smart state

Web3 security easier than ever

OGCommunity

OGC Token

Smart contract audit report

August 14, 2024

Table of contents

Summary

This audit encompasses the examination of smart contracts of the OGCommunity OGC Token, an ERC20 standard token.

Centralization risk of minting to a single address is further addressed by the project team by manual token distribution between CEXes, stakings and launchpads.

However, the private key of the wallet that holds the tokens prior to distribution requires additional security measures, as the token itself has no function to block, burn, and / or transfer from the attacker's wallet in case of theft.

Disclaimer

This is a final public security audit report version that might not include vulnerabilities that might have been found and addressed during the audit process.
An audit does not provide any warranties regarding the code security. We presume that a single audit cannot be considered totally sufficient and always recommend several independent audits and a public bug bounty program to ensure code security.
Please do not consider this report as investment and / or financial advice of any kind.

Methodology

During the audit process we have analyzed various security aspects in line with our methodology, which includes:

- Manual code analysis
- Best code practices
- ERC20/BEP20 compliance (if applicable)
- Locked ether
- Pool Asset Security (backdoors in the underlying ERC-20)
- FA2 compliance (if applicable)
- Logical bugs & code logic issues
- Error handling issues
- General Denial Of Service(DOS)
- Cryptographic errors
- Weak PRNG / Random number generators issues
- Protocol and header parsing errors
- Private data leaks
- Using components with known vulnerabilities
- Unchecked call return method
- Code with no effects
- Unused vars
- Use of deprecated functions
- Authorization issues
- Re-entrancy
- Arithmetic Overflows / Underflows
- Hidden Malicious Code
- External Contract Referencing
- Short Address/Parameter Attack
- Race Conditions / Front Running
- Uninitialized Storage Pointers
- Floating Points and Precision
- Signatures Replay

Vulnerabilities found by type

INFO	0
LOW	0
MEDIUM	0
HIGH	0
CRITICAL	0
Total	0

OGC-token.sol contract methods analysis:

constructor(address)
Vulnerabilities not detected

approve(address,uint256)
Vulnerabilities not detected

allowance(address,address)
Vulnerabilities not detected

balanceOf(address)
Vulnerabilities not detected

decimals()
Vulnerabilities not detected

name()
Vulnerabilities not detected

symbol()
Vulnerabilities not detected

totalSupply()
Vulnerabilities not detected

OGC-token.sol contract methods analysis:

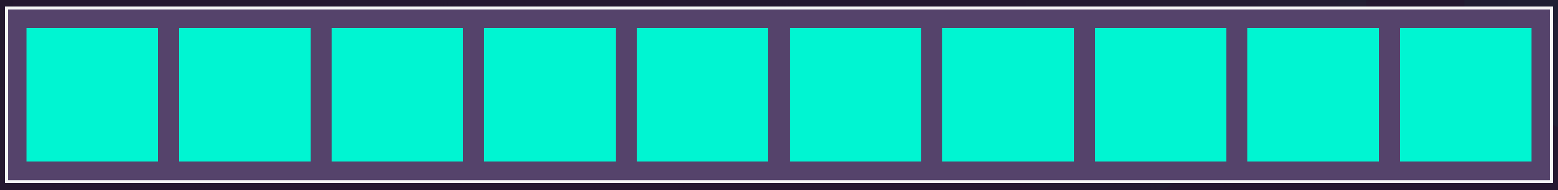
`transfer(address,uint256)`
Vulnerabilities not detected

`transferFrom(address,address,uint256)`
Vulnerabilities not detected

Verification checksums

Contract	Bytecode hash(SHA-256)
OGC-token.sol	bdeec8810cc35046bf10822c72e49041636069364e1e78ca73cc2fc5c8dab8d3

Project evaluation



10/10

Get in touch 👋

@smartstatetech

@smartstate

@SmartStateAudit

@smartstatetech

@smartstate.tech

View this report on Smartstate.tech

info@smartstate.tech

smartstate.tech