



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 its 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 its 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 Projeto Optimus 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 11th November 2021

Solidity compiler v0.7.6

Contract name	Projeto Optimus
Contract address	0xC718755C2838F819e20139138AD8bADD8050fc83
Total supply	200,000
Token ticker	OPTIMUS
Decimals	18
Token holders	92
Transactions count	96
Top 5 holders dominance	Not Launched
Tax fee	6%
Total fees	6% ~ BUY / SELL
Contract deployer address	0x5fb71Dbf7248a01bf96cE2AB2DA34EEAbE58c261
Contract's current owner address	0x4070d652dab3ff9f99521640b5ee15b053a6d48f



Project Overview



Project Details: (Website: <https://projetooptimus.com.br/>)

OPTIMUS is a protocol with the objective of providing users with security through our launchpad, allowing investors the opportunity to invest in advance in the most promising projects on the market.

Tokenomics:

Supply: 200,000 (200 Thousand)

6% Tax for Buys and 6% for Sells comprising of:

- 1% Development
- 1% Liquidity Fee
- 1% Marketing Fee
- 3% BUSD Rewards

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 Projeto Optimus team and community following is currently small but they have shown a good understanding of Cryptocurrency with genuine intentions.

TEAM DOXXED/KYC:

The Projeto Optimus Dev has been doxxed and is noted on their website as the CEO.



CONTRACT FUNCTIONS DETAILS

Functions (Public)

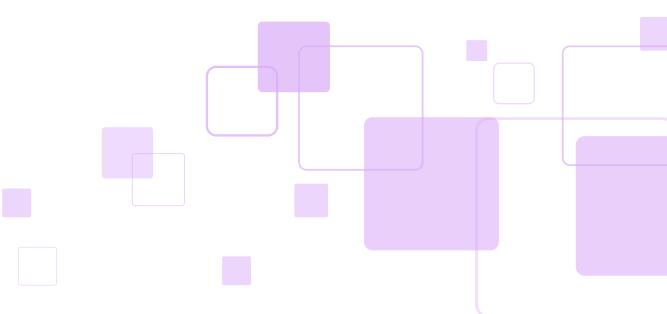
This contract has 24 available public functions which the owner can call.
They can be viewed on BSC Scan.

LINK:

<https://bscscan.com/token/0xc718755c2838f819e20139138ad8badd8050fc83#writeContract>

Function risks:

-No scam functions identified.



Contract Stress Test

Imported Libraries / Interfaces

- ERC20Upgradeable
- IERC20
- OwnableUpgradeable
- SafeMath
- Clones
- IUniswapV2Factory
- IUniswapV2Router02
- IBabyToken
- BabyTokenDividendTracker
- ContextUpgradeable
- IERC20Upgradeable
- SafeMathUpgradeable
- Initializable
- AddressUpgradeable
- ERC20
- Ownable
- IUniswapV2Pair
- SafeMathInt
- SafeMathUint
- IterableMapping
- IPinkAntiBot
- IAntiBotBabyToken
- Context



Overview

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

Nil



Medium Severity Issues

Centralization Risk:

- The Owner can set fees to 100% blocking all transfers. (Common with rewards contracts)
- **Fees can't be set to 0:** If fees are set to 0 the transaction will fail because the contract will try to swap 0 tokens.
- **There is no way to pause internal swaps.** This can be a problem if a migration is needed (eg. Pancakeswap V3)



SECURITY ISSUES



Low Severity Issues

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 sellTokens = contractTokenBalance.mul(tokenRewardsFee).div(totalFees);
```

- Typo Error —> The contracts distributes BUSD but it mentions CAKE



CONCLUSION



Watchtower reviewed the Projeto Optimus deployed and verified contract to conduct this audit.

Watchtower is satisfied that the contract is void of any malicious coding and that the team are operating with integrity.

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

