OKCSwap

Contract Audit Report

VER 1.1

11 Apr 2022

No. 2022041121421

Project Summary

1. Project Introduction

The vision of OKC is to "build the digital cornerstone of the meta universe", and in the near future, OKC will mainly focus on Gamefi, Socialfi and other tracks, with potential demand for massive asset swap. In order to make up for the shortcomings of swap on OKC, the official project OKCSwap was launched, and the stable treasury incentive was used to give back to users. The core functions of OKCSwap include asset swap, providing asset liquidity and yield farming. The contract code mainly refers to uniswap V2 and sushiswap. OKCSwap in phase I only supports the staking as pairs with LP (liquidity provider) transaction, and does not support the staking as single currency. All mining pools in phase I only provide OKT rewards and do not support other token rewards.

2. Audit Summary

Project Name	OKCSwap	**Platform**	N/A
Token	N/A	**Token symbol**	N/A
Start date	28 Mar 2022	**Language**	Solidity
End date	11 Apr 2022	**Website**	N/A
Github	https://github.com/okex/OKCSwap/commit/1fdc7353c3d479a80b0e782aadb0446723954ee5	**whitepaper**	N/A

3. Audit Scope

ID	File	SHA-256 checksum
farm	StakingRewards.sol	268685746cd62c5330e5016cf0e60b6c25b5b99145b1a895ffa2b49fb6a71722
farm	StakingRewardsFactory.sol	15554906d609007b1b136f24b74b6ea6e846a218003b4a762cf87279907ebfca
interfaces	IERC20.sol	4c3eb92afca9f12d682595ce5ee7381de2ab6b752e6f880a428795afede52497
interfaces	IOKCSwapCallee.sol	0de42dda65d3199707c12503c74c4cf4a744892a0d68cc94cfd0c599bf55c785

ID	File	SHA-256 checksum
interfaces	IOKCSwapERC20.sol	08a197b39ca55561709b1ae9d55a83193918877fcb8d3fc8d7fc28f6cf35363a
interfaces	IOKCSwapFactory.sol	288c304729b04cba2beab1361334ea72511d06376b0d513a9e96eb27120ec81e
interfaces	IOKCSwapPair.sol	484b37ba6332afca20b065021a37376e41a364082bbde92fbd1c8b2385681e3c
interfaces	IOKCSwapRouter01.sol	2259360819e12e5c767be95f46a76bb94737492751f1d12928d3ef4044ce10a0
interfaces	IOKCSwapRouter02.sol	3173ef5d7253b558defc2498ade7731225a70854e9c0ff89f7b9a8f6f3eb2d6b
interfaces	IStakingRewards.sol	e0724813ceaf4acf4fd196502d70517261857eda7f88d3dbf84614bedb4a239a
interfaces	IWOKT.sol	c3eeda5f5057932ac963cff3635660d777ccc5ff424aac170811f3d4bb2cd748
libraries	Math.sol	e68b7c4743a8b6b14a2e7e42df7b7fdc8364092a97601f1d4452606bf948f4dd
libraries	OKCSwapLibrary.sol	410cfa6eb1dd7fca4f72b66c9f1ef57385e74c344e149cbc8f7b87cac5b5e206
libraries	OKCSwapOracleLibrary.sol	b0f84906fdd4b4e131fc5a1d99ce396b26a87cbc618d0c61521cf07f78efe59e
libraries	RewardsDistributionRecipient.sol	04383c6f197e9b9a380739aa1c233b1007a4d59d0b39e675ed72a36e425f246d
libraries	SafeMath.sol	a1b95b64f8a15b15ecbb725d372985f1499cf86be38557a4cac784d58dfcf5ba
libraries	UQ112x112.sol	5c7f8b7dc61af3440ce5782d25b210dc92b5d898862d2bb5651a25ff34c8df70
mocks	mockERC20.sol	9191e5ce80b3258dc8f621716dc584b23b8a8e2673c06e80baf6e594187e371f
mocks	mockWETH.sol	d013b3e0d26df562b672cd79b03321e4fe0fc63361a05a5d069481854678e495
pair	OKCSwapERC20.sol	f9ee6b6aa000f4caba0d84b6009ea710c8cd3fe535d4ffb78b4610a6cc835ed5
pair	OKCSwapFactory.sol	9c7450c1bf6738a62b7b641bc635aed8e5f0bda256384ae36416446e256c883a
pair	OKCSwapPair.sol	23ce6bb79ce8833ac86e05ba5ff701fbbe64953daa2cfd27ba2d074224ef721a
router	OKCSwapRouter02.sol	9544742257dd23d1ff6404a483912a6d905689111da0b49abc962b78b1807015

11 Apr 2022

4. Code Structure

```
contracts
|   ├── farm
|   |   ├── StakingRewards.sol
|   |   └── StakingRewardsFactory.sol
|   ├── interfaces
|   |   ├── IERC20.sol
|   |   ├── IOKCSwapCallee.sol
|   |   ├── IOKCSwapERC20.sol
|   |   ├── IOKCSwapFactory.sol
|   |   ├── IOKCSwapPair.sol
|   |   ├── IOKCSwapRouter01.sol
|   |   ├── IOKCSwapRouter02.sol
|   |   ├── IStakingRewards.sol
|   |   └── IWOKT.sol
|   ├── libraries
|   |   ├── Math.sol
|   |   ├── OKCSwapLibrary.sol
|   |   ├── OKCSwapOracleLibrary.sol
|   |   ├──
RewardsDistributionRecipient.sol
|   |   ├── SafeMath.sol
|   |   └── UQ112x112.sol
|   ├── mocks
|   |   ├── mockERC20.sol
|   |   └── mockWETH.sol
|   ├── pair
|   |   ├── OKCSwapERC20.sol
|   |   ├── OKCSwapFactory.sol
|   |   └── OKCSwapPair.sol
|   └── router
|       └── OKCSwapRouter02.sol
```

Audit Report Summary

1. Audit Methods

The audit was conducted to gain a clear understanding of how the project was implemented and how it works. The audit team conducted in-depth research, analysis, and testing of the project code and collected detailed data. In this report, the audit team will list in detail each issue identified, where it is located, the root cause of the issue, and a description of the issue, and will recommend changes to the issue accordingly.

Audit methods	Static analysis, Manual Review

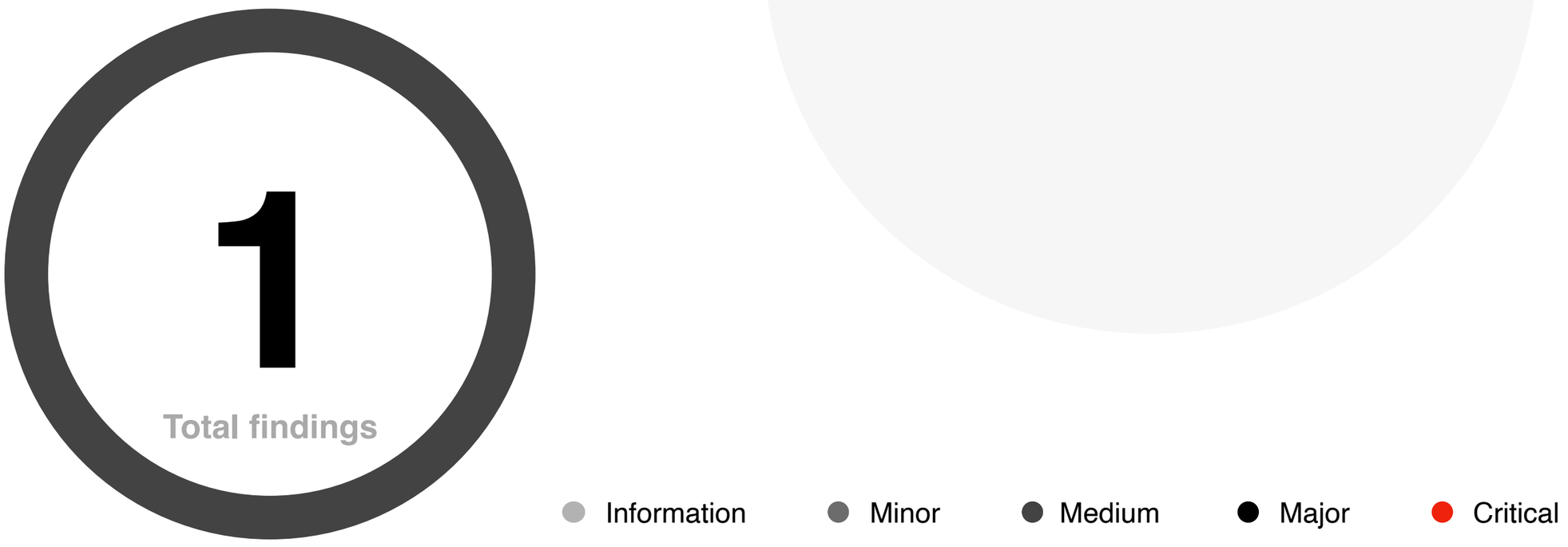
2. Audit Process

Steps	Operation	Description
1	Background	Read project descriptions, white papers, contract source code, and other relevant information the project team provides to ensure a proper understanding of project functions.
2	Automated testing	Scanning source code mainly with automated tools to find common potential vulnerabilities.
3	Manual reveiw	Engineers read the code line by line to find potential vulnerabilities.
4	Logical proofread	The engineer will compare the understanding of the code with the information provided by the project and check whether the code implementation is in line with the project white paper information.
5	Test case	Including test case design, test scope analysis, symbolic execution, etc.
6	Optimization items	Review of projects in terms of maintainability, safety, and operability based on application scenarios, deployment methods, and latest research results.

3. Risk Levels

Risk level	Issue description
Critical	Fatal risks and hazards that need to fixed immediately.
Major	Some high risks and hazards that will lead to related problems that must be solved
Medium	Some moderate risks and pitfalls may lead to potential risks that will eventually need to be addressed
Minor	There are low risks and hazards, mainly details of various types of mishandling or warning messages, which can be set aside for the time being
Information	Some parts can be optimized, such problems can be shelved, but it is recommended that the final solution

4. Audit Results



ID	Audit project	Risk level	Status
1	Reentrancy	None	
2	Injection	None	
3	Authentication bypass	None	
4	MEV Possibility	None	
5	Revert	None	
6	Race condition	None	
7	Insufficient Gas Griefing	None	
8	The major impact of flash loans	None	
9	Unreasonable economic model	None	
10	Predictable random numbers	None	
11	Voting rights management confusion	None	

ID	Audit project	Risk level	Status
12	Privacy leak	None	
13	Improper use of time on chain	None	
14	Improper codes in fallback function	None	
15	Improper identification	None	
16	Inappropriate opcode	None	
17	Inappropriate assembly	None	
18	Constructor irregularities	None	
19	Return value irregularity	None	
20	Event irregularity	None	
21	Keywords irregularity	None	
22	Not following ERC standards	None	
23	Irregularity of condition judgment	None	
24	Risk of liquidity drain	None	
25	Centralization Risk	Medium	Resolved
26	Logic change risk	None	
27	Integer overflow	None	
28	Improper function visiblity	None	
29	Improper initialization of variables	None	
30	Improper contract calls	None	
31	Variable irregularities	None	
32	Replay	None	
33	Write to Arbitrary Storage Location	None	
34	Honeypot logic	None	
35	Hash collision	None	
36	Improper logic in receiving awards	None	
37	Use the not recommended method	None	
38	Basic coding principles were not followed	None	

* In the above table, if the status column is “**Acknowledged**”, the audit team has informed the project owner of the vulnerability. Still, the project owner has not made any changes to the vulnerability or has not announced to the audit team the progress of the changes to the vulnerability. If the status column is “**Resolved**”, the project owner has made changes to the vulnerability, and the audit team has confirmed the changes.

5. Risk and Modification Program

The following section provides detailed information about the risk items learned after the audit, including the type of risk, risk level, location of the issue, description of the problem, recommendations for changes, and feedback from the project owner.

Risk type	Centralization Risk	**Risk level**	**Medium**
Location	All	Contract file	StakingRewardsFactory.sol
Description	Contract functions involving permission control do not have timelock mechanism or multi sign mechanism		
Recommedation	Disperse the permissions of a single private key, and use timelock and multi sign mechanism		
Update	Added timelock contract		

6. Recommandation

N/A

Disclaimer

i. This audit report focuses only on the types of audits identified in the final report issued. Other unknown security vulnerabilities are not part of this audit, and we do not accept responsibility for them.

ii. We shall only issue an audit report based on an attack or vulnerability that existed or occurred before the issuance of the audit report. We cannot determine the likely impact on the security posture of our projects for new attacks or vulnerabilities that may exist or occur in the future, and we are not responsible for them.

iii. The security audit analysis and other elements of our published audit report shall be based solely on documents and materials (including, but not limited to, contract codes) provided to us by the Project Party before the release of the audit report. Such documents and materials shall not be untrue, inaccurate, uninformative, altered, deleted, or concealed, and if the documents and materials provided by the Project Party are false, inaccurate, uninformative, changed, deleted or hidden, or if the documents and materials provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted or concealed, or if the documents and materials provided by the Project Party are uninformative, uninformative, altered, deleted or hidden. If the records and information provided by the Project Party are untrue, inaccurate, uninformative, altered, deleted, or concealed, or if changes to such documents and information are made after the issuance of the audit report, we shall not be liable for any loss or adverse effect arising from any inconsistency between the reflected and actual conditions.

iv. The Project Parties are aware that our audit report is based on documents and information provided by the Project Parties and relies on the technology currently available. However, due to the technical limitations of any organization, there is a possibility that our audit report may not fully detect all risks. Our audit team encourages the project development team and any interested parties to conduct subsequent testing and audits of the project.

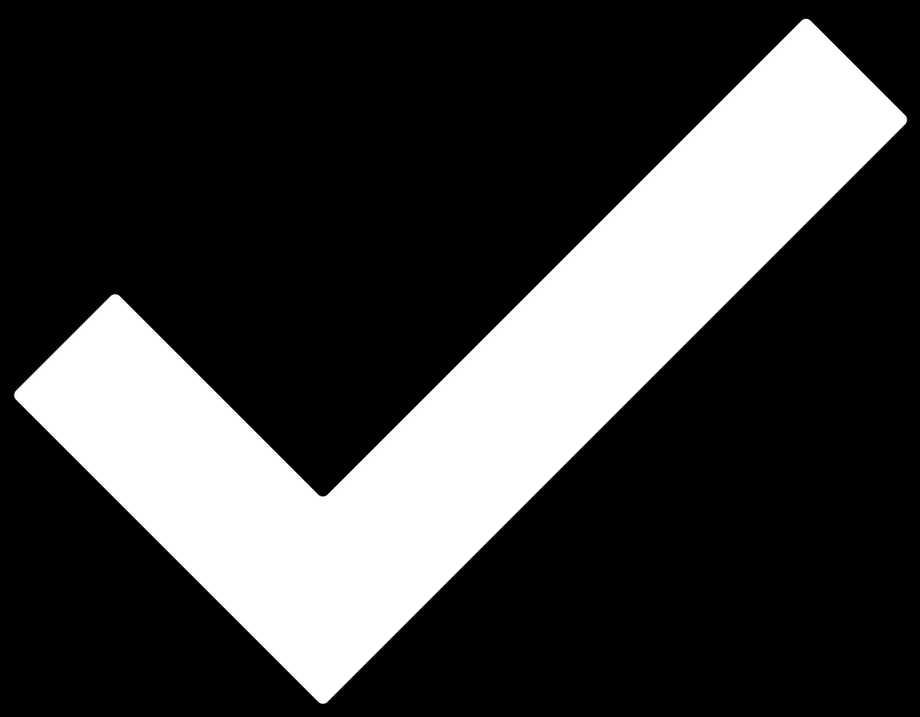
v. The project owner warrants that the project for which we are engaged to provide audit or testing services is legal, compliant, and does not violate applicable laws. The audit report is for the project owner's reference only, and the contents, manner of obtaining, use of, and any services or resources involved in the audit report shall not be relied upon for investment, tax, legal, regulatory, or advisory purposes of any kind, and we shall not be liable therefor. The Project Party shall not refer to, quote, display, or send the Audit Report in whole or in part to any third party without our prior written consent. The Project Party shall bear any loss or liability arising from that place. We assume no responsibility for any reliance on or use of the audit report for any purpose.

vi. This audit report does not cover the compiler of the contract or any areas beyond the programming language of the Smart Contract. The risk and liability of the audited Smart Contract arising from references to off-chain information or resources is the sole responsibility of the project party.

vii. Force Majeure. Force majeure means an unforeseen event whose occurrence and consequences cannot be avoided and cannot be overcome by the parties at the time of entering into the contract, including but not limited to natural disasters such as war, typhoon, flood, fire, earthquake, tidal wave, lightning, natural disaster, strike, nuclear explosion, epidemic and other unforeseen events such as changes in laws, regulations and policies and governmental acts, whose occurrence and consequences cannot be prevented or avoided, and which contains, affects or delays the performance by either party of all or part of its obligations under the contract.

viii. Suppose either party believes that the occurrence of force majeure affects the performance of its obligations under this Agreement. In that case, it shall promptly notify the other party and, depending on the extent of the effect of the event on the performance of the Agreement; the parties shall consult to determine whether to terminate the Agreement or partially relieve itself of its obligations to perform the Agreement, or to extend the performance of the Agreement.

ix. In force majeure, neither party shall be deemed in breach or non-performance of its obligations under this Agreement. Any financial commitments existing before the event shall not be affected, and the project party shall make payment for work performed by us.



Passed.

Date	11 Apr 2022
Audit Team	歐科雲鏈

This audit aimed to review the OKCSwap proposal voting governance and award issuance functionality written in Solidity language for the OKCSwap project, examine its design architecture, identify potential security risks, and attempt to find possible vulnerabilities.