AUDIT

GUARDIANSALE AUDIT

"WWW.GUARDIANSALE.COM"



Guardiansale token is forked token of safemoon so it has the same infrastructure.

quardiansale.com

SUMMARY



01 Summary

02 Understanding



03 Function Map



04 Safemoon Contract Fix



05 Resources & Social media



Renounce ownership and time lock



SUMMARY



PROJECT NAME: GUARDIANSALE TOKEN

DESCRIPTION: THE GUARDIANSALE TOKEN

IS A MIXTURE OF RFI TOKEN

AND ADDED FUNCTION OF A

GENERATED PROTOCOL

PLATFORM: BSC

LANGUAGE: SOLIDITY

CODEBASE: CODEBASE:

AUDIT METHODOLOGY: STATIC ANALYSIS,

MANUAL REVIEW,

TESTNET

UNDERSTANDING

OVERVIEW

The guardiansale protocol is decentralized "DeF|" token deployed on the Binance smart chain "BSC". Guardiansale has 4 features in tax:

- Rewards for holders
- Liquidity
- Marketing
- LP buyback & Burn



UNDERSTANDING

OVERVIEW

As guardiansale we have created the most detailed explanation of smart contracts. Our goal is making our contracts understandable and transparent as well as supporting developers community. In all DeFi market this is a first. Take this chance and look it up in our github and bscscan.

Each guardiansale transaction is taxed 4%.

- * %1 of this tax goes to all holders.
- * %1 of this tax goes for liquidity.
- * %1 of this tax goes for buyback & burn.
- * %1 of this tax goes for marketing.

LP ACQUISITION

The LP acquisition mechanism can be indirectly triggered by any normal transaction of the token as all transfers evaluate the set of conditions that triggers the mechanism. The main conditions of the mechanism are whether the sender is different than the LP pair and whether the accumulation threshold has been breached. Should these conditions be satisfied, the swapAndLiquify function is invoked with the current contract's Guardiansale token balance.

The swapAndLiquify function splits the contract's balance in two halves properly accounting for any truncation that may occur. The first half is swapped to BNB via the PancakeSwap Router using the Guardiansale-BNB pair and thus temporarily driving the price of the Guardiansale token down. Afterwards, the resulting BNB balance along with the remaining Guardiansale balance are supplied to the Guardiansale-BNB liquidity pool as liquidity via the Router.

STATIC REWARD (REFLECTION)

Balances in the Guardiansale token system are calculated in one of two ways. The first method, which most users should be familiar with, is a traditional fixed number of units being associated with a user's address. The second method, which is of interest to static rewards, represents a user's balance as a proportion of the total supply of the token. This method works similarly to how dynamic rebasing mechanisms work such as that of Ampleforth.



UNDERSTANDING



Whenever a taxed transaction occurs, the 1% meant to be re-distributed to token holders is deducted from the total "proportion" supply resulting in a user's percentage of total supply being increased. Within the system, not all users are integrated in this system and as such the 1% fee is rewarded to a subset of the total users of the Guardiansale token. The owner of the contract is able to introduce and exclude users from the dynamic balance system at will.

STATIC REWARD (REFLECTION)

The contract contains the following privileged functions that are restricted by the onlyOwner modifier. They are used to modify the contract configurations and address attributes. We grouped these functions below: Account management functions for inclusion and exclusion in the fee and reward system:

Account management functions for inclusion and exclusion in the fee and reward system:

- excludeFromReward(address account)
- includeInReward(address account)
- excludeFromFee(address account)
- includeInFee(address account)

Modification of liquidation, tax and max transaction percents of the system:

- function setTaxFeePercent(uint256 taxFee)
- function setLiquidityFeePercent(uint256 liquidityFee)
- function setMaxTxPercent(uint256 maxTxPercent)

Toggle feature of the LP acquisition mechanism:

- function setSwapAndLiquifyEnabled(bool _enabled)



FUNCTION MAP



ALL PROCESS WILL BE AUTOMATIC WITHOUT HUMAN INTERVENTION

TOKEN CONTRACT

- 6% token is transferred to presale
- 94 % of token is transferred to timelock contract.
- Exclude presale contract from tax fees
- Exclude timelock contract from rewards

PRESALE CONTRACT

- 6% TOKEN RECEIVE FROM TOKEN CONTRACT
- Each transaction will send BNB'S TO timelock directly

TIME LOCK CONTRACT

- 94 % of token is received from token contract.
- Pair 4 % of token with presale received BNB to open liquidity pool and receive cake LP without human intervention or leaving the lock contract.
- After 3 months 15 % of the tokens will be out for listing purposes.
- Rest of the token and cake LP token will be locked for a year.

PANCAKESWAP POOL











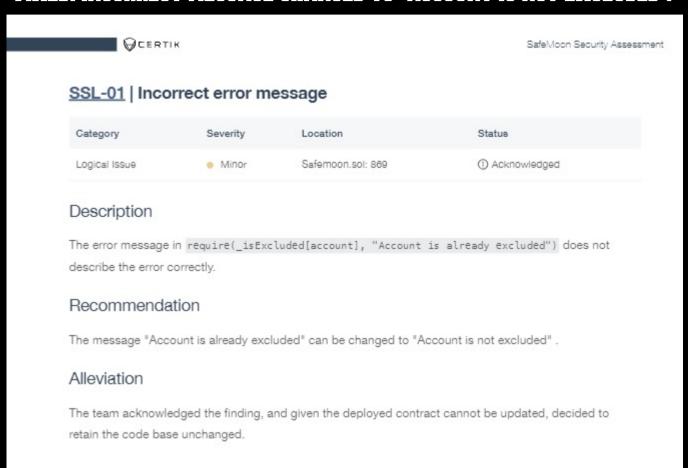


SAFEMOON CONTRACT FIX

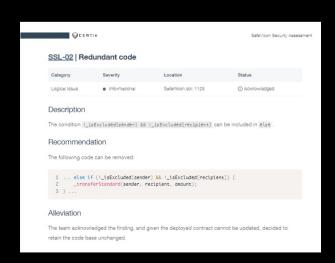


Guardian presale token contract is a forked contract of safemoon and we fixed the errors that spotted by certik. You can check the rest of the explanations on guardiansale bscscan, github, ethscan.

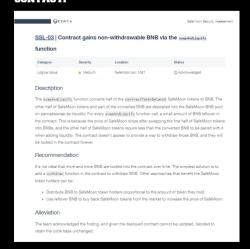
FIXED: INCORRECT MESSAGE CHANGED TO "ACCOUNT IS NOT EXCLUDED".



FIXED: ELSE IF CHANGED TO "ELSE".



WE HAVE CREATED A FUNCTION THAT SENDS LEFTOVER BNB FROM SWAPANDLIQUIFY TO TIMELOCK CONTACT.













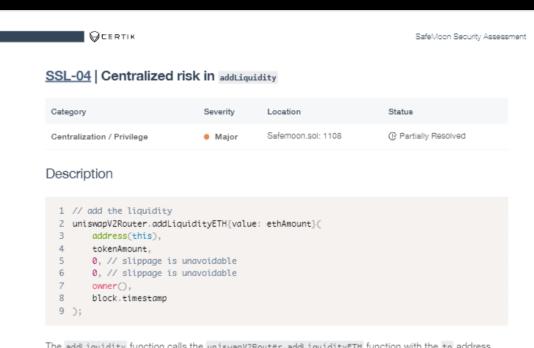




SAFEMOON CONTRACT FIX



IN SAFEMOON CONTACT GENERATED LP TOKEN GOES TO OWNER. WE HAVE CHANGED IT FROM OWNER TO TIMELOCK CONTRACT.



The addLiquidity function calls the uniswapV2Router.addLiquidityETH function with the to address specified as owner() for acquiring the generated LP tokens from the SafeMoon-BNB pool. As a result, over time the _owner address will accumulate a significant portion of LP tokens.If the _owner is an EOA (Externally Owned Account), mishandling of its private key can have devastating consequences to the project as a whole.

Recommendation

We advise the to address of the uniswapV2Router.addLiquidityETH function call to be replaced by the contract itself, i.e. address (this), and to restrict the management of the LP tokens within the scope of the contract's business logic. This will also protect the LP tokens from being stolen if the _owner account is compromised. In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or via smart-contract based accounts with enhanced security practices, f.e. Multisignature wallets.

Indicatively, here are some feasible solutions that would also mitigate the potential risk:

- . Time-lock with reasonable latency, i.e. 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent single point of failure due to the
 private key;
- · Introduction of a DAO / governance / voting module to increase transparency and user involvement.











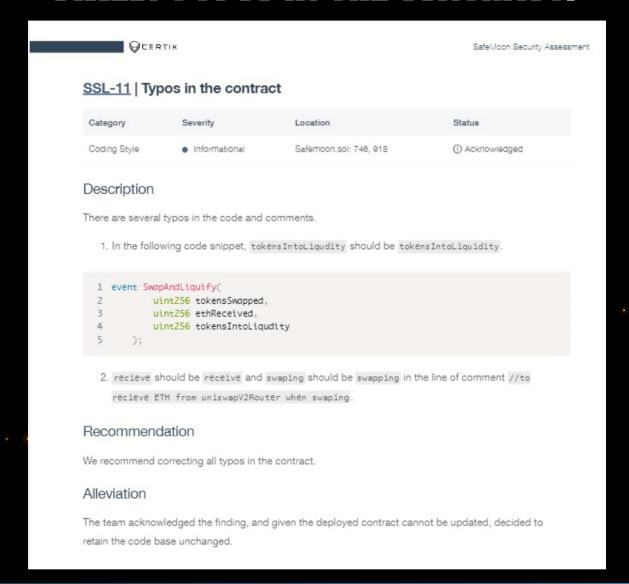




SAFEMOON CONTRACT FIX



FIXED: TYPOS IN THE CONTRACT.



RENOUNCE OWNERSHIP AND LOCK TOKEN

All tokens are locked before the presale.

We have renounced ownership before the presale.





RESOURCES & SOCIAL MEDIA



GUARDIANSALE OFFICAL SOCIAL ACCOUNTS RESOURCES:



WWW.GUARDIANSALE.COM



GITHUB.COM/GUARDIANSALE

SOCIALS:



TWITTER.COM/GUARDIANSALE



FACEBOOK.COM/GUARDIANSALELAUNCHPAD



INSTAGRAM.COM/GUARDIANSALE



YOUTUBE.COM/GUARDIANSALE



TIKTOK.COM/@GUARDIANSALE



T.ME/GUARDIANSALEEN