Pokeswap Smart Contract
Final Security Auditing Report

长亭科技
CHAITIN

BEIJING CHAITIN TECHNOLOGY Co.,Ltd.
Oct 27, 2020

科技有限公司

Copyright Notice

Table of Contents

1. Disclaimer

Except for discussion purposes only, this audit makes no statements or warranties about the utility of the code, safety of the code, suitability of the business model, regulatory regime for the business model, or any other statements about the fitness of the contracts to purpose, or their bug-free status.

2. Summary

Under the authorization of POKESWAP, the security service group of Beijing Chaitin Technology Co., Ltd. conducted this security audit for Pokeswap Smart Contract project from October 16, 2020 to October 27, 2020, including security review and repair review. The medium and high severity vulnerabilities found in the last round have been fixed in this round of code review.

Project manager: Kun.Yang.
Blockchain team contact information: blockchain@chaitin.com

The scope of the audit was defined in the agreement with POKESWAP,
The auditing version used during the first round of security review is:
commit 97623d6483874f61b69d3877bd5a327487b08125
The auditing version used during the last round of repair review is:
commit ba4ad3c72c118a2b184b1e81887bf95a38d2dc29

3. Security Checklist

No.	Type	Check Item	Result
1.	Types and Keyword	Data Type	PASS
2.		Function Type	PASS
3.		Reference Type	PASS
4.		Type Conversion	PASS
5.	Access control	Visibility Settings	PASS
6.		Owner Access Control	PASS
7.		Relay Contract Access Control	PASS
8.	DoS	Unexpected Revert	PASS
9.		Gas Limit Exceed	PASS
10.	Expressions and Control Structure	Signature Verification	PASS
11.		Precision	PASS
12.		Random Number Generator	PASS
13.		Operator	PASS
14.		Internal / External Function Call	PASS

No.	Type	Check Item	Result
15.		Unchecked Return Values	PASS
16.		Code Logic Order	PASS
17.		Reordering Attack	PASS
18.		Replay Attack	PASS
19.		Error Handling	PASS
20.	External Entity Dependency and Interaction	Transactions Order	PASS
21.		Timestamp	PASS
22.		Oracle	PASS
23.		External Contract Reference / Calling	PASS
24.		Multiple inheritance contract execution order	PASS
25.		Short Address Attack	PASS
26.	Customized Checklist	Unexpected ETH	PASS
27.		Uninitialized storage pointer	PASS
28.		Scope of Variables With the Same Name	PASS
29.		Compiler Version	PASS
30.		sensitive information leakage	PASS
31.		Check-Effects-Interactions Coding Standards	PASS
32.	Optimization	Gas Optimization	PASS
33.		Security Component	PASS
34.		Redundant logic	PASS
35.		Modifiers and Syntactic Sugar	PASS
36.		Canonical naming	PASS
37.		Typo	PASS
38.		Reasonable comment	PASS

4. Low Severity Vulnerability

4.1. BallsBar's Reward unexpected decrease

4.1.1. Description

In PokeRouter.sol, BallsBar rewards pool collects Balls token which is exchanged by 0.05% of the Swap trade amount.

contracts/PokeRouter.sol, L260-L285:

```
      function _toBuyPlatToken(address _sender,address _token, uint
_amount ,address[] memory path) internal {
          ...
              uint[] memory amounts = PokeLibrary.getAmountsOut(factory,
_amount, path);
          ...
          TransferHelper.safeTransfer( ballsToken, stakingAddress,
IERC20(ballsToken).balanceOf(address(this)));
      }
```

However, when your token switch to Balls tokens, you will be charged an additional 0.25% of the trade amount.

The fee is calculated as following:

contracts/PokeRouter.sol, L260-L285:

```
   function getAmountOut(uint amountIn, uint reserveIn, uint reserveOut)
internal pure returns (uint amountOut) {
          ...
          uint amountInWithFee = amountIn.mul(9975);
          uint numerator = amountInWithFee.mul(reserveOut);
          uint denominator = reserveIn.mul(10000).add(amountInWithFee);
          amountOut = numerator / denominator;
      }
```

Due to this commission consumption, the reward in BallsBar will be reduced by 0.25%.

4.1.2. Impact

Total rewards in BallsBar decreased by 0.25%.

4.1.3. Remediation

Implement a commission-free getAmountOut method that is used only for lossless currency conversion within a contract.

5. Acknowledgement

With the cooperation of your company, this security assessment has been successfully completed. Beijing Chaitin Technology Co., Ltd. Security Service Group would like to express deep gratitude to all the departments and individuals from POKESWAP, who have participated in and supported this assessment.

Beijing Chaitin Technology Co., Ltd
CEO Yusen Chen