



TechRate
AUDIT COMPANY

Smart Contract Security Audit

Audit Details



Audited project

SummerCake



Deployer address

0x3dFeE8B31CB1A136c468DeAf800962e84A6FA8A7



Client contacts:

SummerCake team



Blockchain

Binance Smart Chain



Project website:

<https://www.summertime.app>

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 SummerCake to perform an audit of smart contracts:

<https://bscscan.com/address/0xe4fb673830741daf3c87354e99d2bf4c39a60828#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 28.07.2021

Contract name	SummerCake
Contract address	0xe4fB673830741dAf3C87354e99d2bf4c39a60828
Total supply	100,000,000,000
Token ticker	SCAKE
Decimals	18
Token holders	451
Transactions count	4,241
Top 100 holders dominance	98.04%
Circulating supply	999999999180000000000000000000
Total reflected	4621990370471497525121
Total fee	1800
LP pair	0x6702977b50c215bbf0383e86c50b126cc348d69a
Contract deployer address	0x3dFeE8B31CB1A136c468DeAf800962e84A6FA8A7
Contract's current owner address	0x3dfee8b31cb1a136c468deaf800962e84a6fa8a7

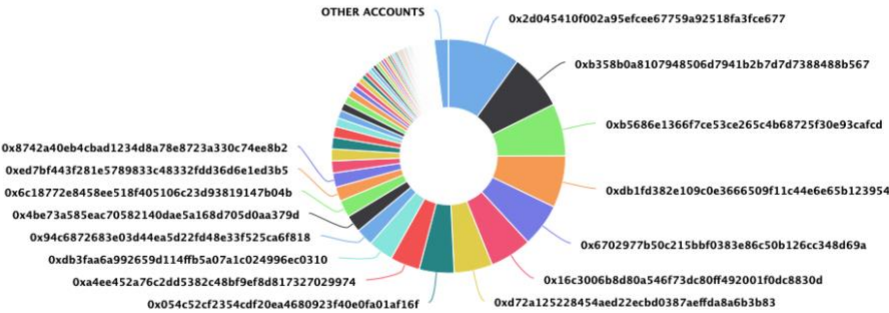
SummerCake Token Distribution

The top 100 holders collectively own 98.04% (98,043,432,273.76 Tokens) of SummerCake

Token Total Supply: 100,000,000,000.00 Token | Total Token Holders: 451

SummerCake Top 100 Token Holders

Source: BscScan.com



(A total of 98,043,432,273.76 tokens held by the top 100 accounts from the total supply of 100,000,000,000.00 token)

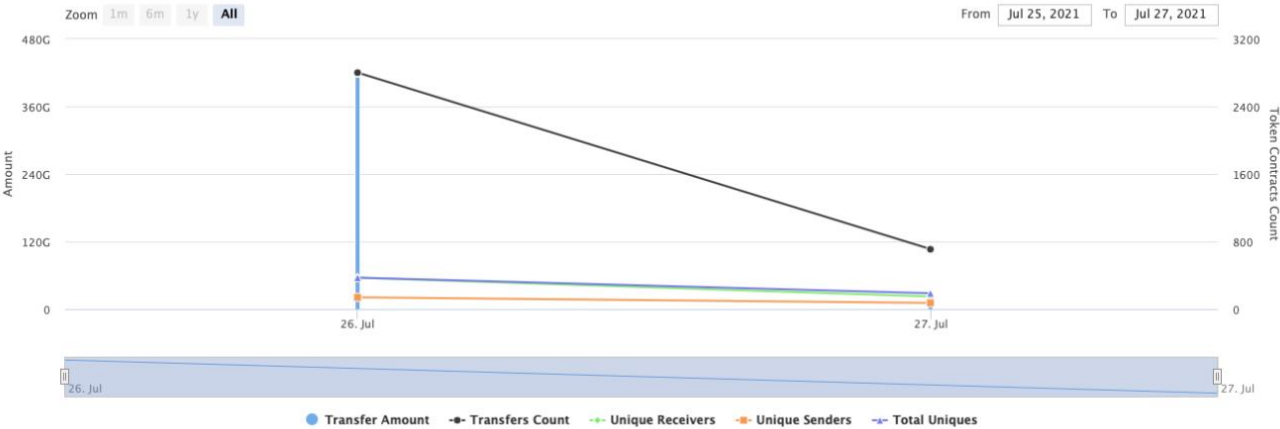
SummerCake Contract Interaction Details

Time Series: Token Contract Overview



Mon 26, Jul 2021 - Tue 27, Jul 2021

Token Contract 0xe4fb673830741daf3c87354e99d2bf4c39a60828 (SummerCake)



Source: BscScan.com



SummerCake Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	 0x2d045410f002a95efcee67759a92518fa3fce677	10,000,000,000	10.0000%
2	0xb358b0a8107948506d7941b2b7d7d7388488b567	7,732,983,666.049317890939879512	7.7330%
3	0xb5686e1366f7ce53ce265c4b68725f30e93cafc	7,253,140,631.570257563154155774	7.2531%
4	0xdb1fd382e109c0e3666509f11c44e6e65b123954	7,163,604,796.322188980648602684	7.1636%
5	 0x6702977b50c215bbf0383e86c50b126cc348d69a	5,986,679,100.496801750896315071	5.9867%
6	0x16c3006b8d80a546f73dc80f492001f0dc8830d	5,789,863,088.238191245991632916	5.7899%
7	0xd72a125228454aed22ecbd0387aeffda8a6b3b83	5,317,368,591.456442088120073397	5.3174%
8	0x054c52cf2354cdf20ea4680923f40e0fa01af16f	4,800,586,201.166507706527566303	4.8006%
9	0xa4ee452a76c2dd5382c48b9ef8d817327029974	4,100,000,000	4.1000%
10	0xdb3faa6a992659d114ffb5a07a1c024996ec0310	3,456,203,482.818433751876925091	3.4562%

SummerCake Top LP Token Holders

Rank	Address	Quantity	Percentage
1	 0x8655e5c4d701186d16765d1cdcef6d5287e4679a	972,111.104761179034643895	78.4396%
2	Burn Address	261,619.7947155303513418	21.1101%
3	0x8cc7bc33f5188b1fb683bedc4dbffa77b136833b	5,580.421599402155256871	0.4503%
4	 0x00	0.000000000000001	0.0000%



Contract functions details

+ Context

- [Int] _msgSender
- [Int] _msgData

+ [Int] IERC20

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

+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod

+ [Lib] Address

- [Int] isContract
- [Int] sendValue #
- [Int] functionCall #
- [Int] functionCall #
- [Int] functionCallWithValue #
- [Int] functionCallWithValue #
- [Prv] _functionCallWithValue #

+ [Int] IUniswapV2Factory

- [Ext] feeTo
- [Ext] feeToSetter
- [Ext] getPair
- [Ext] allPairs
- [Ext] allPairsLength
- [Ext] createPair #
- [Ext] setFeeTo #
- [Ext] setFeeToSetter #

+ [Int] IUniswapV2Pair

- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [Ext] totalSupply
- [Ext] balanceOf

- [Ext] allowance
- [Ext] approve #
- [Ext] transfer #
- [Ext] transferFrom #
- [Ext] DOMAIN_SEPARATOR
- [Ext] PERMIT_TYPEHASH
- [Ext] nonces
- [Ext] permit #
- [Ext] MINIMUM_LIQUIDITY
- [Ext] factory
- [Ext] token0
- [Ext] token1
- [Ext] getReserves
- [Ext] price0CumulativeLast
- [Ext] price1CumulativeLast
- [Ext] kLast
- [Ext] mint #
- [Ext] burn #
- [Ext] swap #
- [Ext] skim #
- [Ext] sync #
- [Ext] initialize #

+ [Int] IUniswapV2Router01

- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidity #
- [Ext] addLiquidityETH (\$)
- [Ext] removeLiquidity #
- [Ext] removeLiquidityETH #
- [Ext] removeLiquidityWithPermit #
- [Ext] removeLiquidityETHWithPermit #
- [Ext] swapExactTokensForTokens #
- [Ext] swapTokensForExactTokens #
- [Ext] swapExactETHForTokens (\$)
- [Ext] swapTokensForExactETH #
- [Ext] swapExactTokensForETH #
- [Ext] swapETHForExactTokens (\$)
- [Ext] quote
- [Ext] getAmountOut
- [Ext] getAmountIn
- [Ext] getAmountsOut
- [Ext] getAmountsIn

+ [Int] IUniswapV2Router02 (IUniswapV2Router01)

- [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
- [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
- [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
- [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens (\$)
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] Cashier

- [Ext] setToken #
- [Ext] whomst
- [Ext] setReflectionCriteria #

- [Ext] setShare #
- [Ext] deposit (\$)
- [Ext] process #
- [Ext] giveMeWelfarePlease #
- [Ext] getTotalDistributed
- + Ownable (Context)
 - [Pub] <Constructor> #
 - [Pub] owner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
- + ReflectionToken (IERC20, Ownable)
 - [Pub] <Constructor> (\$)
 - [Ext] <Fallback> (\$)
 - [Ext] totalSupply
 - [Ext] decimals
 - [Ext] symbol
 - [Ext] name
 - [Ext] getOwner
 - [Pub] balanceOf
 - [Ext] allowance
 - [Pub] approve #
 - [Pub] approveMax #
 - [Prv] _approve #
 - [Ext] transfer #
 - [Ext] transferFrom #
 - [Pub] isSniper
 - [Ext] removeSniper #
 - modifiers: onlyOwner
 - [Ext] setSniperProtectionEnabled #
 - modifiers: onlyOwner
 - [Pub] setDividendExcluded #
 - modifiers: onlyOwner
 - [Pub] setExcludeFromFees #
 - modifiers: onlyOwner
 - [Ext] setTaxes #
 - modifiers: onlyOwner
 - [Ext] setMarketingWallet #
 - modifiers: onlyOwner
 - [Ext] setSwapBackSettings #
 - modifiers: onlyOwner
 - [Ext] setSwapThreshold #
 - modifiers: onlyOwner
 - [Ext] setTargetLiquidity #
 - modifiers: onlyOwner
 - [Ext] setReflectionCriteria #
 - modifiers: onlyOwner
 - [Ext] setReflectorSettings #
 - modifiers: onlyOwner
 - [Pub] getCirculatingSupply
 - [Pub] getLiquidityBacking
 - [Pub] isOverLiquified

- [Ext] giveMeWelfarePlease #
- [Ext] getTotalReflected
- [Ext] setMaxTxPercent #
 - modifiers: onlyOwner
- [Prv] _hasLimits
- [Int] _transfer #
- [Int] _finalizeTransfer #
- [Int] shouldSwapBack
- [Int] processTokenReflect #
- [Int] _basicTransfer #
- [Int] shouldTakeFee
- [Pub] getTotalFee
- [Int] takeTaxes #
- [Int] swapBack #
 - modifiers: swapping
- [Prv] _checkLiquidityAdd #

(\$) = 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.	Low issues
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

1. Safe math

Issue:

- Solidity version acceptable for the contract is “ $\geq 0.6.0 < 0.9.0$ ”, if Solidity version would be lower than 0.8.0, then code blocks without safe math could fail (if there will be inappropriate values).

Recommendation:

Fix solidity version from actual value, not the old one.

Notes:

- swapBack function distributes reflection and marketing fee and adds liquidity.
- If dynamic liquidity fee will equal to zero, liquidity fee part goes to marketing.
- reflector(Cashier) provided only as interface, so actual working of its functions is not audited.

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

- Owner can remove sniper.
- Owner can enable and disable sniper protection.
- Owner can exclude and include in dividends.
- Owner can exclude from the fees.
- Owner can change the fees.
- Owner can change marketing wallet.
- Owner can change swap back settings.
- Owner can change target liquidity.
- Owner can change reflection criteria.
- Owner can change reflector GAS amount.
- Owner can change the maximum transaction amount.

Conclusion

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

Liquidity locking details provided by the team:

https://dxsale.app/app/v2_9/dxlockview?id=0&add=0xCd0ca188c1735C9AA17C4eec839fC1513F41E2Fd&type=lplock&chain=BSC

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.