Smart Contract Security Audit

Audit details:

Audited project:	StopElon
Deployer address:	0x978422D976aEa73140782bA8b3bdC83C288f195F
Client contacts:	StopElon team
Blockchain:	Binance Smart Chain
Project website:	https://t.co/mHTkqmDoSr?amp=1

May, 2021
TechRate

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 StopElon to perform an audit of smart contracts:

- *https://bscscan.com/address/0xd83cec69ed9d8044597a793445c86a5e763b0e3d#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

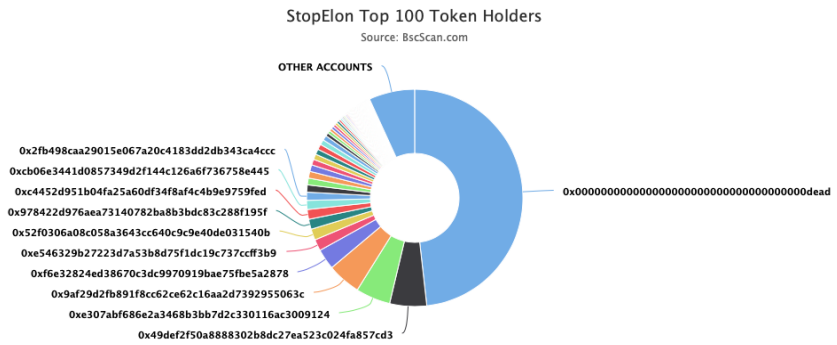
Token contract details for 24.05.2021.

Contract name:	StopElon
Contract address:	0xD83cec69ED9d8044597A793445C86a5e763b0E3D
Total supply:	1000000000000
Token ticker:	STOPELON
Decimals:	9
Token holders:	18,913
Transactions count:	46,168
Top 100 holders dominance:	93.16%
Liquidity fee:	80
Tax fee:	20
Total fees:	10361002172754263335815319292387670715063345790035225094996948268064421374 7
Uniswap V2 pair:	0x2fb498caa29015e067a20c4183dd2db343ca4ccc
Contract deployer address:	0x978422D976aEa73140782bA8b3bdC83C288f195F
Contract’s current owner address:	0x978422d976aea73140782ba8b3bdc83c288f195f

StopElon token distribution

The top 100 holders collectively own 93.16% (931,579,648,483.64 Tokens) of StopElon

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 18,913

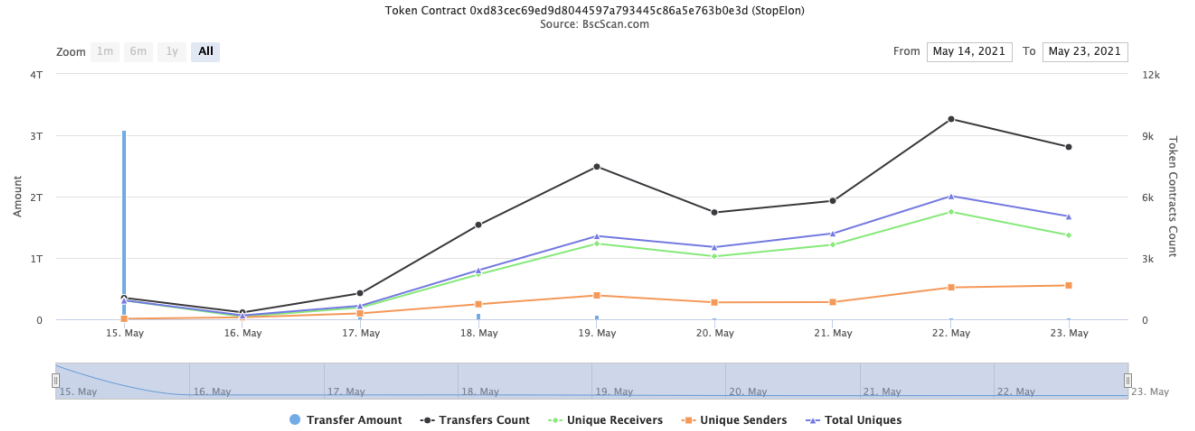


(A total of 931,579,648,483.64 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

StopElon contract interaction details

Time Series: Token Contract Overview

Sat 15, May 2021 - Sun 23, May 2021



StopElon top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	0x000000000000000000000000000000000000dead	482,145,516,347.473883689	48.2146%
2	0x49def2f50a8888302b8dc27ea523c024fa857cd3	55,241,731,218.174026793	5.5242%
3	0xe307abf686e2a3468b3bb7d2c330116ac3009124	51,796,912,910.913724451	5.1797%
4	0x9af29d2fb891f8cc62ce62c16aa2d7392955063c	50,000,000,000	5.0000%
5	0xf6e32824ed38670c3dc9970919bae75fbe5a2878	30,655,338,012.39570107	3.0655%
6	0xe546329b27223d7a53b8d75f1dc19c737ccff3b9	16,977,112,309.275749881	1.6977%
7	0x52f0306a08c058a3643cc640c9c9e40de031540b	16,602,858,838.618008807	1.6603%
8	0x978422d976aea73140782ba8b3bdc83c288f195f	15,001,228,468.880988727	1.5001%
9	0xc4452d951b04fa25a60df34f8af4c4b9e9759fed	14,425,813,077.0776	1.4426%
10	0xcb06e3441d0857349d2f144c126a6f736758e445	13,525,433,844.5285	1.3525%

StopElon LP token holders

Rank	Address	Quantity	Percentage
1	0xeb3a9c56d963b971d320f889be2fb8b59853e449	183.964485463415279	94.2283%
2	0x978422d976aea73140782ba8b3bdc83c288f195f	10.0679723011012999	5.1569%
3	0xdde05da1122494c9af1694b377adbb43b47582c9	0.478393597641282798	0.2450%
4	0xaa7f2b2f55dd2073f7831b4fe55d24f1c4b4e4d0	0.387945629478503177	0.1987%
5	0x29e506843ea98e9eda59dae6dfe4ba9137d4c399	0.091471583517306763	0.0469%
6	0x0bb61e3f69b77d055daba50840308da43c08a7fe	0.058251934024227135	0.0298%
7	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	0.055336676748439087	0.0283%
8	0xea36c8276712ecc5244da708e3729d260b744ec9	0.053753786627902732	0.0275%
9	0xa563f559e98311e296803269953acf22b4470ec7	0.018224099704143669	0.0093%
10	0xd786297f83de0ac5c6c6aed4bd6600f58b7749b1	0.015975561249281061	0.0082%

Contract functions details

+ [Int] IERC20
  - [Ext] totalSupply
  - [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

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

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #

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

+ [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 #

+ StopElon (Context, IERC20, Ownable)
- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] isExcludedFromReward
- [Pub] totalFees
- [Pub] updateRouterAndPair #
  - modifiers: onlyOwner
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Pub] excludeFromReward #
  - modifiers: onlyOwner
- [Ext] includeInReward #
  - modifiers: onlyOwner
- [Prv] _transferBothExcluded #
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #

    - modifiers: onlyOwner
  - [Ext] setTaxFeePercent #
    - modifiers: onlyOwner
  - [Ext] setLiquidityFeePercent #
    - modifiers: onlyOwner
  - [Ext] setMaxTxPercent #
    - modifiers: onlyOwner
  - [Pub] setSwapAndLiquifyEnabled #
    - modifiers: onlyOwner
  - [Ext] <Fallback> ($)
  - [Prv] _reflectFee #
  - [Prv] _getValues
  - [Prv] _getTValues
  - [Prv] _getRValues
  - [Prv] _getRate
  - [Prv] _getCurrentSupply
  - [Prv] _takeLiquidity #
  - [Prv] calculateTaxFee
  - [Prv] calculateLiquidityFee
  - [Prv] removeAllFee #
  - [Prv] restoreAllFee #
  - [Pub] isExcludedFromFee
  - [Prv] _approve #
  - [Prv] _transfer #
  - [Prv] swapAndLiquify #
    - modifiers: lockTheSwap
  - [Prv] swapTokensForEth #
  - [Prv] addLiquidity #
  - [Prv] _tokenTransfer #
  - [Prv] _transferStandard #
  - [Prv] _transferToExcluded #
  - [Prv] _transferFromExcluded #
  - [Pub] safeTransferETH #
    - modifiers: onlyOwner
  - [Pub] safeTransfer #
    - 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. Wrong _tFeeTotal display

Issue:

_tFeeTotal value will be wrongly updated in function includeInReward because there is adding the wrong value to it without division by the rate. So because of that now _tFeeTotal value is very big.

```
uint256 newrOwned = _tOwned[account⬆].mul(_getRate());
_rTotal = _rTotal.sub(_rOwned[account⬆]-newrOwned);
_tFeeTotal = _tFeeTotal.add(_rOwned[account⬆]-newrOwned);
_rOwned[account⬆] = newrOwned;
```

Recommendation:

Please check the logic of this function and fix the issue.

2. Out of gas

Issue:

- The function includeInReward() uses the loop to find and remove addresses from the _excluded list. Function will be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.

```
function includeInReward(address account⬆) external onlyOwner() {
    require(_isExcluded[account⬆], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account⬆) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account⬆] = 0;
            _isExcluded[account⬆] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- The function `_getCurrentSupply` also uses the loop for evaluating total supply. It also could be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
        ) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Use EnumerableSet instead of array or do not use long arrays.

Conclusion

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

Lp locking details provided by the team can be found by this links -
https://dxsale.app/app/pages/dxlockview?id=1&add=0x978422D976aEa73140782bA8b3bdC83C288f195F&type=lplock&chain=BSC
https://dxsale.app/app/pages/dxlockview?id=2&add=0x978422D976aEa73140782bA8b3bdC83C288f195F&type=lplock&chain=BSC
https://dxsale.app/app/pages/dxlockview?id=3&add=0x978422D976aEa73140782bA8b3bdC83C288f195F&type=lplock&chain=BSC
https://dxsale.app/app/pages/dxlockview?id=4&add=0x978422D976aEa73140782bA8b3bdC83C288f195F&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.