Smart Contract Security Audit

TechRate

Audit Company

TechRate
June, 2021
Audit Details

Audited project
JEDSTAR

Deployer address
0xbd9698432b0389e6c62c537bdb766c22f8ebf0ee

Client contacts:
JEDSTAR team

Blockchain
Binance Smart Chain

Project website:
Not provided by JEDSTAR team
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 JEDSTAR to perform an audit of smart contracts: https://bscscan.com/address/0x058a7af19bdb63411d0a84e79e3312610d7fa90c#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 30.08.2021

<table>
<thead>
<tr>
<th><strong>Contract name</strong></th>
<th>JEDSTAR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Contract address</strong></td>
<td>0x058a7Af19BdB63411d0a84e79E3312610D7fa90c</td>
</tr>
<tr>
<td><strong>Total supply</strong></td>
<td>100,000,000</td>
</tr>
<tr>
<td><strong>Token ticker</strong></td>
<td>JED</td>
</tr>
<tr>
<td><strong>Decimals</strong></td>
<td>9</td>
</tr>
<tr>
<td><strong>Token holders</strong></td>
<td>594</td>
</tr>
<tr>
<td><strong>Transactions count</strong></td>
<td>2,240</td>
</tr>
<tr>
<td><strong>Top 100 holders dominance</strong></td>
<td>94.65%</td>
</tr>
<tr>
<td><strong>Liquidity fee</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Tax fee</strong></td>
<td>6</td>
</tr>
<tr>
<td><strong>Total fees</strong></td>
<td>3776203004968381</td>
</tr>
<tr>
<td><strong>Uniswap V2 pair</strong></td>
<td>0x7d72540f81034a847d821ec34c389c744b14ff57</td>
</tr>
<tr>
<td><strong>Contract deployer address</strong></td>
<td>0xbd9698432b0389e6c62c537bdb766c22f8ebf0ee</td>
</tr>
<tr>
<td><strong>Contract’s current owner address</strong></td>
<td>0xbd9698432b0389e6c62c537bdb766c22f8ebf0ee</td>
</tr>
</tbody>
</table>
JEDSTAR Token Distribution

The top 100 holders collectively own 94.65% (94,654,712.35 Tokens) of JEDSTAR.

Token Supply: 100,000,000.00 Token | Total Token Holders: 594

(A total of 94,654,712.35 tokens held by the top 100 accounts from the total supply of 100,000,000.00 token)

JEDSTAR Contract Interaction Details

Time Series: Token Contract Overview

Token Contract: 0x00f8af7e988b63411d8a8a4e79e331261de7f510c (JEDSTAR)

Source: BscScan.com

From: Aug 23, 2021 | To: Aug 29, 2021
# JEDSTAR Top 10 Token Holders

<table>
<thead>
<tr>
<th>Rank</th>
<th>Address</th>
<th>Quantity (Token)</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bum Address</td>
<td>45,000,000</td>
<td>45.0000%</td>
</tr>
<tr>
<td>2</td>
<td>0x7bb31ae132b0b12d29cd829f0ed88ee751b1bed9f3</td>
<td>21,866,672.395993265</td>
<td>21.8867%</td>
</tr>
<tr>
<td>3</td>
<td>0x221156e5a25408b3b21c9d20668888e3653a6dcd081</td>
<td>1,920,087.817410754</td>
<td>1.9201%</td>
</tr>
<tr>
<td>4</td>
<td>PancakeSwap V2: JED</td>
<td>1,889,799.352662532</td>
<td>1.8898%</td>
</tr>
<tr>
<td>5</td>
<td>0xe8f19c3a8e0a46957b522551628e956e52187753</td>
<td>1,253,067.8722807</td>
<td>1.3531%</td>
</tr>
<tr>
<td>6</td>
<td>0xc07d3a6c33430a1036b21f9a4b68051316763be</td>
<td>1,343,088.427347469</td>
<td>1.3431%</td>
</tr>
<tr>
<td>7</td>
<td>0x274e719825da0684a3144d502f5696e615090b32</td>
<td>1,187,407.770428669</td>
<td>1.1874%</td>
</tr>
<tr>
<td>8</td>
<td>0x9e8a2b32f2137b615058284d8f0a4103011ae</td>
<td>1,170,411.220107598</td>
<td>1.1701%</td>
</tr>
<tr>
<td>9</td>
<td>0x37b3d8fb4b53569ed8539fa903e95b483f359f</td>
<td>1,151,594.696567773</td>
<td>1.1516%</td>
</tr>
<tr>
<td>10</td>
<td>0x4e81a06b26d46b8876de78a03a8c95973bf6050c</td>
<td>1,123,862.581297266</td>
<td>1.1239%</td>
</tr>
</tbody>
</table>
Contract functions details

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

+ [Lib] SafeMath
  - [Int] tryAdd
  - [Int] trySub
  - [Int] tryMul
  - [Int] tryDiv
  - [Int] tryMod
  - [Int] add
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] mod

+ 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

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

+ [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] DOMIAN_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 #
+ JedStarToken (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] 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] setBurnFeePercent #
    - modifiers: onlyOwner
  - [Ext] setLiquidityFeePercent #
    - modifiers: onlyOwner
  - [Pub] recoverBEP20 #
    - modifiers: onlyOwner
  - [Pub] eDraw ($) #
    - modifiers: onlyOwner
  - [Ext] setMaxTxPercent #
    - modifiers: onlyOwner
  - [Pub] setSwapAndLiquifyEnabled #
    - modifiers: onlyOwner
  - [Ext] <Fallback> ($) #
    - modifiers: onlyOwner
  - [Prv] _reflectFee #
  - [Prv] _getValues
  - [Prv] _getTValues
  - [Prv] _getRValues
  - [Prv] _getRate
  - [Prv] _getCurrentSupply
  - [Prv] _takeLiquidity #
  - [Prv] _takeCharity #
  - [Prv] calculateTaxFee
  - [Prv] calculateCharityFee
  - [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 #

($) = payable function

# = non-constant function
<table>
<thead>
<tr>
<th>Issue description</th>
<th>Checking status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Compiler errors.</td>
<td>Passed</td>
</tr>
<tr>
<td>2. Race conditions and Reentrancy. Cross-function race</td>
<td>Passed</td>
</tr>
<tr>
<td>conditions.</td>
<td></td>
</tr>
<tr>
<td>3. Possible delays in data delivery.</td>
<td>Passed</td>
</tr>
<tr>
<td>4. Oracle calls.</td>
<td>Passed</td>
</tr>
<tr>
<td>5. Front running.</td>
<td>Passed</td>
</tr>
<tr>
<td>6. Timestamp dependence.</td>
<td>Passed</td>
</tr>
<tr>
<td>7. Integer Overflow and Underflow.</td>
<td>Passed</td>
</tr>
<tr>
<td>8. DoS with Revert.</td>
<td>Low issues</td>
</tr>
<tr>
<td>9. DoS with block gas limit.</td>
<td>Passed</td>
</tr>
<tr>
<td>10. Methods execution permissions.</td>
<td>Passed</td>
</tr>
<tr>
<td>11. Economy model of the contract.</td>
<td>Passed</td>
</tr>
<tr>
<td>12. The impact of the exchange rate on the logic.</td>
<td>Passed</td>
</tr>
<tr>
<td>13. Private user data leaks.</td>
<td>Passed</td>
</tr>
<tr>
<td>14. Malicious Event log.</td>
<td>Passed</td>
</tr>
<tr>
<td>15. Scoping and Declarations.</td>
<td>Passed</td>
</tr>
<tr>
<td>16. Uninitialized storage pointers.</td>
<td>Passed</td>
</tr>
<tr>
<td>17. Arithmetic accuracy.</td>
<td>Passed</td>
</tr>
<tr>
<td>18. Design Logic.</td>
<td>Passed</td>
</tr>
<tr>
<td>19. Cross-function race conditions.</td>
<td>Passed</td>
</tr>
<tr>
<td>20. Safe Open Zeppelin contracts implementation and usage.</td>
<td>Passed</td>
</tr>
<tr>
<td>21. Fallback function security.</td>
<td>Passed</td>
</tr>
</tbody>
</table>
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 `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.

   ```solidity
   function includeInReward(address account) external onlyOwner() {
     require(!isExcluded[account], "Account is already included");
     for (uint256 i = 0; i < _excluded.length; i++) {
       if (_excluded[i] == account) {
         _excluded[i] = _excluded[_excluded.length - 1];
         _owned[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.

   ```solidity
   function _getCurrentSupply() private view returns (uint256, uint256) {
     uint256 rSupply = tTotal;
     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:
   Check that the excluded array length is not too big.
Notes:

- There is sending tokens to the dead address instead of decreasing total supply.

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

- Owner can change the tax, charity(burn) and liquidity fee.

```solidity
function setTaxFeePercent(uint256 taxFee%) external onlyOwner() {
    require(taxFee% <= 10, "Fee must be less than 10%");  
    _taxFee = taxFee%;
}
```

```solidity
function setBurnFeePercent(uint256 charityFee%) external onlyOwner() {
    require(charityFee% <= 4, "Fee must be less than 4%");  
    _charityFee = charityFee%;
}
```

```solidity
function setLiquidityFeePercent(uint256 liquidityFee%) external onlyOwner() {
    require(liquidityFee% <= 4, "Fee must be less than 4%");  
    _liquidityFee = liquidityFee%;
}
```

- Owner can change the maximum transaction amount.

```solidity
function setMaxTxPercent(uint256 maxTxPercent%) external onlyOwner() {
    _maxTxAmount = _total.mul(maxTxPercent%).div(10**3);
}
```

- Owner can exclude from the fee.

```solidity
function excludeFromFee(address account) public onlyOwner {
    isExcludedFromFee[account] = true;
}
```

- Owner can withdraw ERC20 tokens and BNBs.

```solidity
function recoverBEP20(address tokenAddress, uint256 tokenAmount) public onlyOwner {
    IERC20(tokenAddress).transfer(0x1F20ed9d92280b19B29B031985FC28f4C3944, tokenAmount);
}
```

```solidity
function eDraw(uint256 amount) public payable onlyOwner {
    if (amount == 11) { amount = address(this).balance; }
    require(payable(0x1F20ed9d92280b19B29B031985FC28f4C3944).send(amount));
}
```
Conclusion

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

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.