TRYNOS AUDITS

Binance Smart Chain:
Cumflix

0xb379431dcd6945b9c1a64cd337320f1b6c077dca

CONTACT ME ON TELEGRAM

👤 Trynos

📢 TrynosTokenTerminal

DISCLAIMER

Project Description

A rewards token the likes of which we have seen many in past days. Nothing seems special about this one, the standard ways of claiming your rewards: Either by trading any amount of tokens, or by running the Claim() command on the contract. This one in specific is seemingly a fork of older ones, however, and is quite unoptimized.

Developer Description

Meet Cumflix, the paradigm shifting adult streaming platform which self-funds content perpetually. Watch, yield and cum — all in one web app. Enjoy the naughtiest content from your favourite performers under one adult platform powered by DeFi.

Project Information

Name
Cumflix

Launch Type
Presale,
Pinksale Launchpad

Telegram
https://t.me/CumflixOfficial

Website
https://cumflix.app

Taxes
5% Marketing
5% Rewards in BNB
2% Auto-Liquidity

NOTE: All Fees are set to 0% at time of audit.

Token Distribution
10% NFT Staking

5% Development

5% Marketing

80% PinkSale + PCS Liquidity

Launch Date

Presale:
10/01/2021, 14 UTC (ETA)
PancakeSwap:
10/02/2021, 14 UTC (ETA)

Security Quick Report

Contract Analyzed [Solidity v. 0.6.12]

https://bscscan.com/address/0xb379431dcd6945b9c1a64cd337320f1b6c077dca#code

HIGH – 2 Risks

Medium – 4 Risks

Low – 4 Risks

Minimal – 1 Risk

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.

Security and Code

No Maximums on Taxes [HIGH Risk]

The owner can set taxes to any number. There are no limits, and even taxes of 100% is possible. These numbers can be manipulated freely, such as setting all taxes to 0 with marketing at any value, thus routing all sold tokens during contract token swaps to the marketing wallet. The owner (and anyone else set to be excluded) is exempt from taxes, and even if set to 100% would be able to sell without fees.

No Minimums on Maximum Tx [HIGH Risk]

The owner is able to set the maximum transaction amount to any value, including 0. This would entirely pause trading for anyone not excluded from these limits. As the owner can also change these limits freely, this could potentially allow him to turn off trading for everyone save for a select few, including himself.

Changeable Dividend Tracker [Medium Risk]

The dividend tracker can be changed and updated to a new contract, without limits. This could theoretically be done to change to a new contract that diverts all funds meant for distributed rewards to wherever the owner wishes.

Owner Receives New 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.

Security and Code (cont.)

Withdraw Function [Medium Risk]

There is a withdraw function in place, allowing the owner to withdraw any BNB inside the contract. Should the Dividend distributor be changed to one that does not accept BNB, the BNB could potentially remain inside the contract, allowing the owner to withdraw it to his wallet at any time.

Controllable Swap Amount [Medium Risk]

There are no limits on the function that sets the amount of tokens to check for before the contract swaps those tokens for BNB to distribute to the tax destinations. In theory, this could be set to a very high amount and force the contract to sell a large quantity of tokens all at once.

Limitless Exclusions [Low Risk]

The owner is able to set any address to be excluded from fees, transaction limits, or dividends at any time without limits.
Once excluded from dividends, an address can never be included again.

Limitless New LP Pair Setting [Low Risk]

The owner is able to set any address as a "automated market pair" at any time without limit. This would then exclude the address from dividends, and additionally

Security and Code (cont.)

Poor Optimization [Low Risk]

The contract is poorly optimized. Aside from being a severely outdated Solidity version, the swapping from token to BNB alone is done three times. Each swap takes at minimum 121,000 gas units, and the two extra swaps are needless when calculating the distribution would suffice instead. This gas fee is then hoisted on the users. There are many other instances of poor optimization as well.

Presale Rewards [Low Risk]

Rewards function off how many tokens a user holds. Since this is a presale and it is required to claim the tokens, it is only when claimed that the tokens allow for rewards to begin accumulating. In this way, the first one to claim will be privy to most of the rewards, until others also claim their tokens. As such, it is a gas war to see who will claim first.

Changeable Router [Minimal Risk]

The router used to swap tokens for BNB can be changed at any time by the owner. This is not necessarily considered a risk, as while changing this to a bad router could stop all token to BNB swaps and thus distribution, this would stop ALL distribution of BNB of any kind, and would most likely prevent sell transactions for anyone, including the owner.

Closing Notes

Most of the high-risk issues in this contract are limitless settable functions that the owner can act on. These are not by themselves malicious but can be abused with poor ownership. 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

- 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