Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

August, 2021

Audit Details

Audited project

1OF1

Deployer address

0x9e39A5Ebc53388378134b06A978ff91316D2f8a5

Client contacts:

1OF1 team

Blockchain

Binance Smart Chain

Project website:

1of1token.finance

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 1OF1 to perform an audit of smart contracts:

https://bscscan.com/address/0xdcf8ad3a93269207eb0b0d7c9eb048f2dd512113#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

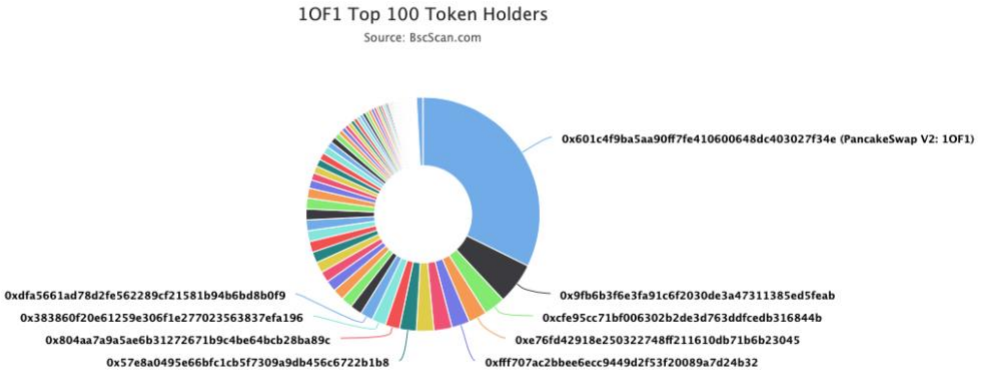
Token contract details for 04.08.2021

Contract name	1OF1
Contract address	0xdcF8aD3A93269207Eb0b0d7C9eB048F2dd512113
Total supply	1
Token ticker	1OF1
Decimals	10
Token holders	5,061
Transactions count	8,436
Top 100 holders dominance	99.10%
Cooldown interval	1
Autoliquidity fee receiver	0x9fb6b3f6e3fa91c6f2030de3a47311385ed5feab
Marketing fee receiver	0x9fb6b3f6e3fa91c6f2030de3a47311385ed5feab
Pair	0x601c4f9ba5aa90ff7fe410600648dc403027f34e
Contract deployer address	0x9e39A5Ebc53388378134b06A978ff91316D2f8a5
Contract's current owner address	0x9fb6b3f6e3fa91c6f2030de3a47311385ed5feab

1OF1 Token Distribution

The top 100 holders collectively own 99.10% (0.99 Tokens) of 1OF1

Token Total Supply: 1.00 Token | Total Token Holders: 5,061

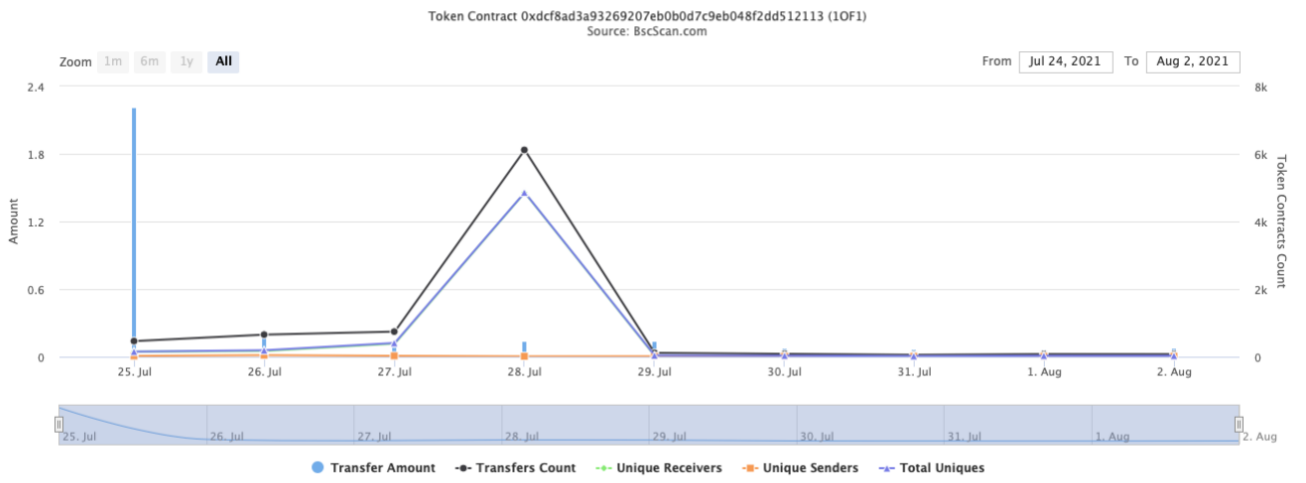


(A total of 0.99 tokens held by the top 100 accounts from the total supply of 1.00 token)

1OF1 Contract Interaction Details

Time Series: Token Contract Overview

Sun 25, Jul 2021 - Mon 2, Aug 2021



1OF1 Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap V2: 1OF1	0.322924399	32.2924%
2	0x9fb6b3f6e3fa91c6f2030de3a47311385ed5feab	0.0572665226	5.7267%
3	0xcfe95cc71bf006302b2de3d763ddfcedb316844b	0.0297449533	2.9745%
4	0xe76fd42918e250322748ff211610db71b6b23045	0.025090353	2.5090%
5	0xfff707ac2bbee6ecc9449d2f53f20089a7d24b32	0.0250285408	2.5029%
6	0x4f44d8170bc89bde856c74768c1bf542a5390e38	0.0250276537	2.5028%
7	0x46b05fff861f0e163eb8149235b462ebe3deafba	0.0242246352	2.4225%
8	0x57e8a0495e66bfc1cb5f7309a9db456c6722b1b8	0.0230633785	2.3063%
9	0x804aa7a9a5ae6b31272671b9c4be64bcb28ba89c	0.0200000017	2.0000%
10	0x383860f20e61259e306f1e277023563837efa196	0.0194114748	1.9411%

Contract functions details

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

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ Auth
  - [Pub] <Constructor> #
  - [Pub] authorize #
    - modifiers: onlyOwner
  - [Pub] unauthorize #
    - modifiers: onlyOwner
  - [Pub] isOwner
  - [Pub] isAuthorized
  - [Pub] transferOwnership #
    - modifiers: onlyOwner

+ [Int] IDEXFactory
  - [Ext] createPair #

+ [Int] IDEXRouter
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] IDividendDistributor
  - [Ext] setDistributionCriteria #
  - [Ext] setShare #
  - [Ext] deposit ($)
  - [Ext] process #

+ DividendDistributor (IDividendDistributor)
  - [Pub] <Constructor> #

- [Ext] setDistributionCriteria #
  - modifiers: onlyToken
- [Ext] setShare #
  - modifiers: onlyToken
- [Ext] deposit ($)
  - modifiers: onlyToken
- [Ext] process #
  - modifiers: onlyToken
- [Int] shouldDistribute
- [Int] distributeDividend #
- [Ext] claimDividend #
- [Pub] getUnpaidEarnings
- [Int] getCumulativeDividends
- [Int] addShareholder #
- [Int] removeShareholder #

+ ONEOFONE (IBEP20, Auth)
  - [Pub] <Constructor> #
    - modifiers: Auth
  - [Ext] <Fallback> ($)
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Pub] balanceOf
  - [Ext] allowance
  - [Pub] approve #
  - [Ext] approveMax #
  - [Ext] transfer #
  - [Ext] transferFrom #
  - [Ext] setMaxWalletPercent #
    - modifiers: onlyOwner
  - [Int] _transferFrom #
  - [Int] _basicTransfer #
  - [Int] checkTxLimit
  - [Int] shouldTakeFee
  - [Int] takeFee #
  - [Int] shouldSwapBack
  - [Ext] clearStuckBalance #
    - modifiers: onlyOwner
  - [Pub] tradingStatus #
    - modifiers: onlyOwner
  - [Pub] cooldownEnabled #
    - modifiers: onlyOwner
  - [Int] swapBack #
    - modifiers: swapping
  - [Ext] setTxLimit #
    - modifiers: authorized
  - [Ext] setIsDividendExempt #
    - modifiers: authorized
  - [Ext] setIsFeeExempt #
    - modifiers: authorized
  - [Ext] setIsTxLimitExempt #
    - modifiers: authorized

- [Ext] setIsTimelockExempt #
  - modifiers: authorized
- [Ext] setFees #
  - modifiers: authorized
- [Ext] setFeeReceivers #
  - modifiers: authorized
- [Ext] setSwapBackSettings #
  - modifiers: authorized
- [Ext] setTargetLiquidity #
  - modifiers: authorized
- [Ext] setDistributionCriteria #
  - modifiers: authorized
- [Ext] setDistributorSettings #
  - modifiers: authorized
- [Pub] getCirculatingSupply
- [Pub] getLiquidityBacking
- [Pub] isOverLiquified
- [Ext] makeItRain #
  - 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 makeItRain() uses the loop to airdrop rewards by the list. Function will be aborted with OUT_OF_GAS exception if there will be a long receivers list.

```
ftrace | funcSig
function makeItRain(address from⬆, address[] calldata addresses⬆, uint256[] calldata tokens⬆) external onlyOwner {

    uint256 ShowerCapacity = 0;

    require(addresses⬆.length == tokens⬆.length,"Mismatch between Address and token count");

    for(uint i=0; i < addresses⬆.length; i++){
        ShowerCapacity = ShowerCapacity + tokens⬆[i];
    }

    require(balanceOf(from⬆) >= ShowerCapacity, "Not enough tokens to airdrop");

    for(uint i=0; i < addresses⬆.length; i++){
        _basicTransfer(from⬆,addresses⬆[i],tokens⬆[i]);
        if(!isDividendExempt[addresses⬆[i]]) {
            try distributor.setShare(addresses⬆[i], _balances[addresses⬆[i]]) {} catch {}
        }
    }

    // Dividend tracker
    if(!isDividendExempt[from⬆]) {
        try distributor.setShare(from⬆, _balances[from⬆]) {} catch {}
    }
}

    event AutoLiquify(uint256 amountBNB, uint256 amountBOG);

}
```

Recommendation:

Check that the array length is not too big.

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

- Owner can change the maximum transaction amount.
- Owner can include in and exclude from dividends.
- Owner can include in and exclude from fee and transaction amount.
- Owner can change fees.
- Owner can change max wallet percent.
- Owner can change fee receivers.
- Owner can change swap threshold and disable/enable swap.
- Owner can change target liquidity values.
- Owner can change distribution criteria.
- Owner can change distribution GAS.
- Owner can withdraw BNBs to the marketing receiver address.
- Owner can change trading status.
- Owner can change cooldown status.
- Owner can change buybackKeepItSimple value.
- Owner can change addresses' isTimelockExempt value.

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=0x9e39A5Ebc53388378134b06A978ff91316D2f8a5&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.