Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

October, 2021

Audit Details

Audited project

INSTINCT

Deployer address

0x84b30aac7f5abb0b5447eb1ab9f54ffb0d5b1efb

Client contacts:

INSTINCT team

Blockchain

Binance Smart Chain

Project website:

instinct.game

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 INSTINCT to perform an audit of smart contracts:
https://www.bscscan.com/address/0xc4eeb3199df249a6bce8ff706fe86c08c5f847d0#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.

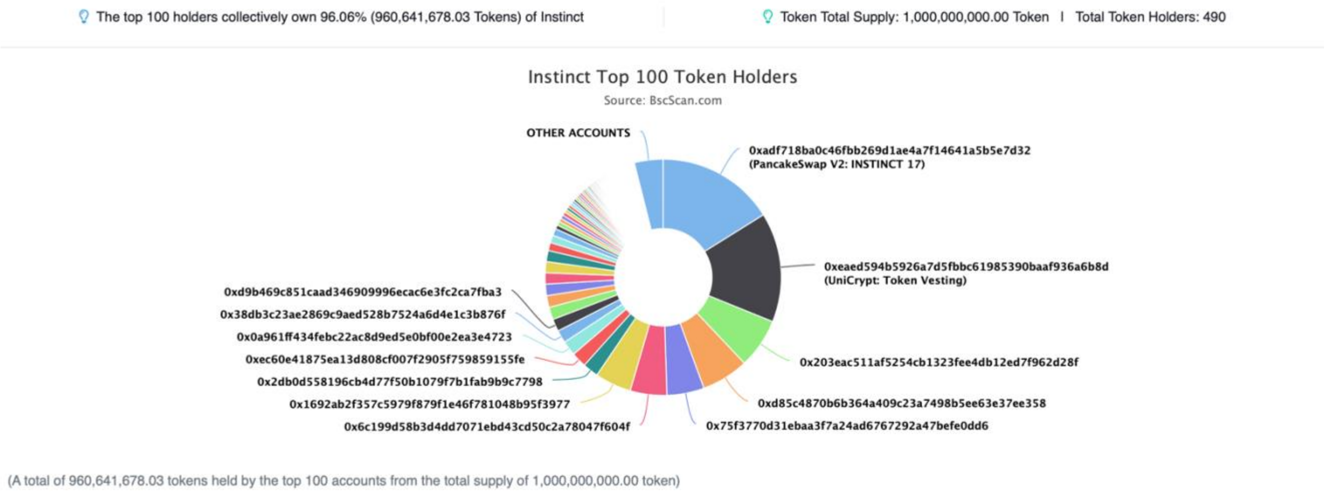
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 13.10.2021

Contract name	INSTINCT
Contract address	0xc4eEb3199dF249a6BCE8fF706Fe86C08c5f847D0
Total supply	1,000,000,000
Token ticker	INSTINCT
Decimals	18
Token holders	490
Transactions count	1,787
Top 100 holders dominance	96.06%
Buy buyback fee	2
Buy charity fee	1
Buy token rewards fee	7
Buy market fee	6
Buy total fees	16
Dividend tracker	0xcb1c806e71357cad9db6f839c990fe02273feb85
Uniswap V2 pair	0xadf718ba0c46fbb269d1ae4a7f14641a5b5e7d32
Contract deployer address	0x84b30aac7f5abb0b5447eb1ab9f54ffb0d5b1efb
Contract’s current owner address	0x84b30aac7f5abb0b5447eb1ab9f54ffb0d5b1efb

INSTINCT Token Distribution



The top 100 holders collectively own 96.06% (960,641,678.03 Tokens) of Instinct

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 490

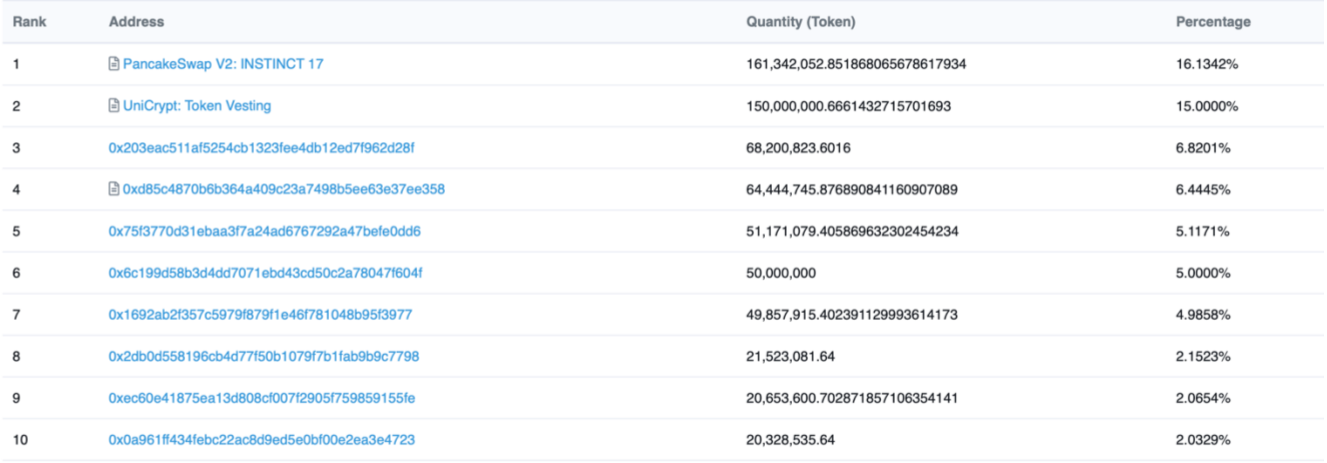
Instinct Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0xadf718ba0c46fbb269d1ae4a7f14641a5b5e7d32 (PancakeSwap V2: INSTINCT 17)
0xeaed594b5926a7d5fbbc61985390baaf936a6b8d (UniCrypt: Token Vesting)
0x203eac511af5254cb1323fee4db12ed7f962d28f
0xd85c4870b6b364a409c23a7498b5ee63e37ee358
0x75f3770d31ebaa3f7a24ad6767292a47befe0dd6
0x6c199d58b3d4dd7071ebd43cd50c2a78047f604f
0x1692ab2f357c5979f879f1e46f781048b95f3977
0x2db0d558196cb4d77f50b1079f7b1fab9b9c7798
0xec60e41875ea13d808cf007f2905f759859155fe
0x0a961ff434febc22ac8d9ed5e0bf00e2ea3e4723
0x38db3c23ae2869c9aed528b7524a6d4e1c3b876f
0xd9b469c851caad346909996ecac6e3fc2ca7fba3

(A total of 960,641,678.03 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

INSTINCT Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap V2: INSTINCT 17	161,342,052.851868065678617934	16.1342%
2	UniCrypt: Token Vesting	150,000,000.6661432715701693	15.0000%
3	0x203eac511af5254cb1323fee4db12ed7f962d28f	68,200,823.6016	6.8201%
4	0xd85c4870b6b364a409c23a7498b5ee63e37ee358	64,444,745.876890841160907089	6.4445%
5	0x75f3770d31ebaa3f7a24ad6767292a47befe0dd6	51,171,079.405869632302454234	5.1171%
6	0x6c199d58b3d4dd7071ebd43cd50c2a78047f604f	50,000,000	5.0000%
7	0x1692ab2f357c5979f879f1e46f781048b95f3977	49,857,915.402391129993614173	4.9858%
8	0x2db0d558196cb4d77f50b1079f7b1fab9b9c7798	21,523,081.64	2.1523%
9	0xec60e41875ea13d808cf007f2905f759859155fe	20,653,600.702871857106354141	2.0654%
10	0x0a961ff434febc22ac8d9ed5e0bf00e2ea3e4723	20,328,535.64	2.0329%

Contract functions details

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

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

+ [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] 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 #

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

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

+ [Int] IDividendPayingTokenOptional
  - [Ext] withdrawableDividendOf
  - [Ext] withdrawnDividendOf
  - [Ext] accumulativeDividendOf

+ [Int] IDividendPayingToken
  - [Ext] dividendOf
  - [Ext] distributeDividends ($)
  - [Ext] withdrawDividend #

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

+ [Lib] SafeMathUint
  - [Int] toInt256Safe

+  ERC20 (Context, IERC20)
  - [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] _setupDecimals #
  - [Int] _beforeTokenTransfer #

+ [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

+  DividendPayingToken (ERC20, IDividendPayingToken,
IDividendPayingTokenOptional)
  - [Pub] <Constructor> #
    - modifiers: ERC20
  - [Ext] <Fallback> ($)
  - [Pub] updateMasterContract #
    - modifiers: onlyMaster
```

  - [Pub] updateUniswapV2Router #
    - modifiers: onlyMaster
  - [Pub] updateDividendTokenUser #
    - modifiers: onlyMaster
  - [Pub] getDividendTokenUser
  - [Pub] distributeDividends ($)
  - [Pub] distributeTokenDividends #
    - modifiers: onlyMaster
  - [Pub] withdrawDividend #
  - [Prv] swapEthForTokens #
  - [Int] _withdrawDividendOfUser #
  - [Pub] dividendOf
  - [Pub] withdrawableDividendOf
  - [Pub] withdrawnDividendOf
  - [Pub] accumulativeDividendOf
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _setBalance #

+ INSTINCT (ERC20, Ownable)
  - [Pub] <Constructor> #
    - modifiers: ERC20
  - [Ext] <Fallback> ($)
  - [Int] restoreFees #
  - [Ext] swapAndLiquifyOwner #
    - modifiers: onlyOwner
  - [Ext] swapAndSendDividendsOwner #
    - modifiers: onlyOwner
  - [Ext] updateMaxSellTx #
    - modifiers: onlyOwner
  - [Ext] updateMaxBuyTx #
    - modifiers: onlyOwner
  - [Ext] updateDividendTokenUser #
  - [Ext] getDividendTokenUser
  - [Ext] updatedividendTime #
    - modifiers: onlyOwner
  - [Ext] updateBuyBackMode #
    - modifiers: onlyOwner
  - [Ext] updateTradingEnabledTime #
    - modifiers: onlyOwner
  - [Ext] updateMinimumBalanceForDividends #
    - modifiers: onlyOwner
  - [Ext] updateMaxWalletAmount #
    - modifiers: onlyOwner
  - [Ext] updateSwapAtAmount #
    - modifiers: onlyOwner
  - [Ext] updateMarketAddress #
    - modifiers: onlyOwner
  - [Ext] updateCharityAddress #
    - modifiers: onlyOwner
  - [Ext] updateBuyBackAddress #
    - modifiers: onlyOwner
  - [Ext] updateMarketTokenFeeAddress #
    - modifiers: onlyOwner

  - [Ext] updateCharityTokenFeeAddress #
    - modifiers: onlyOwner
  - [Ext] updateBuyBackTokenFeeAddress #
    - modifiers: onlyOwner
  - [Ext] updateFees #
    - modifiers: onlyOwner
  - [Ext] updateBuyFees #
    - modifiers: onlyOwner
  - [Ext] updateSellFees #
    - modifiers: onlyOwner
  - [Ext] updateDividendTracker #
    - modifiers: onlyOwner
  - [Ext] updateUniswapV2Router #
    - modifiers: onlyOwner
  - [Pub] excludeFromFees #
    - modifiers: onlyOwner
  - [Pub] excludeFromDividends #
    - modifiers: onlyOwner
  - [Pub] enableDividends #
    - modifiers: onlyOwner
  - [Ext] excludeMultipleAccountsFromFees #
    - modifiers: onlyOwner
  - [Ext] setAutomatedMarketMakerPair #
    - modifiers: onlyOwner
  - [Prv] _setAutomatedMarketMakerPair #
  - [Pub] updateGasForProcessing #
    - modifiers: onlyOwner
  - [Ext] updateClaimWait #
    - modifiers: onlyOwner
  - [Ext] getClaimWait
  - [Ext] getTotalDividendsDistributed
  - [Pub] isExcludedFromFees
  - [Pub] withdrawableDividendOf
  - [Pub] dividendTokenBalanceOf
  - [Ext] getAccountDividendsInfo
  - [Ext] getAccountDividendsInfoAtIndex
  - [Ext] processDividendTracker #
  - [Ext] claim #
  - [Ext] getLastProcessedIndex
  - [Ext] getNumberOfDividendTokenHolders
  - [Pub] getTradingIsEnabled
  - [Prv] swapAndLiquify #
  - [Prv] swapEthForTokens #
  - [Prv] swapTokensForEth #
  - [Prv] swapTokensForTokens #
  - [Int] addLiquidity #
  - [Prv] swapAndSendDividends #
  - [Int] _transfer #

+ INSTINCTDividendTracker (DividendPayingToken, Ownable)
  - [Pub] <Constructor> #
    - modifiers: DividendPayingToken
  - [Ext] updateMinimumBalanceForDividends #
    - modifiers: onlyOwner
  - [Ext] updateTokenForDividend #

  - modifiers: onlyOwner
- [Int] _transfer #
- [Pub] withdrawDividend #
- [Ext] excludeFromDividends #
  - modifiers: onlyOwner
- [Ext] enableDividends #
  - 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.	Low issues
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.	Low issues
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:

Check that the accounts list is not too big.

Notes:

- Owner can change dividend tracker to new, that could be not audited, so some functions may work in different ways.

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

- Owner can manually call swapAndSendDividends().
- Owner can change maxSellTransactionAmount and maxBuyTransactionAmount.
- Owner can change dividend time.
- Owner can change buyback mode.
- Owner can change trading enabled timestamp.
- Owner can change minimum balance for dividends.
- Owner can change max wallet amount.
- Owner can change swapTokensAtAmount.
- Owner can change marketing, charity, buyback, markting token fee, charity token fee and buyback token fee addresses.
- Owner can change fees.
- Owner can change dividend tracker.
- Owner can change Uniswap router.
- Owner can exclude from the fees.
- Owner can exclude from dividends.
- Owner can enable dividends for address.
- Owner can exclude and include addresses in automatedMarketMakerPairs array.
- Owner can change gas for processing.
- Owner can update claimWait value.
- Owner can manually swap and liquify.
- Owner can change DividendToken address.

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://app.unicrypt.network/amm/pancake-v2/pair/0xadf718ba0c46fbb269d1ae4a7f14641a5b5e7d32

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.