# smart state

> Smart
Contract
Audit #

# BullPerks


Oct 31
2021

# TABLE OF CONTENTS

# METHODOLOGY

## MAIN TESTS LIST:

- Best code practices
- ERC20/BEP20 compliance (if applicable)
- Logical bugs
- General Denial Of Service(DOS)
- Locked ether
- Private data leaks
- Using components with known vulns
- Weak PRNG
- Unsed vars
- Uncheked call return method
- Code with no effects
- Pool Asset Security (backdoors in the underlying ERC-20)
- Function visibility
- Use of deprecated functions
- Authorization issues
- Re-entrancy
- Arithmetic Over/Under Flows
- Hidden Malicious Code
- External Contract Referencing
- Short Address/ Parameter Attack
- Race Conditions / Front Running
- Uninitialized Storage Pointers
- Floating Points and Precision
- Signatures Replay

# STRUCTURE OF CONTRACT

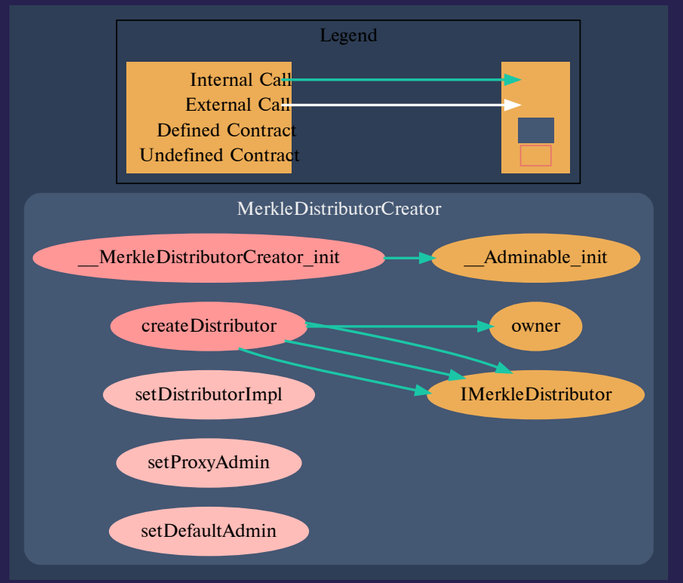
MERKLEDISTRIBUTORCREATOR.SOL

## CONTRACT METHODS ANALYSIS:

- __MerkleDistributorCreator_init(address _distributorImpl, address _proxyAdmin, address _defaultAdmin)
  Vulnerabilities not detected

- createDistributor(address _token, bytes32 _merkleRoot)
  Vulnerabilities not detected

- setDistributorImpl(address _distributorImpl)
  Vulnerabilities not detected




Pic. 1.1.
MerkleDistributorCreator.sol

- setProxyAdmin(address _proxyAdmin)
  Vulnerabilities not detected

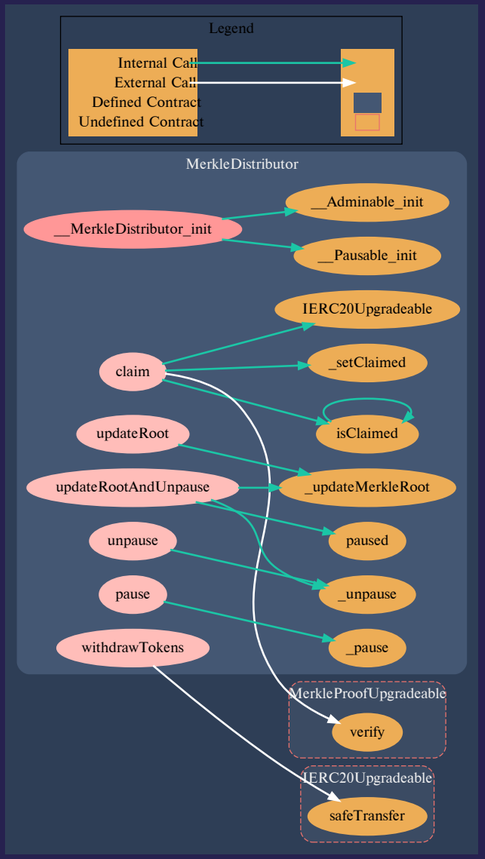
- setDefaultAdmin(address _defaultAdmin)
  Vulnerabilities not detected

# STRUCTURE OF CONTRACT

MERKLEDISTRIBUTOR.SOL

## CONTRACT METHODS ANALYSIS:

- __MerkleDistributor_init(address _token, bytes32 _merkleRoot)
  Vulnerabilities not detected
- isClaimed(uint256 _index)
  Vulnerabilities not detected
- isClaimed(uint256 _merkleIndex, uint256 _index)
  Vulnerabilities not detected




Pic. 1.2.
MerkleDistributor.sol

**PAYABLE**

- claim(uint256 _index, address _account, uint256 _amount, bytes32[] calldata _merkleProof)
  Vulnerabilities not detected

tokens out, public

- updateRoot(bytes32 _merkleRoot)
  An ability to update root allows admin to set malicious root, which for example will enclude his address with all tokens on the contract, which will potentially lead to abuse in withdrawing tokens. We recommend to remove this rights from admin.

- updateRootAndUnpause(bytes32 _merkleRoot)
  An ability to update root allows admin to set malicious root, which for example will enclude his address with all tokens on the contract, which will potentially lead to abuse in withdrawing tokens. We recommend to remove this rights from admin.

**PAYABLE**

- withdrawTokens(IERC20Upgradeable _token, uint256 _amount)
  Vulnerabilities not detected

tokens out, only owner

- _updateMerkleRoot(bytes32 _merkleRoot)
  Vulnerabilities not detected

- _setClaimed(uint256 _index)
  Vulnerabilities not detected

# VERIFICATION CHECK SUMS

| Contract Name | Solc version | Optimisation | Bytecode hash (SHA 256) |
|---|---|---|---|
| MerkleDistributorCreator | 0.8.7 | 200 | 6c4e85bc42bca29c3cd7da050ee16dfd8e4899769d3d752dabc352ff2028d8f7 |
| MerkleDistributor | 0.8.7 | 200 | 1a5b0a48730efeb76436c5d5b8b343418ca13ff1fe376386b8aa3fafb139c1ae |

# Get In Touch

*and Happy Halloween!*

info@smartstate.tech

smartstate.tech