TERRA CASH
SMART CONTRACT
SECURITY AUDIT

SNIPEFINANCE.COM
October 20th 2022

AUDIT STRUCTURE

Audit Process

Step 1
Review Source Code

Step 2
Send Custom Quote

Step 3
Manual line-by-line code reviews by multiple auditors to ensure the logic behind each function

Step 4
Automated smart contract tests + Manual smart contract tests on testnet

Step 5
Suggest remediations

Step 6
Complete audit & provide certificate

Audit Package Selected

Type of Analysis
Manual Review: Yes
Dynamic Analysis: Yes
Static Analysis: Yes
Tests On Testnet: Yes

Type of Publication
Website Audit Publication: Yes
Twitter Audit Publication: Yes

SUMMARY

Project Details

Project Name: Terra Cash

Platform: BSC

Language: Solidity

Source Code: Click here

Deployed: Yes

Liquidity Locked: Not Provided

Team Tokens Locked: Not Provided

Anon Team: Yes

Lines of Code: 2149 With Comments

Website: terracash.io

Project's Social Media: 

Vulnerability Check

Total Issues: 0

Critical: 0

Medium: 0

Low: 0

Discussion: 0

ISSUES CHECKER TABLE

Issue Description	Passed
1. Compiler Errors	✓
2. Race Conditions and Reentrancy. Cross-function race Conditions	✓
3. Possible delays in data delivery	✓
4. Burn LUNC	✓
5. Dividends in LUNC	✓
6. Timestamp dependence	✓
7. Integer Overflow and Underflow	✓
8. DoS with Revert	✓
9. DoS with block gas limit	✓
10. Methods execution permissions	✓
11. Economy model of the contract	✓
12. The impact of the exchange rate on the logic	✓
13. Private user data leaks	✓
14. Malicious Event log	✓
15. Scoping and Declarations	✓
16. Uninitialized storage pointers	✓
17. Arithmetic accurancy	✓
18. Design Logic	✓

FINDINGS

High severity issues

No high severity issues

Medium severity issues

No Medium severity issues

Low severity issues

No Low severity issues

Tests were performed with automated private scripts, manual tests were also performed on Binance testnet to ensure easy understanding for all

TESTS

Smart-Contract link and source code

https://bscscan.com/address/0xe377e527dda3fb703216d3f92af65a333de7d12b#code

What we have changed: As there isnt't LUNC in the testnet network we changed it to BUSD (the logic remains the same so we can test if LUNC would be burned (BUSD in this case).

Token Smart Contract(testnet) link and source code

https://testnet.bscscan.com/address/0xb9ac46b80a7d524f92b57c9b951810c2a310a944#code

Action: Setup Buyback address (0xdead):

https://testnet.bscscan.com/tx/0xd049b29639cdb223ad03e4989d39db70f0850763a70e3edc907a4126a5698038

Action: Burn BUSD (Terra Cash will burn LUNA)

https://testnet.bscscan.com/tx/0xf068cf38229c3fca465dbdadecb6993be83951123d99b9747b917c0f4a3d769c

Action: Set minimum balance for token dividends to 1 (for testing)

https://testnet.bscscan.com/tx/0xb41678b0b96b96b7e32873bddbb2b8bedf2b183f6a9033191b9b2e9fe4ff0900

Action: Swapatamount edit to 100 TLC

https://testnet.bscscan.com/tx/0x28d2b65d323ff509a4f6c6cbb6dfa8d241f6b698651eb753835846fe48a55536

TESTS

Action: Set BUSD as dividend token (TLC mainnet contract will give wrapped lunc as dividends)

https://testnet.bscscan.com/tx/0x97f0014571228259709cd0b844ac3415d34085139ab7063377b7d29351c1e1d8

Action: Set BUSD treasury wallet

0xd6184F499D19cC7A7e0b4B5309af077870bEeBc7 (bnb and busd, in mainnet the terra cash team will collect treasury funds in BUSD and LUNC)

https://testnet.bscscan.com/tx/0x8dea745362b407acdb64d75f2932840be3663d6fdd61e472cc445a96199551e1

Action: Set LUNC treasury wallet

https://testnet.bscscan.com/tx/0x034fe919dfaa00604635ec888578c701eaa8e581b4112807175bd83a0ce030fa

SWAPS TESTS

Action: Approve router for 300000000 TLC

https://testnet.bscscan.com/tx/0xdd557cd27de4faec6912b606e7a542e4453e810842bad5bb94058bf958f1a53e

Action: ADD liquidity 300000000 TLC and 0.32 bnb

https://testnet.bscscan.com/tx/0x33b976fd5d66545dcc93f14a1c8fb5dd3e670b094e50826bd3e27b9901fc819b

Action:Swap BNB for TLC

https://testnet.bscscan.com/tx/0x659118ec015d8da1d23111d7fde051b02c87718322348d7ed2ba9fdf81c2068c

Action: approve to sell TLC

https://testnet.bscscan.com/tx/0xc3ee2f556605d1170ded20602027c44c009def067d6708cf74072511a83c70fe

Action: SELL TLC

https://testnet.bscscan.com/tx/0x81dcf6da979457ea1739387ee51bfb1cf00d860126dfe2063092fd27d16f7539

This sell triggered the swapatamount so the contract sold the tokens to distribute the fees
and the dividends.
We checked and:
-Burn happens correctly
-Fees are distributed

CONCLUSION

This is a dividend contract with transfers on fees;
every transaction (swaps,transfers) will take fees that are needed to provide the dividends and treasury funds; Terra Cash smart contract will burn LUNC correctly.

The contract has owner privileges that will allow the owner to change the following parameters:
Fees, treasury wallet where treasury fees will go, blacklist, minimum tokens to hold to get the dividends,exclude/include from fees and dividends.
Suggestion: Renounce ownership once the parameters are set and the owner doesn't need to change the parameters anymore, however the owner must take in consideration that by renuncing the ownership he won't be able to change any parameter that could be useful such as exclude from fees an exchange address.

Terra Cash Smart contract could take a high amount of gas due to the triggering of the swapatamount function needed to distribute dividends, burn lunc and collect treasury funds.

The smart contract only works properly if there is enough liquidity in the token pool pther-wise transactions will fail and the contract will be stuck untill there will be enough liquidity to allow the contract to swap and liquify the tokens in the contract itself

Terra Cash smart contract audited works as expected and it can be used in production.

DISCLAIMER

By reading this report or any part of it, you agree to the terms of this Disclaimer.
This report is provided for information purposes only and on a non-reliance basis and does not constitute investment advice. No one shall have any right to rely on the report or its contents and SnipeFinance.com owns no duty of care towards you or any other person, nor does Snipefinance.com make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided as is, without any conditions, warranties or other terms of any kind except as set out in this disclaimer, SnipeFinance.com hereby excludes all representations, warranties, conditions and other terms, SnipeFinance.com hereby excludes all liability and responsibility and neither you nor any other person shall have any claim against SnipeFinance.com for any amount or kind of loss or damage that may result to you or any other person(including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and water in delict, tort(including without limitations negligence), contract, breach of statutory duty, misinterpretation (weather innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intended to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. SnipeFinance.com's positions that each company and individual are responsible for their own due diligence and continuous security. SnipeFinance.com's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.