smart state

Web3 security
easier than ever

DAO Maker

Dao Maker

Oct 04

2022

TABLE OF CONTENTS

METHODOLOGY

MAIN TESTS LIST:

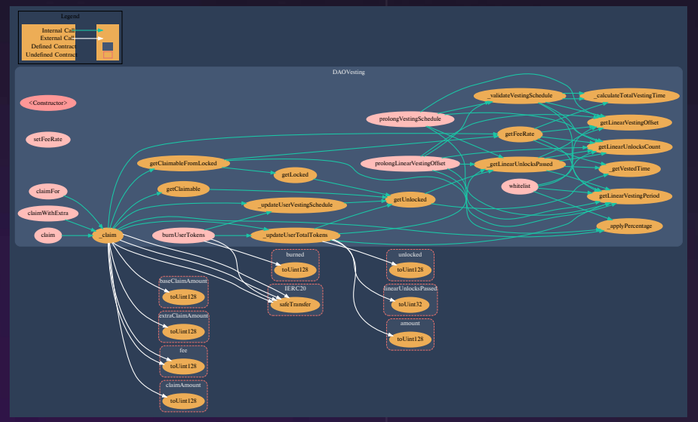
- Best code practices
- ERC20/BEP20 compliance (if applicable)
- FA2 compliance (if applicable)
- Logical bugs
- General Denial Of Service(DOS)
- Locked ether
- Private data leaks
- Using components with known vulns
- Weak PRNG
- Unused vars
- Unchecked call return method
- Code with no effects
- Pool 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

DAOVESTING.SOL

CONTRACT METHODS ANALYSIS:

- setFeeRate(uint16 _feeRateStart, uint16 _feeRateEnd)
  Vulnerabilities not detected
- prolongVestingSchedule(uint32 _linearVestingPeriod, uint32 _linearUnlocksCount)
  Vulnerabilities not detected
- prolongLinearVestingOffset(uint32 _linearVestingOffset)
  Vulnerabilities not detected
- whitelist(address[] calldata userAddresses,uint128[] calldata userTotalTokens,bool last)
  Vulnerabilities not detected



Pic. 1.1
DAOVesting.sol

TOKEN FLOW

- burnUserTokens(address userAddress, uint amount)
  Vulnerabilities not detected

Tokens out, onlyOwner

- claim()
  Vulnerabilities not detected
- claimFor(address userAddress)
  Vulnerabilities not detected
- claimWithExtra(uint extraClaimAmount)
  Vulnerabilities not detected

TOKEN FLOW

- _claim(address userAddress, uint extraClaimAmount)
  Vulnerabilities not detected

Tokens out, public

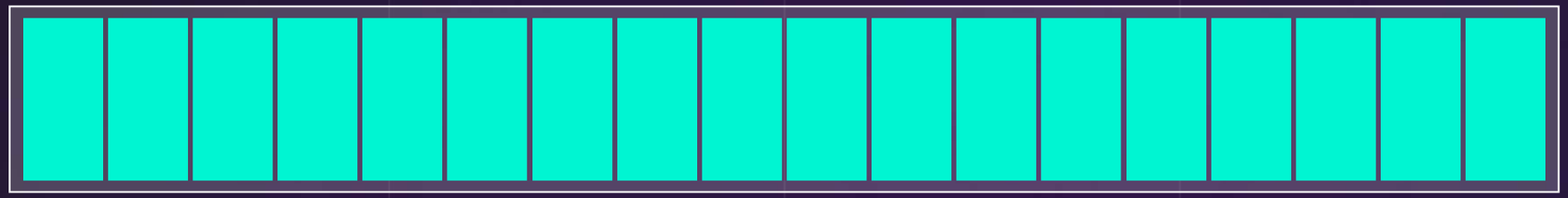
- _updateUserTotalTokens(address userAddress, uint amount)
  Vulnerabilities not detected
- _updateUserVestingSchedule(address userAddress)
  Vulnerabilities not detected
- getClaimable(address userAddress)
  Vulnerabilities not detected
- getClaimableFromLocked(address userAddress)
  Vulnerabilities not detected
- getFeeRate()
  Vulnerabilities not detected
- getUnlocked(address userAddress, uint timestampAt)
  Vulnerabilities not detected

- getLocked(address userAddress)
  Vulnerabilities not detected
- getLinearVestingOffset()
  Vulnerabilities not detected
- getLinearVestingPeriod()
  Vulnerabilities not detected
- getLinearUnlocksCount()
  Vulnerabilities not detected
- _getVestedTime(uint timestampAt)
  Vulnerabilities not detected
- _getLinearUnlocksPassed(address userAddress, uint timestampAt)
  Vulnerabilities not detected
- _applyPercentage(uint value, uint percentage)
  Vulnerabilities not detected
- _calculateTotalVestingTime(uint linearVestingOffset, uint linearVestingPeriod, uint linearUnlocksCount)
  Vulnerabilities not detected
- _validateVestingSchedule()
  Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Solc version	Optimization	Bytecode hash (SHA 256)
DAOVesting.sol	0.8.14	200	dcca2f67a066f6d8483b5973cd31891a76de1bdb54f3006462c182887196361c

PROJECT EVALUATION



10/10

smart state

GET IN TOUCH

info@smartstate.tech
smartstate.tech

View this report on smartstate.tech