TRYNOS AUDITS

Binance Smart Chain:
Baby Santa Token

0xfccF3229063b1aa16af6b9b5DE1B7E0c1bfE4046

CONTACT ME ON TELEGRAM

Trynos

TrynosTokenTerminal

DISCLAIMER

Project Description

A rewards token with buyback functionality in place. Nothing special or otherwise too custom, just the usual code in place. Limits are in place but there are some exceptions, and some functions are missing them altogether.

Developer's Submitted Description

Baby Santa is working over time on the BSC. Delivering diamond hands to all the good little boys and girls. Pack your bags, hop on and hold tight. The sleigh has been upgraded with rocket power fueled by good times and reindeer farts. 💨 Join the Santa revolution, earn Santa coin rewards, compound reward earnings in BUSD, and give back this holiday season and beyond. Happy holidays, and LFG. Whitelisted addresses will have 60 minutes to buy then will be opened to the public!

Project Information

Name
Baby Santa Token

Launch Type
Presale,
Pinksale Launchpad

Telegram
http://t.me/babysantatoken

Website
www.babysantatoken.com

Taxes
2% Auto-Liquidity
3% Buyback
3% Marketing (External Wallet)
6% Rewards

Token Distribution
4% Team (Vested) **
1.64% Venture Capital
50% Burn
44.36% Liquidity + Presale

** Please inspect all vestings and timelocks, as they are not covered by this audit.

Launch Date

Pinksale:
November 7th, 2021 17:00 UTC
PancakeSwap:
24Hrs After HC Fill of Pinksale

Security Quick Report

Contract Analyzed [Solidity v. 0.8.7]

https://bscscan.com/address/0xfccF3229063b1aa16af6b9b5DE1B7E0c1bfE4046#code

HIGH – **No Risks**

Medium – 4 Risks

Low – 4 Risks

Minimal – 1 Risks

**Risk assessment is color-coded for convenience.
The risks are as follows, and their respective colors:**

HIGH – SEVERE risk. Could either honeypot, rug, somehow scam the user, or prevent the contract from functioning as intended.
Medium – Could allow the owner to stop trading while being able to trade himself, make the user lose money, or something similar.
Low – Risks that could allow the owner to somehow have an edge, allow users he choose to have an edge, or the ability to manipulate the contract, prices, or something similar.
Minimal - Risks that are not potentially investment-threatening, but needs be mentioned anyway. This could include poor code or poor optimization, etc.

Security and Code

Mutable Taxes [Medium Risk]

The owner can set taxes as high as 25%. With the buyback multiplier starting at x2, this could go further as high as 50% when selling, which would disable sells on sites such as Pancakeswap where slippage caps out at 49.9%.

Owner Receives Auto-Liquidity [Medium Risk]

The owner receives all new liquidity from the auto-liquidity tax. He can then do anything with this liquidity, including unpairing it. There is a function in place to change this as well which also has no limits.

No True Ownership Renounce [Medium Risk]

The contract uses authorizations, which can be granted to any address. Because of this, if the owner were to transfer ownership to a dead address, it would not be a true renouncement, as those previous addresses would still have authorization and control over functions.

Re-Entrancy Potential [Medium Risk]

There is a potential for a re-entrancy attack. The tokens for rewards are transferred prior to the amount being excluded from future rewards, and if this transfer occurs and a new transaction is sent by a malicious contract before the amount is excluded, the rewards could be claimed multiple times.

Security and Code

Hidden Taxes [Low Risk]

The individual tax values are not public, nor are there any getters to view them. totalFees is visible, but the destination of where the taxes goes ends up being obfuscated. They can still be found by tracking the owner's transactions and locating those that set the fees.

Mutable Maximum Transaction [Low Risk]

The owner is able to set the maximum transaction amount as low as 0.1%.

Limitless Exclusions [Low Risk]

The owner is able to set any address to be excluded from fees, rewards, or limits at any time.

Currency Sweep [Low Risk]

There is a sweep function that can be called to withdraw the contract's full BNB amount. In this specific contract's case, even if ownership is renounced this can be called by the marketing wallet.

Rewards Token Choice [Minimal Risk]

The token that is being rewarded is another rewards token. As the gas is set to 500,000 units and rewards tokens typically cost a large amount of gas to transfer, the result is that the automatic distribution for this token would be slow. Because of this, more transactions or manual claiming would be required.

Closing Notes

Most of the high-risk issues in this contract are limitless settable functions that the owner can act on, as well as poor contract optimization. These are not by themselves malicious but can be abused easily with poor ownership or malicious developers. Please do your own research and ensure you have trust in the project and its team before investing.

Always make sure to always inspect all values and variables.

This includes, but is not limited to:

- Ownership

- Proper Ownership Renouncement (if any)

- Taxes

- Transaction/Wallet Limits

- Token Distributions

- Timelocks

- Liqudity Locks

- Any other owner-adjustable settings or variables.

Final Disclaimer

I am solely a smart contract writer/auditor. I do not promote, own, or lead projects unless specifically and explicitly stated. I am not a good trader, I know nothing of Technical Analysis, and for the most part I do not trade. Despite my best efforts, I can never guarantee full safety, though I do my best to check for and announce all risks. There are many tricks and variations that unscrupulous people can enact even with safe contracts. Please always do your research.

I am only human, and I make mistakes as well.

Nothing written in this report is financial advice. Please make sure you are interacting with the correct socials below when contacting me, to avoid scamming impersonators.

CONTACT ME ON TELEGRAM

@Trynos

TrynosTokenTerminal