Smart Contract Security Audit

Audit details:

Audited project:	Polycatfi
Deployer address	0x1cb757f1eB92F25A917CE9a92ED88c1aC0734334
Blockchain:	Matic
Project website:	https://polycat.finance

May, 2021
TechRate

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and TechRate hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

TechRate was commissioned by Polycatfi to perform an audit of smart contracts:

- *https://explorer-mainnet.maticvigil.com/address/0xB67aD6C2Fe7dd6Ba346706b833cCF4234256266D/contracts*
- *https://explorer-mainnet.maticvigil.com/address/0xf5a824B077Cc0aaF50Cf83a9E82714b89B684925/contracts*
- *https://explorer-mainnet.maticvigil.com/address/0x3a3Df212b7AA91Aa0402B9035b098891d276572B/contracts*
- *https://explorer-mainnet.maticvigil.com/address/0x8CFD1B9B7478E7B0422916B72d1DB6A9D513D734/contracts*

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts details

Token contract details for 06.05.2021.

Contract name:	Polycatfi
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0x3a3Df212b7AA91Aa0402B9035b098891d276572B
Total supply:	142_794_890_024_156_075_008_058
Token ticker:	FISH
Decimals:	18
Token holders:	2001
Transactions count:	6266
Contract deployer address:	0x1cb757f1eB92F25A917CE9a92ED88c1aC0734334
Contract’s current owner address:	0x8CFD1B9B7478E7B0422916B72d1DB6A9D513D734

Top 10 token holders

0x289cf2B63c5Edeeeab89663639674d9233E8668E
68,262.464 FISH 47.8151%

0x8CFD1B9B7478E7B0422916B72d1DB6A9D513D734
58,990.958 FISH 41.3208%

0x4879712c5D1A98C0B88Fb700daFF5c65d12Fd729
12,208.548 FISH 8.5516%

0x000000000000000000000000000000000000dEaD
2,167.934 FISH 1.5186%

0xb2197558Da56D35709797C08418D5B238326A29C
218.253112840276256845 FISH 0.1529%

0x7963fBD04523Ed0D995BBbb3132Aed448fC22869
166.251841150303965052 FISH 0.1165%

0x85DE62f3124317fd43643306081C919b5b0Bb15b
164.818260209081665318 FISH 0.1154%

0xf0F7216046A0B477e701764E115FE598b089Ebfb
126.25004632410745442 FISH 0.0884%

0x9BE96A6e861D2e5aFF1Fe0738BeD664b6F0B543e
55 FISH 0.0385%

0x6b9B70021e31532872df4E5C638Da335ec6d3D3F
53.138967514447957832 FISH 0.0372%

Masterchef contract details for 06.05.2021.

Contract name:	MasterChefV2
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0x8CFD1B9B7478E7B0422916B72d1DB6A9D513D734
Dev address:	0x4879712c5D1A98C0B88Fb700daFF5c65d12Fd729
Fee address:	0x47231b2EcB18b7724560A78cd7191b121f53FABc
Fish contract address:	0x3a3Df212b7AA91Aa0402B9035b098891d276572B
Fish per block:	1_000_000_000_000_000_000
Contract owner address:	0xf5a824B077Cc0aaF50Cf83a9E82714b89B684925
Pool length:	12
Start block:	14009000
Total alloc point:	22600
Bonus multiplier:	1

Issues Checking Status

№	Issue description.	Checking status
1	Compiler errors.	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.	Passed
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 of the contract.	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 Open Zeppelin contracts implementation and usage.	Passed
21	Fallback function security.	Passed

MasterChef functions outline

+ Context
  - [Int] _msgSender
  - [Int] _msgData

+ Ownable (Context)
  - [Int] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #

+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ ERC20 (Context, IERC20)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals

  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _approve #
  - [Int] _setupDecimals #
  - [Int] _beforeTokenTransfer #

+ [Lib] SafeERC20
  - [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeApprove #
  - [Int] safeIncreaseAllowance #
  - [Int] safeDecreaseAllowance #
  - [Prv] _callOptionalReturn #

+ ReentrancyGuard
  - [Int] <Constructor> #

+ FishToken (ERC20, Ownable)
  - [Pub] mint #
    - modifiers: onlyOwner
  - [Ext] delegates
  - [Ext] delegate #
  - [Ext] delegateBySig #
  - [Ext] getCurrentVotes
  - [Ext] getPriorVotes
  - [Int] _delegate #
  - [Int] _moveDelegates #
  - [Int] _writeCheckpoint #
  - [Int] safe32
  - [Int] getChainId

+ [Int] IReferral
  - [Ext] recordReferral #
  - [Ext] getReferrer

+ MasterChef (Ownable, ReentrancyGuard)
  - [Pub] <Constructor> #
  - [Ext] poolLength

- [Ext] add #
  - modifiers: onlyOwner,nonDuplicated
- [Ext] set #
  - modifiers: onlyOwner
- [Pub] getMultiplier
- [Ext] pendingFish
- [Pub] massUpdatePools #
- [Pub] updatePool #
- [Pub] deposit #
  - modifiers: nonReentrant
- [Pub] withdraw #
  - modifiers: nonReentrant
- [Pub] emergencyWithdraw #
  - modifiers: nonReentrant
- [Int] safeFishTransfer #
- [Ext] setDevAddress #
  - modifiers: onlyOwner
- [Ext] setFeeAddress #
  - modifiers: onlyOwner
- [Ext] setVaultAddress #
  - modifiers: onlyOwner
- [Ext] updateEmissionRate #
  - modifiers: onlyOwner
- [Ext] setReferralAddress #
  - modifiers: onlyOwner
- [Ext] setReferralCommissionRate #
  - modifiers: onlyOwner
- [Int] payReferralCommission #
- [Pub] updateStartBlock #
  - modifiers: onlyOwner

($) = payable function
= non-constant function

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

1. Block gas limit

Issue:

The updateEmissionRate function can fail due to block gas limit if the pool size is too big.

```
function updateEmissionRate(uint256 _fishPerBlock⬆) external onlyOwner {
    massUpdatePools();
    fishPerBlock = _fishPerBlock⬆;
    emit UpdateEmissionRate(msg.sender, _fishPerBlock⬆);
}
```

Owner privileges

- ❏ Owner can change the dev, fee, vault and referral addresses.
- ❏ Owner can change the referral commission rate.
- ❏ Owner can change the start block.

Conclusion

Smart contracts contain low severity issues!

Techrate note:
Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.