Smart Contract Security Audit

TechRate

October, 2021

Audit Details

Audited project

SquidGameToken

Deployer address

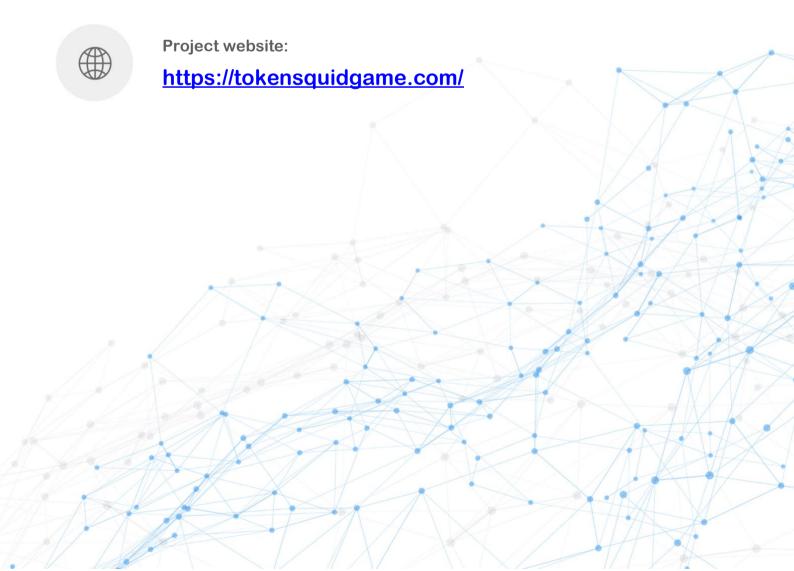0xd308b1199d09556c02ca491aeaceecaa67f7b465

Client contacts:

SquidGameToken team

Blockchain

Binance Smart Chain

Project website:

https://tokensquidgame.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 SquidGameToken to perform an audit of smart contracts:
https://bscscan.com/address/0x440fc7da66e34e01af5201bdf5815739b0ae743f#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 26.10.2021

Contract name	SquidGameToken
Contract address	0x440Fc7DA66e34e01af5201BdF5815739B0Ae743f
Total supply	100,000,000,000
Token ticker	SGT
Decimals	18
Token holders	13,163
Transactions count	68,100
Top 100 holders dominance	64.21%
Liquidity fee	3
ETH reward fee	5
Marketing fee	8
Total fees	16
Dividend tracker	0x9a69641ed201d314b6030673eecf76143eaabc6b
Uniswap V2 pair	0xae7db8558a37353beab610710236ed886cd50442
Contract deployer address	0xd308b1199d09556c02ca491aeaceecaa67f7b465
Contract's current owner address	0xd308b1199d09556c02ca491aeaceecaa67f7b465

SquidGameToken Token Distribution

SquidGameToken Top 100 Token Holders
Source: BscScan.com

0x81e0ef68e103ee65002d3cf766240ed1c070334d

0xae7db8558a37353beab610710236ed886cd50442
(PancakeSwap V2: SGT 44)

0x22540107cc687153ff2d7d8dff7102586fc45a92

0x0000000000000000000000000000000000000001

0x2d3e91563d67e81478944f5f1f08a029c5bf176c

0x91325e3332d55752bff8f1e1707382a5839cf6a0

0x79be56c63589bb920faf1ac812d3b0df34059a2c

0xf0d882c3633e96c30eeb54a381225cc3e04920f1

0x012836b24764b172a970401f92ce77bed2f0b2b1

OTHER ACCOUNTS

0x0e1464134575e5d74620509b847e02d21cf9ec03

0xc554b8ff4dbbd393ace5c3497ab8b51c0e1c6f77

0x8c8bc1d0db3c0096c6798ffc6f1e1993083e3d26

(A total of 64,214,284,571.74 tokens held by the top 100 accounts from the total supply of 100,000,000,000.00 token)

SquidGameToken Contract Interaction Details

Time Series: Token Contract Overview   Thu 21, Oct 2021 - Mon 25, Oct 2021

Token Contract 0x440fc7da66e34e01af5201bdf5815739b0ae743f (SquidGameToken)
Source: BscScan.com

Zoom 1m 6m 1y All   From Oct 20, 2021 To Oct 25, 2021

● Transfer Amount ─●─ Transfers Count ─+─ Unique Receivers ─■─ Unique Senders ─▲─ Total Uniques

SquidGameToken Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x81e0ef68e103ee65002d3cf766240ed1c070334d	5,000,000,000	5.0000%
2	PancakeSwap V2: SGT 44	4,996,737,595.557492579519047835	4.9967%
3	0x22540107cc687153ff2d7d8dff7102586fc45a92	3,435,506,142.410973079699127566	3.4355%
4	0x0000000000000000000000000000000000000001	2,500,000,000	2.5000%
5	0x2d3e91563d67e81478944f5f1f08a029c5bf176c	2,258,487,659.649564656	2.2585%
6	0x91325e3332d55752bff8f1e1707382a5839cf6a0	1,497,277,381.133064868723708865	1.4973%
7	0x79be56c63589bb920faf1ac812d3b0df34059a2c	1,462,686,345.84816565	1.4627%
8	0xf0d882c3633e96c30eeb54a381225cc3e04920f1	1,305,704,082.078311884927111901	1.3057%
9	0x012836b24764b172a970401f92ce77bed2f0b2b1	1,250,000,000	1.2500%
10	0x83f9118bdf74e8b6c334a7881b0004dc3caee0e3	1,250,000,000	1.2500%

Contract functions details

+ **[Lib]** SafeMathUint
  - **[Int]** toInt256Safe

+ **[Lib]** SafeMathInt
  - **[Int]** mul
  - **[Int]** div
  - **[Int]** sub
  - **[Int]** add
  - **[Int]** abs
  - **[Int]** toUint256Safe

+ **[Lib]** SafeMath
  - **[Int]** add
  - **[Int]** sub
  - **[Int]** sub
  - **[Int]** mul
  - **[Int]** div
  - **[Int]** div
  - **[Int]** mod
  - **[Int]** mod

+ Ownable (Context)
  - **[Pub]** <Constructor> **#**
  - **[Pub]** owner
  - **[Pub]** renounceOwnership **#**
    - modifiers: onlyOwner
  - **[Pub]** transferOwnership **#**
    - modifiers: onlyOwner

+ **[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]** 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]** IUniswapV2Factory
  - **[Ext]** feeTo
  - **[Ext]** feeToSetter
  - **[Ext]** getPair
  - **[Ext]** allPairs
  - **[Ext]** allPairsLength
  - **[Ext]** createPair **#**
  - **[Ext]** setFeeTo **#**
  - **[Ext]** setFeeToSetter **#**

+ **[Lib]** IterableMapping
  - **[Pub]** get
  - **[Pub]** getIndexOfKey
  - **[Pub]** getKeyAtIndex
  - **[Pub]** size
  - **[Pub]** set **#**
  - **[Pub]** remove **#**

+ **[Int]** IERC20Metadata **(IERC20)**
  - **[Ext]** name

- **[Ext]** symbol
- **[Ext]** decimals

+ **[Int] IERC20**
  - **[Ext]** totalSupply
  - **[Ext]** balanceOf
  - **[Ext]** transfer **#**
  - **[Ext]** allowance
  - **[Ext]** approve **#**
  - **[Ext]** transferFrom **#**

+ **ERC20 (Context, IERC20, IERC20Metadata)**
  - **[Pub]** <Constructor> **#**
  - **[Pub]** name
  - **[Pub]** symbol
  - **[Pub]** decimals
  - **[Pub]** totalSupply
  - **[Pub]** balanceOf
  - **[Pub]** transfer **#**
  - **[Pub]** allowance
  - **[Pub]** approve **#**
  - **[Pub]** transferFrom **#**
  - **[Pub]** increaseAllowance **#**
  - **[Pub]** decreaseAllowance **#**
  - [Int] _transfer **#**
  - [Int] _mint **#**
  - [Int] _burn **#**
  - [Int] _approve **#**
  - [Int] _beforeTokenTransfer **#**

+ **[Int] DividendPayingTokenOptionalInterface**
  - **[Ext]** withdrawableDividendOf
  - **[Ext]** withdrawnDividendOf
  - **[Ext]** accumulativeDividendOf

+ **[Int] DividendPayingTokenInterface**
  - **[Ext]** dividendOf
  - **[Ext]** withdrawDividend **#**

+ **DividendPayingToken (ERC20, Ownable, DividendPayingTokenInterface, DividendPayingTokenOptionalInterface)**
  - **[Pub]** <Constructor> **#**
    - modifiers: ERC20
  - **[Pub]** distributeETHDividends **#**
    - modifiers: onlyOwner
  - **[Pub]** withdrawDividend **#**
  - [Int] _withdrawDividendOfUser **#**
  - **[Pub]** dividendOf
  - **[Pub]** withdrawableDividendOf
  - **[Pub]** withdrawnDividendOf
  - **[Pub]** accumulativeDividendOf
  - [Int] _transfer **#**
  - [Int] _mint **#**
  - [Int] _burn **#**
  - [Int] _setBalance **#**

+ **Context**
  - [Int] _msgSender
  - [Int] _msgData

+ **SquidGameToken** (ERC20, Ownable)
  - **[Pub]** <Constructor> #
    - modifiers: ERC20
  - **[Ext]** <Fallback> ($)
  - **[Pub]** updateDividendTracker #
    - modifiers: onlyOwner
  - **[Pub]** updateUniswapV2Router #
    - modifiers: onlyOwner
  - **[Pub]** excludeFromFees #
    - modifiers: onlyOwner
  - **[Pub]** excludeMultipleAccountsFromFees #
    - modifiers: onlyOwner
  - **[Ext]** setMarketingWallet #
    - modifiers: onlyOwner
  - **[Ext]** setETHRewardsFee #
    - modifiers: onlyOwner
  - **[Ext]** setLiquiditFee #
    - modifiers: onlyOwner
  - **[Ext]** setMarketingFee #
    - modifiers: onlyOwner
  - **[Ext]** setMaxWalletLimit #
    - modifiers: onlyOwner
  - **[Pub]** setAutomatedMarketMakerPair #
    - modifiers: onlyOwner
  - **[Ext]** blacklistAddress #
    - modifiers: onlyOwner
  - **[Prv]** _setAutomatedMarketMakerPair #
  - **[Pub]** updateGasForProcessing #
    - modifiers: onlyOwner
  - **[Ext]** updateClaimWait #
    - modifiers: onlyOwner
  - **[Ext]** getClaimWait
  - **[Ext]** getTotalDividendsDistributed
  - **[Pub]** isExcludedFromFees
  - **[Pub]** withdrawableDividendOf
  - **[Pub]** dividendTokenBalanceOf
  - **[Ext]** excludeFromDividends #
    - modifiers: onlyOwner
  - **[Ext]** getAccountDividendsInfo
  - **[Ext]** getAccountDividendsInfoAtIndex
  - **[Ext]** processDividendTracker #
  - **[Ext]** claim #
  - **[Ext]** getLastProcessedIndex
  - **[Ext]** getNumberOfDividendTokenHolders
  - **[Int]** _transfer #
  - **[Prv]** swapAndSendToFee #
  - **[Prv]** swapAndLiquify #
  - **[Prv]** swapTokensForEth #
  - **[Prv]** swapTokensForETH #
  - **[Prv]** addLiquidity #

- **[Prv]** swapAndSendDividends **#**

+ **SquidGameTokenDividendTracker** (Ownable, DividendPayingToken)
  - **[Pub]** <Constructor> **#**
    - modifiers: DividendPayingToken
  - **[Int]** _transfer **#**
  - **[Pub]** withdrawDividend **#**
  - **[Ext]** excludeFromDividends **#**
    - modifiers: onlyOwner
  - **[Ext]** updateClaimWait **#**
    - modifiers: onlyOwner
  - **[Ext]** getLastProcessedIndex
  - **[Ext]** getNumberOfTokenHolders
  - **[Pub]** getAccount
  - **[Pub]** getAccountAtIndex
  - **[Prv]** canAutoClaim
  - **[Ext]** setBalance **#**
    - modifiers: onlyOwner
  - **[Pub]** process **#**
  - **[Pub]** processAccount **#**
    - modifiers: onlyOwner

($) = 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.	Low issues
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

1. Out of gas

Issue:

- **The function excludeMultipleAccountsFromFees() uses the loop to exclude multiple accounts from fees. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.**

Recommendation:
Be careful about accounts array length.

Notes:

- **Dividend tracker may be changed. So that logic of setBalance and other functions could be another and not audited.**

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

- **Owner can change dividend tracker.**
- **Owner can change Uniswap router address.**
- **Owner can exclude from the fees.**
- **Owner can change _maxWalletLimit.**
- **Owner can blacklist addresses.**
- **Owner can change liquidity, marketing and ETH reward fees.**
- **Owner can exclude and include addresses in automatedMarketMakerPairs array.**
- **Owner can exclude from dividends.**
- **Owner can change marketing wallet.**
- **Owner can change gas for processing.**
- **Owner can update claimWait value.**

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details are provided by the team:
https://dxsale.app/app/v3/dxlockview?id=0&add=0xD308B1199d09556c02ca491AEacEeCAa67f7b465&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.