TechRate

Blockchain solutions and consulting

Smart Contract Security Audit

Audit details:

Audited project:	WindSwap
Deployer address	0x4103999ae80b771a6229783d55a9e8d334c66747
Client contacts:	WindSwap team
Blockchain:	Binance Smart Chain
Project website:	https://windswap.finance

April, 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 WindSwap to perform an audit of smart contracts:

- *https://bscscan.com/address/0xd1587ee50e0333f0c4adcf261379a61b1486c5d2#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.

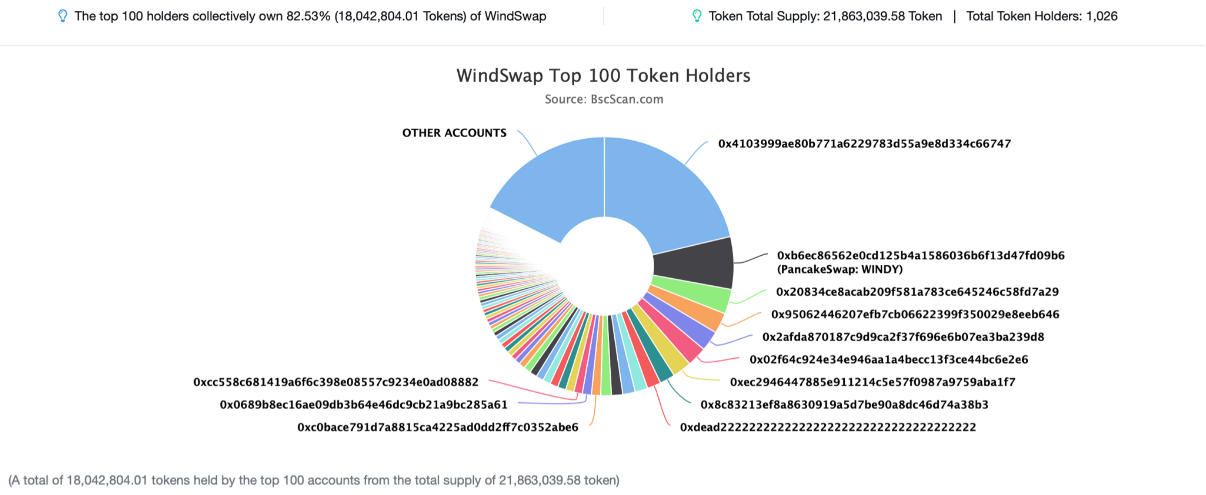
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts details

Token contract details for 10.04.2021.

Contract name:	WindSwap
Compiler version:	v0.6.9+commit.3e3065ac
Contract address:	0xd1587ee50e0333f0c4adcf261379a61b1486c5d2
Total supply:	2_186_303_957_714_251
Token ticker:	WINDY
Decimals:	8
Token holders:	1026
Transactions count:	4423
Top 100 holders dominance:	82.53 %
Contract deployer address:	0x4103999ae80b771a6229783d55a9e8d334c66747
Contract’s current owner address:	0x4103999ae80b771a6229783d55a9e8d334c66747
Burn levy:	650
Burn rotations:	9_946_042_285_749
Rotations:	36
Traded rotations:	227_492_301_399_722
Total burn:	414_946_042_285_749
Total levies:	0

WindSwap top 100 token distribution



The top 100 holders collectively own 82.53% (18,042,804.01 Tokens) of WindSwap

Token Total Supply: 21,863,039.58 Token | Total Token Holders: 1,026

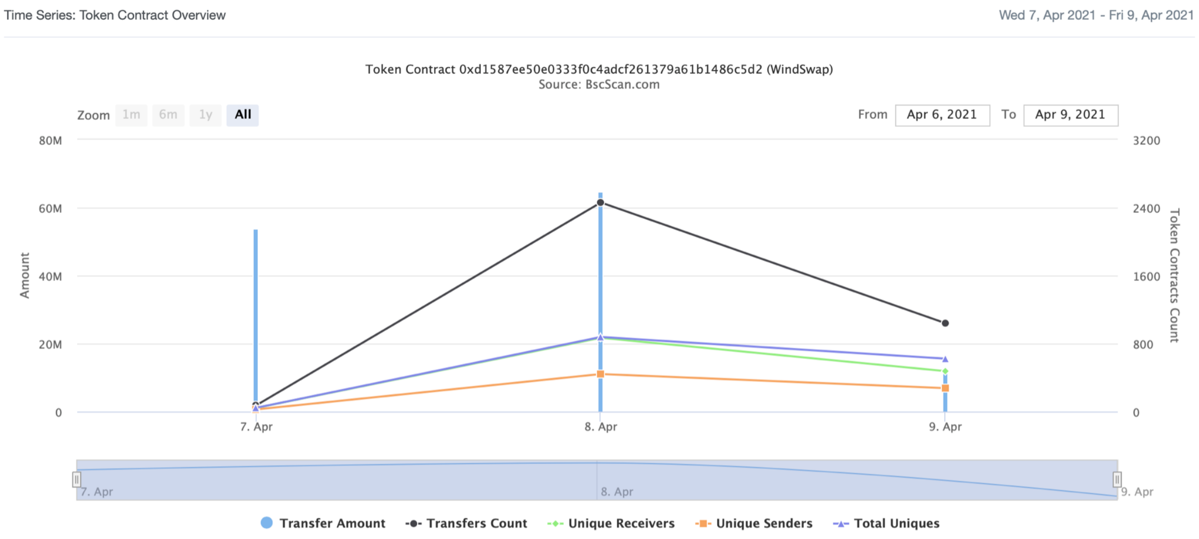
WindSwap Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0x4103999ae80b771a6229783d55a9e8d334c66747
0xb6ec86562e0cd125b4a1586036b6f13d47fd09b6 (PancakeSwap: WINDY)
0x20834ce8acab209f581a783ce645246c58fd7a29
0x95062446207efb7cb06622399f350029e8eeb646
0x2afda870187c9d9ca2f37f696e6b07ea3ba239d8
0x02f64c924e34e946aa1a4becc13f3ce44bc6e2e6
0xec2946447885e911214c5e57f0987a9759aba1f7
0x8c83213ef8a8630919a5d7be90a8dc46d74a38b3
0xdead222222222222222222222222222222222222
0xcc558c681419a6f6c398e08557c9234e0ad08882
0x0689b8ec16ae09db3b64e46dc9cb21a9bc285a61
0xc0bace791d7a8815ca4225ad0dd2ff7c0352abe6

(A total of 18,042,804.01 tokens held by the top 100 accounts from the total supply of 21,863,039.58 token)

WindSwap contract interaction details



Time Series: Token Contract Overview

Wed 7, Apr 2021 - Fri 9, Apr 2021

Token Contract 0xd1587ee50e0333f0c4adcf261379a61b1486c5d2 (WindSwap)

Source: BscScan.com

Zoom 1m 6m 1y All

From Apr 6, 2021 To Apr 9, 2021

Contract functions details

Function	Return value	Who can call
name()	string	public
symbol()	string	public
decimals()	uint8	public
totalSupply()	uint256	public
balanceOf(address)	uint256	public
transfer(address, uint256)	bool	public
allowance(address, address)	uint256	public
approve(address, uint256)	bool	public
transferfrom(address, address, uint256)	bool	public
increaseAllowance(address, uint256)	bool	public
decreaseAllowance(address, uint256)	bool	public
totalLevies()	uint256	public
deliver()	void	public
reflectionFromToken(unit256, bool)	uint256	public
tokenFromReflection(unit256)	uint256	public
excludeAccount(address)	void	owner
includeAccount(address)	void	owner
isExcluded(address)	bool	public
setLevy(uint256)	void	owner
totalBurn()	uint256	public
_getBurnLevy()	uint256	public
_getRotations()	uint256	public
_getBurnRotations()	uint256	public
_getTradedRotations()	uint256	public

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 severity issues only
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

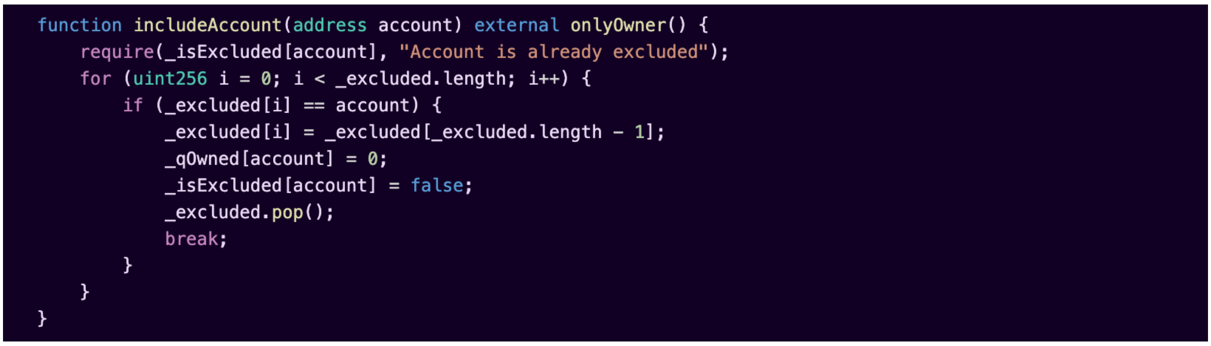
No medium severity issues found.

Low Severity Issues

1. Out of gas

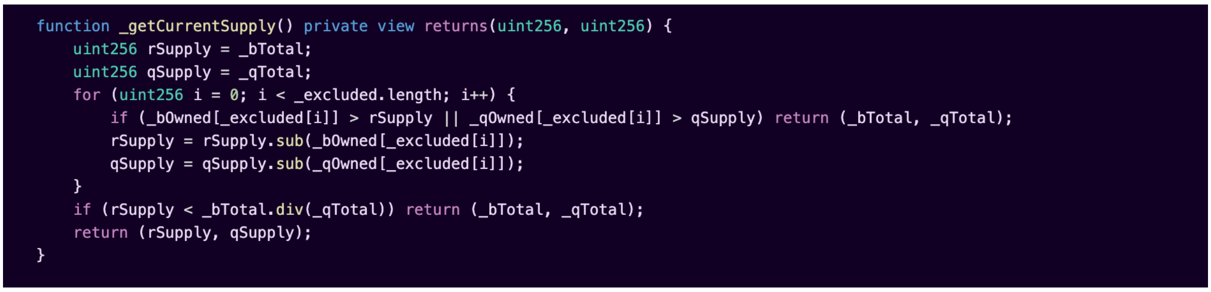
Issue:

- The function includeAccount() 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 includeAccount(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];
            _qOwned[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 = _bTotal;
    uint256 qSupply = _qTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_bOwned[_excluded[i]] > rSupply || _qOwned[_excluded[i]] > qSupply) return (_bTotal, _qTotal);
        rSupply = rSupply.sub(_bOwned[_excluded[i]]);
        qSupply = qSupply.sub(_qOwned[_excluded[i]]);
    }
    if (rSupply < _bTotal.div(_qTotal)) return (_bTotal, _qTotal);
    return (rSupply, qSupply);
}
```

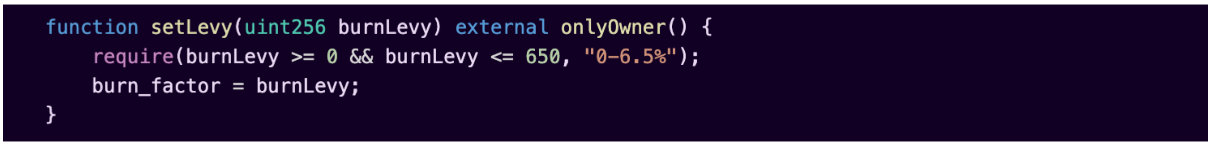
Recommendation:

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

Owner privileges

1. Owner privileges

❑ Owner can change the levy in range 0 - 6.5%.



```
function setLevy(uint256 burnLevy) external onlyOwner() {
    require(burnLevy >= 0 && burnLevy <= 650, "0-6.5%");
    burn_factor = burnLevy;
}
```

Conclusion

Smart contracts do not contain any high severity issues!

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.