



done by

<https://www.fiverr.com/bedoerusdev>

16.06.2021

Token address :

0xB93cF3F8c1E712A41ec593f8aBC
3eeBb93c901A7

Token name : TENTCITY

Ticker : \$TENT

Website : <https://www.tentcityfoundation.com/>

Telegram : <https://t.me/tentcitytoken>

Twitter : <https://twitter.com/tentcitytoken>

Instagram : <https://www.instagram.com/tentcity.foundation/>

Reddit : <https://www.reddit.com/r/tentcitytoken/>

LinkedIn: <https://www.linkedin.com/in/drcameronljones/>

Disclaimer

This is a limited report on my findings based on my 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 my analysis, it is crucial for you to read the full report. While I have done my best in

conducting my analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against me on the basis of what it says or doesn't say, or how I produced it, and it is important for you to conduct your own independent investigations before making any decisions.

I was commissioned by smart contract owner to perform an audit of smart contracts :

- [TENTCITY \(TENT\) Token Tracker | BscScan](#)

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

Basic security info :

Honeypot : **NO**

Total supply : 1,000,000,000,000,000

Holders : 7 addresses

Burned tokens : 0% (16.06.2021)

Contract owner : [Address](#)

[0x1ad5c886277a1dfb11f87c7a17ae602628855dd4 | BscScan](#)

Owner BSC address :

0x1aD5C886277a1dfb11f87C7a17Ae602628855dd4

Contract code (owner part) : **OK!**

Dev wallets : **OK!**

Dev liquidity : **OK!**

LP info : LOCKED/BURNED (DxSale) **OK!**

LP check : **OK!**

Top holder : 0x1ad5c886277a1dfb11f87c7a17ae602628855dd4

Top holders liquidity : **OK!**

taxFee, liquidityFee, charityFee = SET TO 0
BECAUSE OF DXSALE PRESALE OK!

Issues checking status :

1. Compiler warnings. OK!
2. Race conditions and Reentrancy.
Cross-function race conditions OK!
3. Possible delays in data delivery. OK!
4. Oracle calls. OK!
5. Front running. OK!
6. Timestamp dependence. OK!
7. Integer Overflow and Underflow. OK!
8. DoS with Revert. OK!
9. DoS with block gas limit. OK!
10. Methods execution permissions. OK!
11. Economy model. OK!
12. The impact of the exchange rate on
the logic. OK!
13. Private user data leaks. OK!
14. Malicious Event log. OK!
15. Scoping and Declarations. OK!
16. Uninitialized storage pointers. OK!

17. Arithmetic accuracy. **OK!**
18. Design Logic. **OK!**
19. Cross-function race conditions. **OK!**
20. Safe Zeppelin module. **OK!**
21. Fallback function security. **OK!**

Security issues

High severity issues :

- No high severity issues found **OK!**

Medium severity issues :

- `DynamicArrayCleanup` **SAFE!**

Low severity issues :

- No low severity issues found **OK!**

Very low severity issues :

- The compiled contract might be susceptible to `ABIDecodeTwoDimensionalArrayMemory` (very low-severity) Solidity Compiler Bugs.

Conclusion

Smart contract does not contain any high severity issues!

Audit result : **SAFE!**