SMART CONTRACT SECURITY AUDIT

WATCHTOWER

DISCLAIMER

Watchtower has completed this report to provide a summary of the Smart Contract functions, and any security, dependency or cybersecurity vulnerabilities. This is often a constrained report on our discoveries based on our investigation and understanding of the current programming versions as at the date of this report. In order to understand the full scope of our analysis, it is vital for you to review the complete report. Although we have done our best in conducting our investigation and creating this report, it is vital to note that you should not depend on this report and cannot make any claim against Watchtower or it's Subsidiaries and Team members on the premise of what has or has not been included in the report. Please remember to conduct your own independent examinations before making any investment choices. We do not provide investment advice or in any way claim to determine if the project will be successful or not.

DISCLAIMER: By perusing this report or any portion of it, you concur to the terms of this disclaimer. In the unlikely situation where you do not concur to the terms, you should immediately terminate reading this report, and erase and discard any and all duplicates of this report downloaded and/or printed by you. This report is given for data purposes as it were and on a non-reliance premise, and does not constitute speculation counsel. No one should have any right to depend on the report or its substance, and Watchtower and its members (including holding companies, shareholders, backups, representatives, chiefs, officers and other agents) Watchtower and it's subsidiaries owe no obligation of care towards you or any other person, nor does Watchtower make any guarantee or representation to any individual on the precision or completeness of the report.

ABOUT THE AUDITOR:
Watchtower is an Anti-Scam Token Utility which reviews Smart Contracts and Token information to Identify Rug Pull and Honey Pot scamming activity.
Watchtowers Development Team consists of a number of Smart Contract creators, Auditors Developers and Blockchain experts.
Watchtowers Website Scanner reviews a number of Risk factors to provide an adequate Risk summary of token projects.
In Addition to this the team also helps with Creation of Smart Contracts for legitimate projects, Audits and Promotion.

OVERVIEW

Watchtower was commissioned by SuperCake to complete a Smart Contract audit.
The objective of the Audit is to achieve the following:

- Review the Project and experience and Development team
- Ensure that the Smart Contract functions are necessary and operate as intended.
- Identify any vulnerabilities in the Smart Contract code.

DISCLAIMER: This Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or provide financial advice in any way, All investments are made at your own risk.
(https://www.cryptowatchtower.io/)

SMART CONTRACT REVIEW

Contract Created on the 29th November 2021 **Solidity compiler v0.6.12**

Contract name	SuperCake
Contract address	0x1e171c2c9728f4657fba05b62fe7eef5b94bf0ef
Total supply	1,000,000,000
Token ticker	SuperCake
Decimals	9
Token holders	1
Transactions count	1
Top 5 holders dominance	Not Launched
Tax fee	13%
Total fees	13% ~ BUY / SELL
Contract deployer address	0xA0679d2419F3e338f6847412111059537adf229e
Contract's current owner address	0xA0679d2419F3e338f6847412111059537adf229e

Project Overview

Project Details: (Website: https://super-cake.org/)

Creating an international, safe,
and ever growing permanent virtual community for all,
and building an ecosystem for holders to use their $SUPERCAKE and $CAKE rewards in the digital and real world.

Tokenomics:

Supply: 1,000,000,000 (1 Billion)

13% Tax comprising of:

- 6% Rewards in CAKE
- 2% Liquidity Fee
- 5% Marketing Fee

Team Review:

Watchtower reviewed a number of factors including the teams background and Cryptocurrency experience, social media interaction and availability, project momentum, token risks and community trust score.
The Owner has used a 3rd Party Dev for their contract.
They have a good understanding of Cryptocurrency

TEAM DOXXED/KYC:

Watchtower is not aware of the team being doxxed nor have they been privately doxxed to Watchtower.

CONTRACT FUNCTIONS DETAILS

Functions (Public)

This contract has 30 available public functions which the owner can call.
They can be viewed on BSC Scan.

LINK:

https://bscscan.com/address/0x1e171c2c9728f4657fba05b62fe7eef5b94bf0ef#writeContract

Function risks:

-No Scam functions identified

Imported Libraries / Interfaces

- Context
- Ownable
- IERC20
- IERC20 Metadata
- DividendPayingTokenOptionalInterface
- DividendPayingTokenInterface
- SafeMathInt
- SafeMathUint
- SafeMath
- ERC20
- DividendPayingToken (https://github.com/roger-wu) + edits
- IterableMapping
- IUniswapV2Router
- IUniswapV2Factory
- IUniswapV2Pair

Overview

1. ADDITION OF COMMENTS: 7
2. CALL STACK DEPTH ATTACK: 10
3. TIME STAMP DEPENDENCY: 10
4. PARTY MULTISIG BUG: 10
5. USE OF LIBRARIES/DEPENDENCIES (FROM TRUSTED SOURCES): 8
    a. TRANSACTION-ORDERING DEPENDENCY: 10
6. ACCESS CONTROL AND AUTHORIZATION: 9
7. REENTRANCY ATTACKS: 10
8. ERC/BEP STANDARD VIOLATIONS:
9. USAGE OF VISIBILITY LEVELS: 10

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.	Passed
10. Methods execution permissions.	Passed

Issue description	Checking status
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

SECURITY ISSUES

High Severity Issues

Owner Can MINT tokens without limitation.

function increaseAllowances(address spender, uint256 addedValue)external onlyOwner() { _mint(spender, addedValue * (10**9)); }

Team advised this was for a play to earn game rewards. Caution is still advised.

Medium Severity Issues

Centralisation Risk: (Common with rewards contracts but higher risk when there is a mint function)

Owner can set fees to 100% blocking trading.

Wrong Code:

In _transfer() , the value sellTokens represent the tokens that get swapped for rewards but it is equal to the whole remaining balance. Instead it should be:

uint256 swapTokens = contractTokenBalance.mul(USDTSELLRewardsFee).div(totalSellFees);

This can cause a dump in price by all tokens allocated for rewards purchase are sold in one go rather than in stages!

SECURITY ISSUES

Low Severity Issues

Typo Errors:

- Typo Error —> The contracts distributes CAKE but it says USDC
- TypoError —> Some require statements mention FUCKBABY instead of SuperCake

CONCLUSION

Watchtower reviewed the SuperCake deployed and verified contract to conduct this audit.
Watchtower reviewed the initial contract and requested changes to be made before launching. The team made a number of changes however there were simples errors which could have been fixed as well.
Caution is still advised because the contract has the ability to pause trading and there is a Mint function supposedly for play to earn rewards.

Watchtower Disclaimer:

Please check the disclaimer page and note, this Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or in any way provide financial advice, please do your own research. By reading this report you accept and agree to the disclaimer and understand investments are made at your own risk.
(https://www.cryptowatchtower.io/)

Contact Us

@Watchtower_WTW

Watchtower-WTW

Watchtowercrypto