-function race conditions.	PASSED
20	Safe Zeppelin module.	PASSED
21	Fallback function security.	PASSED
22	Overpowered functions / Owner privileges	MEDIUM ISSUES

3.0 Security Issues

3.1 High severity issues [0]

No high severity issues found.

3.2 Medium severity issues [1]

1. Centralization:

Owner has authority over the next functions:

setSwapTokensAtAmount()

setMaxTxAmount(): We recommend to add a limit as if the MaxTXamount is 0 trading will be disabled.

setSwapEnable()

excludeFromFees()

setAutomatedMarketMakerPair()

setWalletsFee()

setWallets()

Any compromise to the owner account may allow the hacker to take advantage of this and change the above significant states of the contract.

Recommendation:

-Add a time lock on privileged operations.

-Use a multisig wallet to prevent SPOF on the Private Key.

-Introduce DAO mechanism for owner functions (will add transparency and user involvement).

3.3 Low severity issues [2]

1. Sandwich attack

A sandwich attack might happen when an attacker observes a transaction swapping tokens or adding liquidity without setting restrictions on slippage or minimum output amount. The attacker can manipulate the exchange rate by frontrunning (before the transaction being attacked) a transaction to purchase one of the assets and make profits by backrunning (after the transaction being attacked) a transaction to sell the asset, this can happen on large input amounts.

Recommendation:

It's better to set a reasonable minimum output amount, instead of 0 based on token price when you call uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens.

```
function swapTokensForBNB(uint256 tokenAmount) private {
    address[] memory path = new address[](3);
    path[0] = address(this);
    path[1] = BUSDAddress;
    path[2] = pancakeSwapV2Router.WETH();

    _approve(address(this), address(pancakeSwapV2Router), tokenAmount);
    pancakeSwapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount, 0, path, address(this), block.timestamp);
}
```

2. Out of gas

a) The function _transfer() uses a loop to add balances of each wallet. Function will be aborted with OUT_OF_GAS exception if there will be a long amount of addresses listed.

b) The function _setwallets() uses a loop to add length of each wallet. Function will be aborted with OUT_OF_GAS exception if there will be a long amount of addresses listed.

Recommendation:

Check that the arrays can’t be so big.

4.0 Summary of the audit

Contract has low & medium issues and is safe to be deployed.