Smart Contract Security Audit

Audit details:

Audited project:	LionSwap
Deployer address	0x432c2f8b51941cf87ee2ab33d822a0c129a5d6c1
Blockchain:	Binance Smart Chain
Project website:	https://lionswapdefi.com

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 LionSwap to perform an audit of smart contracts:

- *https://bscscan.com/address/0x4DCe9d77F628A4c3e2CD60E832cEa34ec3a8AcC1#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

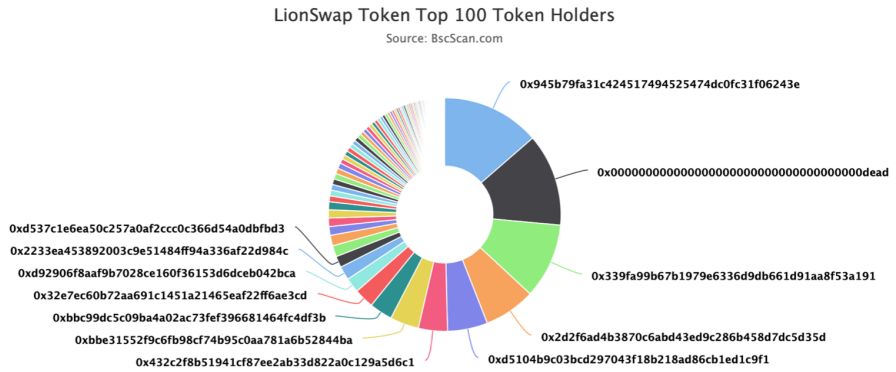
Token contract details for 21.05.2021.

Contract name:	LionSwap
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0x4DCe9d77F628A4c3e2CD60E832cEa34ec3a8AcC1
Total supply:	250
Token ticker:	LION
Decimals:	18
Token holders:	115
Transactions count:	2949
Top 100 holders dominance:	99.94 %
Contract deployer address:	0x432c2f8b51941cf87ee2ab33d822a0c129a5d6c1
Contract’s current owner address:	0x339fa99b67b1979e6336d9db661d91aa8f53a191

LionSwap top 100 token distribution

The top 100 holders collectively own 99.94% (249.84 Tokens) of LionSwap Token

Token Total Supply: 250.00 Token | Total Token Holders: 115



(A total of 249.84 tokens held by the top 100 accounts from the total supply of 250.00 token)

LionSwap top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	0x945b79fa31c424517494525474dc0fc31f06243e	34.147364726603451982	13.6589%
2	0x000000000000000000000000000000000000dead	32.031860949899805991	12.8127%
3	0x339fa99b67b1979e6336d9db661d91aa8f53a191	26.049423418935500962	10.4198%
4	0x2d2f6ad4b3870c6abd43ed9c286b458d7dc5d35d	17.847953178718071134	7.1392%
5	0xd5104b9c03bcd297043f18b218ad86cb1ed1c9f1	13.93930979026125065	5.5757%
6	0x432c2f8b51941cf87ee2ab33d822a0c129a5d6c1	10.122008222323095882	4.0488%
7	0xbbe31552f9c6fb98cf74b95c0aa781a6b52844ba	10.000007835826772598	4.0000%
8	0xbbc99dc5c09ba4a02ac73fef396681464fc4df3b	8.012108572368922427	3.2048%
9	0x32e7ec60b72aa691c1451a21465eaf22ff6ae3cd	6.865509658580091816	2.7462%
10	0xd92906f8aaf9b7028ce160f36153d6dceb042bca	5.126573139231870957	2.0506%

Functions outline

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

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Int] functionStaticCall
  - [Int] functionStaticCall
  - [Int] functionDelegateCall #
  - [Int] functionDelegateCall #
  - [Prv] _verifyCallResult

+ [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

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

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol

- [Ext] name
- [Ext] getOwner
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ BEP20 (Context, IBEP20, Ownable)
- [Pub] <Constructor> #
- [Ext] getOwner
- [Pub] name
- [Pub] decimals
- [Pub] symbol
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] mint #
  - modifiers: onlyOwner
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _approve #
- [Int] _burnFrom #

+ LionToken (BEP20)
- [Pub] mint #
  - modifiers: onlyOwner
- [Int] _transfer #
- [Ext] delegates
- [Ext] delegate #
- [Ext] delegateBySig #
- [Ext] getCurrentVotes
- [Ext] getPriorVotes
- [Int] _delegate #
- [Int] _moveDelegates #
- [Int] _writeCheckpoint #
- [Int] safe32
- [Int] getChainId

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.	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.	Medium 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

1. Wrong burning

Issue:

There is sending tokens to the dead address in overridden _transfer functions, instead of burning them in token contract.

```
function _transfer(address sender⬆, address recipient⬆, uint256 amount⬆) internal virtual override {
    if (recipient⬆ == BURN_ADDRESS) {
        super._transfer(sender⬆, recipient⬆, amount⬆);
    } else {
        // 2% of every transfer burnt
        uint256 burnAmount = amount⬆.mul(2).div(100);
        // 98% of transfer sent to recipient
        uint256 sendAmount = amount⬆.sub(burnAmount);
        require(amount⬆ == sendAmount + burnAmount, "LION::transfer: Burn value invalid");

        super._transfer(sender⬆, BURN_ADDRESS, burnAmount);
        super._transfer(sender⬆, recipient⬆, sendAmount);
        amount⬆ = sendAmount;
    }
}
```

Recommendation:

There should be a burn instead of sending to the dead address.

Low Severity Issues

No low severity issues found.

Owner privileges

- ❑ Owner can mint tokens before sending ownership to the masterchef.

Conclusion

Smart contracts contain medium 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.