Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

August, 2021

Audit Details

Audited project

Predator Token

Deployer address

0x4f09AF61a587e3d16aB6cF6389D0130dCB1b71e2

Client contacts:

Predator Token team

Blockchain

Binance Smart Chain

Project website:

http://predatortoken.org/

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 Predator Token to perform an audit of smart contracts:

https://bscscan.com/address/0xe59046e1a4a83c11ccc578e26da4eeec8484ed8d#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

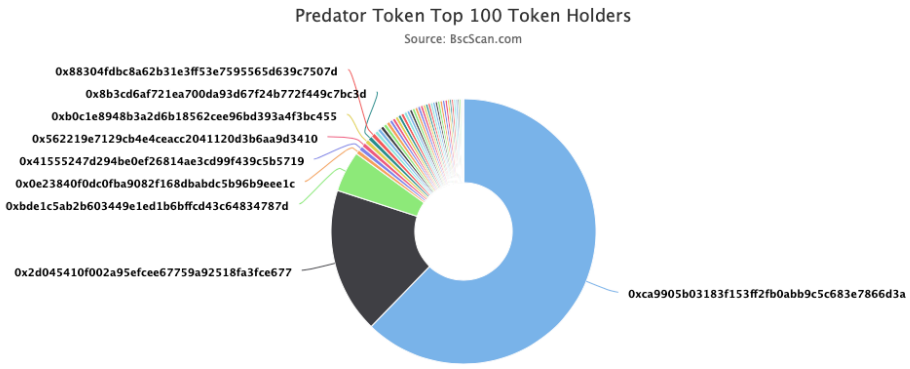
Token contract details for 10.08.2021

Contract name	Predator Token
Contract address	0xE59046E1a4A83C11ccC578e26da4eEeC8484ed8d
Total supply	1,000,000,000
Token ticker	PRED
Decimals	9
Token holders	45
Transactions count	47
Top 100 holders dominance	100.00%
Dividend token	0xe9e7cea3dedca5984780bafc599bd69add087d56
Total fees	15
Dividend rewards fee	0
Uniswap V2 pair	0xdd2f504a5b94122921c1833d6522def3853e5ee9
Contract deployer address	0x4f09AF61a587e3d16aB6cF6389D0130dCB1b71e2
Contract's current owner address	0x4f09AF61a587e3d16aB6cF6389D0130dCB1b71e2

Predator Token Token Distribution

The top 100 holders collectively own 100.00% (1,000,000,000.00 Tokens) of Predator Token

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 45

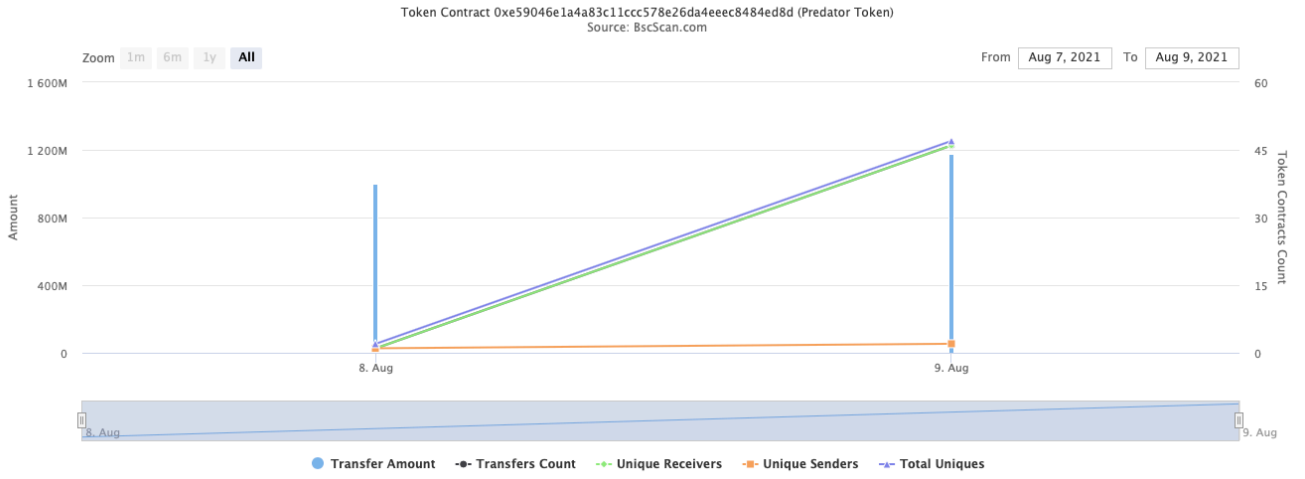


(A total of 1,000,000,000.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

Predator Token Contract Interaction Details

Time Series: Token Contract Overview

Sun 8, Aug 2021 - Mon 9, Aug 2021



Predator Token Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xca9905b03183f153ff2fb0abb9c5c683e7866d3a	622,720,000	62.2720%
2	0x2d045410f002a95efcee67759a92518fa3fce677	177,280,000	17.7280%
3	0xbde1c5ab2b603449e1ed1b6bffcd43c64834787d	50,000,000	5.0000%
4	0x0e23840f0dc0fba9082f168dbabdc5b96b9eee1c	5,500,000	0.5500%
5	0x41555247d294be0ef26814ae3cd99f439c5b5719	5,500,000	0.5500%
6	0x562219e7129cb4e4ceacc2041120d3b6aa9d3410	5,500,000	0.5500%
7	0xb0c1e8948b3a2d6b18562cee96bd393a4f3bc455	5,500,000	0.5500%
8	0x8b3cd6af721ea700da93d67f24b772f449c7bc3d	5,500,000	0.5500%
9	0x88304fdbc8a62b31e3ff53e7595565d639c7507d	5,500,000	0.5500%
10	0x19f427d14dc5e5dcd5d85718c6a69893b882da34	4,500,000	0.4500%

Contract functions details

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

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

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

+ 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 #

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

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

+ DividendPayingToken (ERC20, IDividendPayingToken, IDividendPayingTokenOptional)
  - [Pub] <Constructor> #
    - modifiers: ERC20
  - [Ext] <Fallback> ($)
  - [Pub] distributeDividends ($)
  - [Pub] distributeDividends #
  - [Pub] withdrawDividend #
  - [Pub] setDividendTokenAddress #
  - [Int] _withdrawDividendOfUser #
  - [Pub] dividendOf
  - [Pub] withdrawableDividendOf
  - [Pub] withdrawnDividendOf
  - [Pub] accumulativeDividendOf
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _setBalance #

+ [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 #

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

+ [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

+ [Lib] SafeMathInt

- [Int] mul
- [Int] div
- [Int] sub
- [Int] add
- [Int] toUint256Safe

+ [Lib] SafeMathUint
- [Int] toInt256Safe

+ PredatorToken (ERC20, Ownable)
- [Pub] <Constructor> #
  - modifiers: ERC20
- [Ext] <Fallback> ($)
- [Pub] whitelistDxSale #
  - modifiers: onlyOwner
- [Ext] setMaxBuyTransaction #
  - modifiers: onlyOwner
- [Ext] setMaxSellTransaction #
  - modifiers: onlyOwner
- [Ext] setMaxWalletToken #
  - modifiers: onlyOwner
- [Ext] setSellTransactionMultiplier #
  - modifiers: onlyOwner
- [Ext] setMarketingDivisor #
  - modifiers: onlyOwner
- [Ext] prepareForPreSale #
  - modifiers: onlyOwner
- [Ext] afterPreSale #
  - modifiers: onlyOwner
- [Pub] setTradingIsEnabled #
  - modifiers: onlyOwner
- [Pub] setBuyBackEnabled #
  - modifiers: onlyOwner
- [Pub] setBuyBackRandomEnabled #
  - modifiers: onlyOwner
- [Pub] triggerBuyBack #
  - modifiers: onlyOwner
- [Pub] updateDividendTracker #
  - modifiers: onlyOwner
- [Pub] updateDividendRewardFee #
  - modifiers: onlyOwner
- [Pub] updateMarketingFee #
  - modifiers: onlyOwner
- [Pub] updateUniswapV2Router #
  - modifiers: onlyOwner
- [Pub] excludeFromFees #
  - modifiers: onlyOwner
- [Pub] excludeMultipleAccountsFromFees #
  - modifiers: onlyOwner
- [Pub] setAutomatedMarketMakerPair #
  - modifiers: onlyOwner
- [Prv] _setAutomatedMarketMakerPair #
- [Pub] updateBuyBackWallet #
  - modifiers: onlyOwner
- [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
  - [Pub] rand
  - [Ext] getNumberOfDividendTokenHolders
  - [Pub] isBlackListed
  - [Pub] blacklistUpdate #
    - modifiers: onlyOwner
  - [Int] _transfer #
  - [Prv] swapTokensForBNB #
  - [Prv] swapBNBForTokens #
  - [Prv] swapTokensForDividendToken #
  - [Prv] swapAndSendDividends #
  - [Prv] swapAndSendDividendsInBNB #
  - [Prv] transferToBuyBackWallet #

+ PredatorTokenDividendTracker (DividendPayingToken, Ownable)
  - [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.	Low issues
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. Wrong distributeDividends

(Low issue due to dividendTracker is not verified, otherwise it will be high issue)

Issue:

- The function `distributeDividends(uint256 amount)` has public access modifier. So that, anybody can call this function with any amount and put at risk part of the contract logic.

Recommendation:

Change access modifier for this function to avoid whole access to the function.

Issue:

- Function `distributeDividends()` increases magnifiedDividendPerShare not in dividentToken proportion(In case when dividentToken not equal to BNB).

Recommendation:

Recheck logic of distributeDividends() and add correlation parameters or remove function if it is not needed.

2. Redundant access

(Low issue due to dividendTracker is not verified, otherwise it will be high issue)

Issue:

- `setDividendTokenAddress()` function has public access modifier. So that, anybody can call this function and change token address.

Recommendation:

Change access modifier for this function to avoid whole access to the function.

3. Rounding error

Issue:

- At each calculation with division, it is goes first. In Solidity we don't have floating points, but instead we get rounding errors.

Recommendation:
Do division after multiplication.

4. 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:

- Owner can change dividend tracker that could be not audited and some functions may work in different ways.

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

- Owner can change max buy and sell transaction amounts and fees.
- Owner can change max wallet token number.
- Owner can change sellFeeIncreaseFactor.
- Owner can change marketingDivisor.
- Owner can enable before and after presale modes.
- Owner can enable and disable trading.
- Owner can enable and disable buyBack.
- Owner can enable and disable random buyback.
- Owner can manually do buyback.
- Owner can change dividendTracker.
- Owner can change dividend rewards and marketing fees.
- Owner can change Uniswap router.
- Owner can exclude from the fee.
- Owner can exclude and include addresses in automatedMarketMakerPairs array.
- Owner can change buyback wallet address.
- Owner can change gas for processing.
- Owner can update claimWait value.
- Owner can blacklist addresses.

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 NOT provided by the team.

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.