SMART CONTRACT SECURITY AUDIT

WATCHTOWER

AUDIT DETAILS

Project Name

BabyKrypto

Contract address

0x60Bbc91be24850636eE3028dfC309e755A4e3411

Deployer Address:

0xfb1A25688660CCABE04B5b92d7F058e01629daDb

Blockchain

Binance Smart Chain

Project website:

https://babykrypto.com/

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 BabyKrypto to complete a Smart Contract audit. The objective of the Audit is to achieve the following:

- 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 09.19.2021

Contract name	BabyKrypto
Contract address	0x60Bbc91be24850636eE3028dfC309e755A4e3411
Total supply	100,000,000,000
Token ticker	$BabyK
Decimals	4
Token holders	1726
Transactions count	13368
Top 5 holders dominance	43.8% (High Price Impact Risk)
Tax fee /Slippage required	16%-18%
Total fees	16/17% ~ BUY / SELL
Contract deployer address	0xfb1A25688660CCABE04B5b92d7F058e01629daDb
Contract's current owner address	0xE7F171D1196FE432aFAC8dD21C831A6a644a83DC

Baby Krypto Overview

Project Details:

BabyKrypto is a rewards Token that offers Holders 8% in BNB Rewards from every transaction. It is also looking to implement a Dynamic rewards system linked to NFT's that will be minted and offer owners of particular NFT's higher percentage of rewards in different tokens.

Tokenomics:

Starting Supply: 100,000,000,000 (100 Billion)
8% BNB or Alternative Rewards to Holders
4% Auto Liquidity
4% Marketing
1% Extra Sell fee

Team Review:

Watchtower did not conduct a team review for this project!

CONTRACT FUNCTIONS DETAILS

Functions (Public)

1. Claim Tokens
2. Airdrop **
3. Airdrop Fixed **
4. Approve
5. Approve Max
6. Authorise
7. Claim Process
8. Clear Stuck Balance
9. Cooldown Enabled
10. Purge before Switch
11. Set Ban Fees
12. Set Ban Block
13. Set Buy Fees
14. Set Distribution Criteria
15. Set Distributor settings
16. Set Fee receivers
17. Set is Dividend Exempt
18. Set is Fee Exempt
19. Set is Time Lock Exempt
20. Set is Transaction Limit Exempt
21. Set Max Wallet Percent
22. Set Sell Fees
23. Set Swap Back settings

Functions Continued

24. Set Target Liquidity
25. Set Transaction Limit
26. Switch Token
27. Trading Status
28. Transfer To
29. Transfer From
30. Transfer Ownership
31. Unauthorise

Functions Risk

Upon review of Smart Contract Coding and Functions, Watchtower found a number of issues which can be identified as malicious. Watchtower raised this with the Baby Krypto team who seemingly did not realise there was Functions Risks in the contract.
Most notably the Airdrop functions starred above allow the Contract owner to withdraw holders tokens from their wallets and transfer them to another wallet address.
This can be remediated if the Owners renounce the contract!

Note:
Most Rewards Contracts include Functions which allow the contract owner to increase fees to levels which make it impossible to sell.
The team has provided transparency by allowing the set fees to be viewed on BSC Scan however due to the Airdrop function error it is noted as High Risk, since the owner can pause trading, withdraw tokens and essential Rug Pull the project.
In addition to this the Top Holders wallets which portray Dev wallets hold over 40$ of token supply in an unlocked state which can be classified as a High Price Impact risk or Rug Pull Risk.

Imported Libraries / Interfaces

- SafeMath
- IBEP20
- Auth
- IDEXFactory
- IDEXRouter
- IDividendDistributor

Overview

ISSUES CHECKING STATUS

Issue description	Checking status
1. Compiler errors.	Caution
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.	Caution
21. Fallback function security.	Passed

SECURITY ISSUES

High Severity Issues

Owner can transfer tokens from any address:
airdrop() and airdropFixed() allow the Owner to transfer tokens from any address. Allowance is not checked in _basicTransfer()
CONTRACT RENOUNCED- FUNCTION CANNOT BE CALLED.

Medium Severity Issues

Centralisation Risk:
The owner has the privilege to:

1. **withdraw all BNB in contract balance**
2. **start/stop trading**
3. **start/stop cooldown**
4. **withdraw all the rewards not distributed yet**
5. **change reward token**

CONTRACT RENOUNCED - FUNCTION CANNOT BE CALLED

Low Severity Issues

- **Fees declared as private: Private variables can't be viewed so users can't know the current fees values**
- **High Gas Limit: distributorGas = 500000. If the price of BNB increases then gas fees can be higher than rewards. It can be adjusted by authorized users.**

CONCLUSION

Watchtower reviewed BabyKryptos' deployed and verified contract to conduct this audit.
Watchtower identified Smart Contract coding that can be used in a Malicious manner. Watchtower believes the team may have accidentally included these functions and requested the team to renounce the contract.
The team agreed and on upon updated audit on 26/09/2021 we can confirm that the CONTRACT HAS NOW BEEN RENOUNCED

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