



TechRate
AUDIT COMPANY

Smart Contract Security Audit

Audit Details



Audited project

Christmas Elf



Deployer address

0xb9ec396a1522a2fc3133af9d4fd5faaf355c3b8b



Client contacts:

Christmas Elf team



Blockchain

Binance Smart Chain



Project website:

<https://www.christmaselftoken.com>

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. 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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate 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, and TechRate hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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 whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether 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.

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.

Background

TechRate was commissioned by Christmas Elf to perform an audit of smart contracts:

<https://bscscan.com/address/0xc139e2cc7a99885d8bd7af6ff21c7a2b58605a3e#code>

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 12.11.2021

Contract name	Christmas Elf
Contract address	0xC139E2CC7a99885D8BD7aF6FF21c7a2B58605A3e
Total supply	10,000,000,000,000,000
Token ticker	cElf
Decimals	4
Token holders	528
Transactions count	4,627
Top 100 holders dominance	82.75%
Total fee	1300
Autoliquidity fee receiver	0x0000000000000000000000000000000000dead
Marketing fee receiver	0xd4bca17c4b2d5517c35f0c393b78c4ee46c2c5af
Pair	0xc8065853aede3c1f56a2e10b24d95827745c573b
Contract deployer address	0xb9ec396a1522a2fc3133af9d4fd5faaf355c3b8b
Contract's current owner address	0xb9ec396a1522a2fc3133af9d4fd5faaf355c3b8b

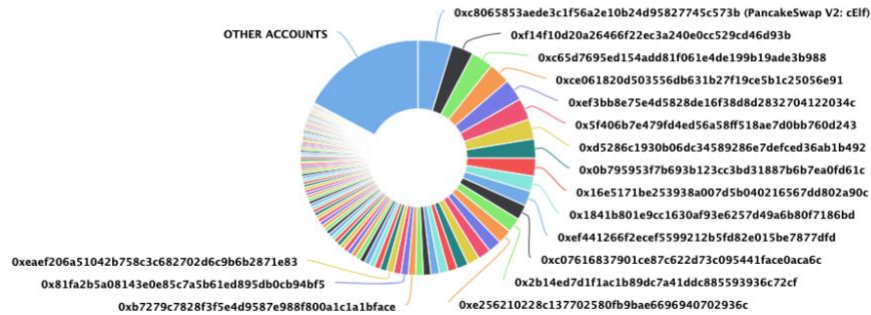
Christmas Elf Token Distribution

The top 100 holders collectively own 82.75% (8,274,621,405,757,420.00 Tokens) of Christmas Elf

Token Total Supply: 10,000,000,000,000.00 Token | Total Token Holders: 528

Christmas Elf Top 100 Token Holders

Source: BscScan.com



(A total of 8,274,621,405,757,420.00 tokens held by the top 100 accounts from the total supply of 10,000,000,000,000.00 token)

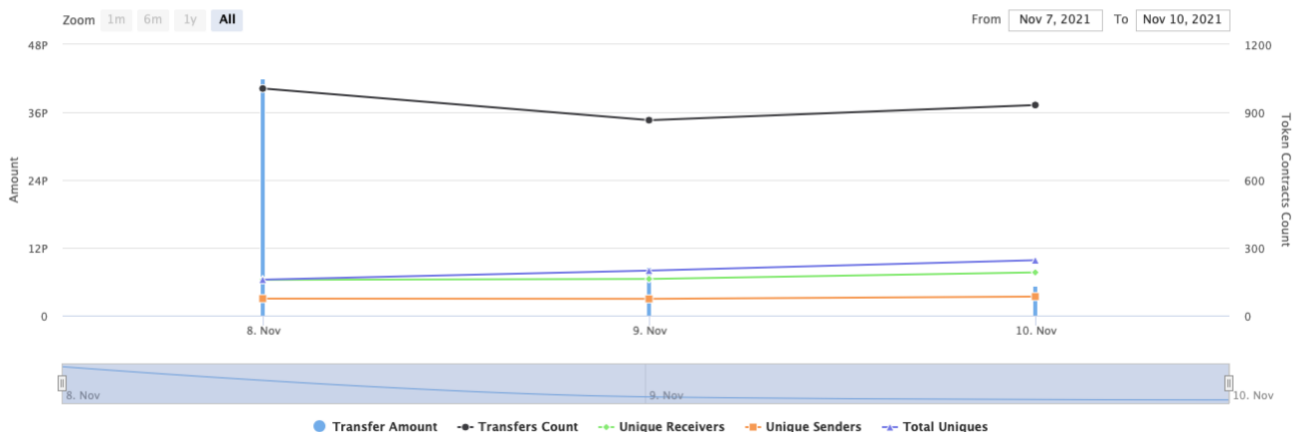
Christmas Elf Contract Interaction Details

Time Series: Token Contract Overview


Mon 8, Nov 2021 - Wed 10, Nov 2021

Token Contract 0xc139e2cc7a99885d8bd7af6ff21c7a2b58605a3e (Christmas Elf)

Source: BscScan.com



Christmas Elf Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	 PancakeSwap V2: cElf	473,862,758,358,357.5604	4.7386%
2	0xf14f10d20a26466f22ec3a240e0cc529cd46d93b	299,999,999,999,925.2326	3.0000%
3	0xc65d7695ed154add81f061e4de199b19ade3b988	299,815,179,545,301.8044	2.9982%
4	0xce061820d503556db631b27f119ce5b1c25056e91	299,712,864,977,361.4127	2.9971%
5	0xef3bb8e75e4d5828de16f38d8d2832704122034c	297,257,645,672,105.0251	2.9726%
6	0x5f406b7e479fd4ed56a58ff518ae7d0bb760d243	296,563,121,501,790.3113	2.9656%
7	0xd5286c1930b06dc34589286e7defced36ab1b492	275,838,986,219,864.4099	2.7584%
8	0x0b795953f7b693b123cc3bd31887b6b7ea0fd61c	265,120,453,035,838.286	2.6512%
9	0x16e5171be253938a007d5b040216567dd802a90c	244,716,093,351,551.3533	2.4472%
10	0x1841b801e9cc1630af93e6257d49a6b80f7186bd	209,796,082,570,776.4532	2.0980%



Contract functions details

+ [Lib] SafeMath

- [Int] tryAdd
- [Int] trySub
- [Int] tryMul
- [Int] tryDiv
- [Int] tryMod
- [Int] add
- [Int] sub
- [Int] mul
- [Int] div
- [Int] mod
- [Int] sub
- [Int] div
- [Int] mod

+ [Int] IBEP20

- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ Auth

- [Pub] <Constructor> #
- [Pub] authorize #
 - modifiers: onlyOwner
- [Pub] isOwner
- [Pub] isAuthorized
- [Pub] transferOwnership #
 - modifiers: onlyOwner

+ [Int] IDEXFactory

- [Ext] createPair #

+ [Int] IDEXRouter

- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidity #
- [Ext] addLiquidityETH (\$)
- [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
- [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens (\$)
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] IDividendDistributor

- [Ext] setDistributionCriteria #
- [Ext] setShare #

- [Ext] deposit (\$)
- [Ext] process #
- + DividendDistributor (IDividendDistributor)
 - [Pub] <Constructor> #
 - [Ext] setDistributionCriteria #
 - modifiers: onlyToken
 - [Ext] setShare #
 - modifiers: onlyToken
 - [Ext] deposit (\$)
 - modifiers: onlyToken
 - [Ext] process #
 - modifiers: onlyToken
 - [Int] shouldDistribute
 - [Int] distributeDividend #
 - [Ext] claimDividend #
 - [Pub] getUnpaidEarnings
 - [Int] getCumulativeDividends
 - [Int] addShareholder #
 - [Int] removeShareholder #
- + ChristmasElf (IBEP20, Auth)
 - [Pub] <Constructor> #
 - modifiers: Auth
 - [Ext] <Fallback> (\$)
 - [Ext] totalSupply
 - [Ext] decimals
 - [Ext] symbol
 - [Ext] name
 - [Ext] getOwner
 - [Pub] balanceOf
 - [Ext] allowance
 - [Pub] approve #
 - [Ext] approveMax #
 - [Ext] transfer #
 - [Ext] transferFrom #
 - [Ext] setMaxWalletPercent #
 - modifiers: onlyOwner
 - [Int] _transferFrom #
 - [Int] _basicTransfer #
 - [Int] checkTxLimit
 - [Int] shouldTakeFee
 - [Int] takeFee #
 - [Int] shouldSwapBack
 - [Ext] clearStuckBalance #
 - modifiers: onlyOwner
 - [Pub] cooldownEnabled #
 - modifiers: onlyOwner
 - [Int] swapBack #
 - modifiers: swapping
 - [Ext] setTxLimit #
 - modifiers: authorized
 - [Ext] setIsDividendExempt #
 - modifiers: authorized
 - [Ext] setIsFeeExempt #

- modifiers: authorized
- [Ext] setLsTxLimitExempt #
 - modifiers: authorized
- [Ext] setLsTimelockExempt #
 - modifiers: authorized
- [Ext] setFees #
 - modifiers: authorized
- [Ext] setFeeReceivers #
 - modifiers: authorized
- [Ext] setSwapBackSettings #
 - modifiers: authorized
- [Ext] setTargetLiquidity #
 - modifiers: authorized
- [Ext] setDistributionCriteria #
 - modifiers: authorized
- [Ext] setDistributorSettings #
 - modifiers: authorized
- [Pub] getCirculatingSupply
- [Pub] getLiquidityBacking
- [Pub] isOverLiquified

(\$) = payable function

= non-constant function

Issues Checking Status

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

Security Issues

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

No low severity issues found.

Owner privileges (In the period when the owner is not renounced)

- Owner can change the maximum transaction amount.
- Owner can include in and exclude from dividends.
- Owner can include in and exclude from fee and transaction amount.
- Owner can change fees.
- Owner can enable/disable trading.
- Owner can change fee receivers.
- Owner can change swap threshold and disable/enable swap.
- Owner can change target liquidity values.
- Owner can change distribution criteria.
- Owner can change distribution GAS.
- Owner can change setMaxWalletPercent.
- Owner can withdraw BNBs to the marketing receiver address.
- Owner can change trading status.
- Owner can change cooldown status.
- Owner can change buybackKeepItSimple value.
- Owner can change addresses' isTimelockExempt value.

Conclusion

Smart contracts do not contain high severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details provided by the team:

<https://bscscan.com/tx/0xea64ed45c481708a67cd5cb8a154e766e20e2fb73d8e1d41967b0f5a877c7ed6>

TechRate note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.