smart state

> Smart
Contract
Audit #

WONO

Nov 21
2021

TABLE OF CONTENTS

METHODOLOGY

MAIN TESTS LIST:

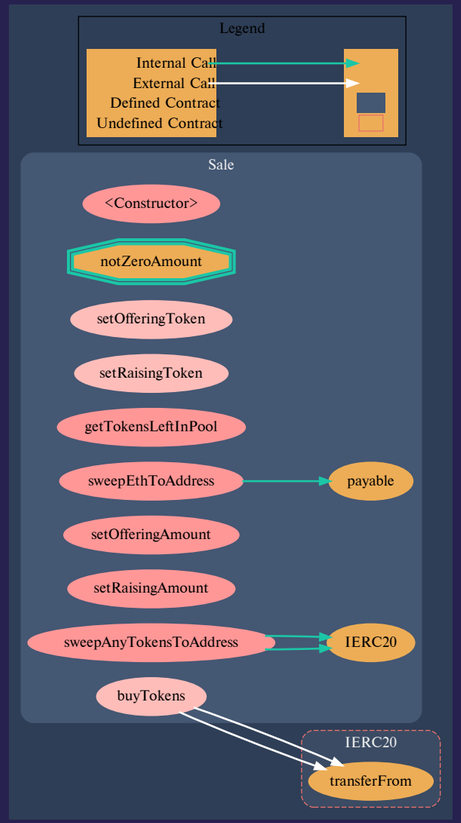
- Best code practices
- ERC20/BEP20 compliance (if applicable)
- Logical bugs
- General Denial Of Service(DOS)
- Locked ether
- Private data leaks
- Using components with known vulns
- Weak PRNG
- Unsed vars
- Uncheked call return method
- Code with no effects
- Pool Asset Security (backdoors in the 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

SALE.SOL

CONTRACT METHODS ANALYSIS:

- setOfferingToken(IERC20 _offeringToken)
  Vulnerabilities not detected
- setRaisingToken(IERC20 _raisingToken)
  Vulnerabilities not detected
- getTokensLeftInPool()
  Function should emit an event



Pic. 1.1.
Sale.sol

PAYABLE

- buyTokens(uint _tokensToBuy)
  Function should emit an event

raising tokens in, offer tokens out, public

- setOfferingAmount(uint _offerAmount)
  Vulnerabilities not detected

- setRaisingAmount(uint _raisingAmount)
  Vulnerabilities not detected

PAYABLE

- sweepEthToAddress(address _user)
  Vulnerabilities not detected

eth out, only owner

PAYABLE

- sweepAnyTokensToAddress(address _token, address _user)
  Vulnerabilities not detected

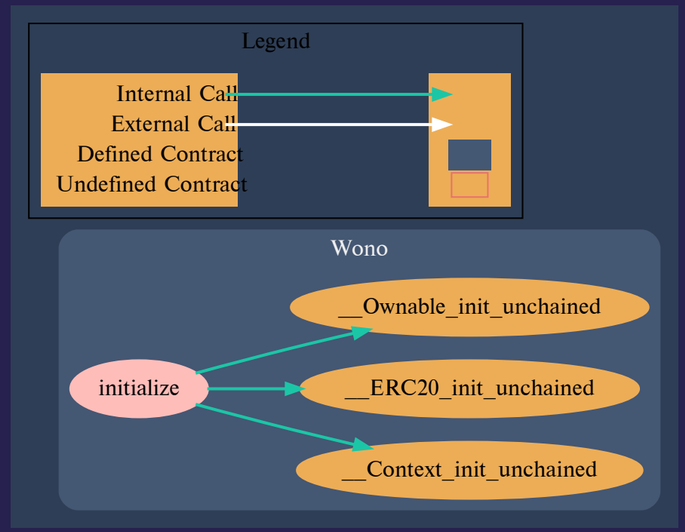
tokens out, only owner

STRUCTURE OF CONTRACT

WONO.SOL

CONTRACT METHODS ANALYSIS:

- initialize()
  Vulnerabilities not detected



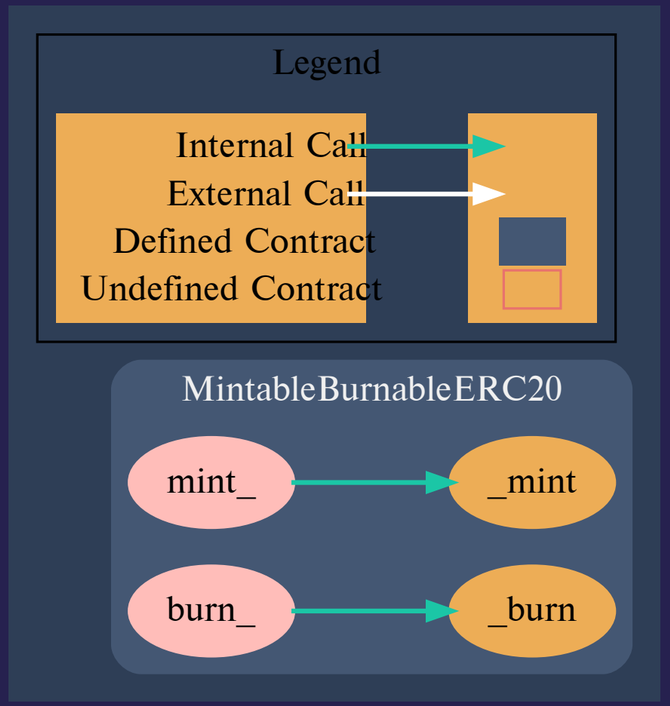
Pic. 1.2.
Wono.sol

STRUCTURE OF CONTRACT

MINTABLEBURNABLEERC20.SOL

CONTRACT METHODS ANALYSIS:

- mint_(address acct, uint amt)
  Vulnerabilities not detected
- burn_(address acct, uint amt)
  Vulnerabilities not detected



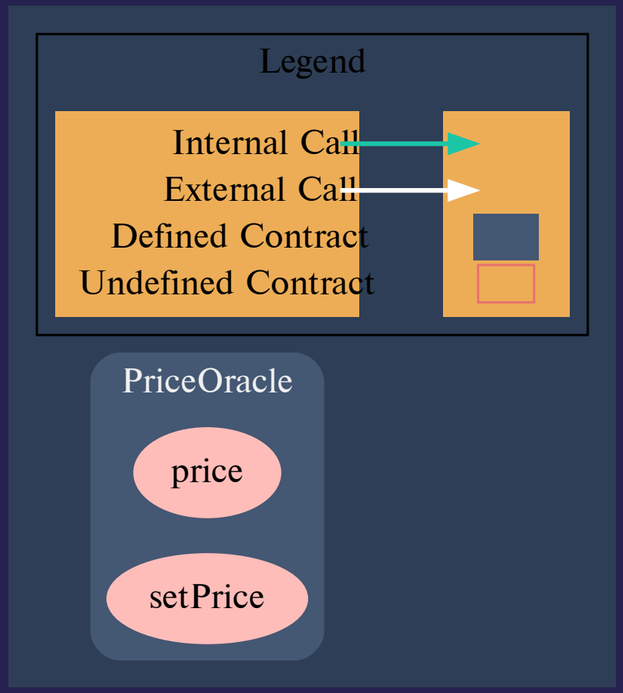
Pic. 1.3.
MintableBurnableERC20.sol

STRUCTURE OF CONTRACT

PRICEORACLE.SOL

CONTRACT METHODS ANALYSIS:

- price()
  Vulnerabilities not detected
- setPrice(uint _currentPrice)
  Vulnerabilities not detected



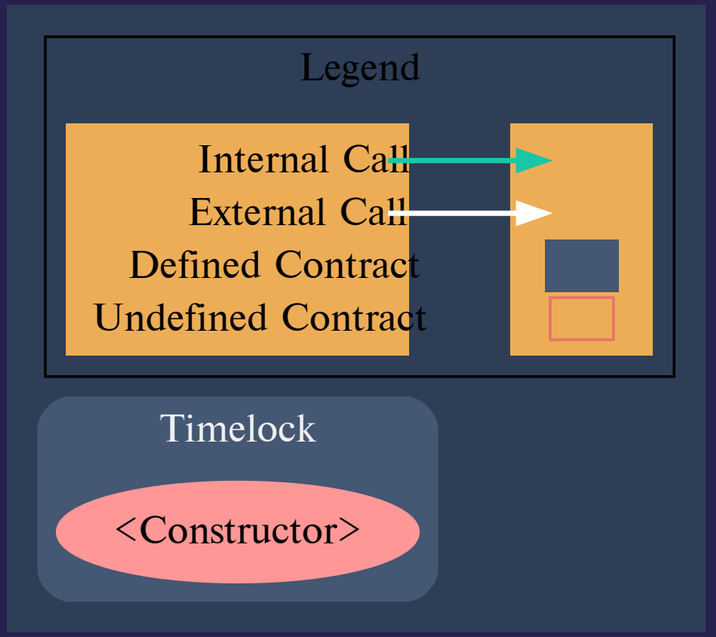
Pic. 1.4.
PriceOracle.sol

STRUCTURE OF CONTRACT

TIMELOCK.SOL

CHECK SUMMARY:

Vulnerabilities not detected



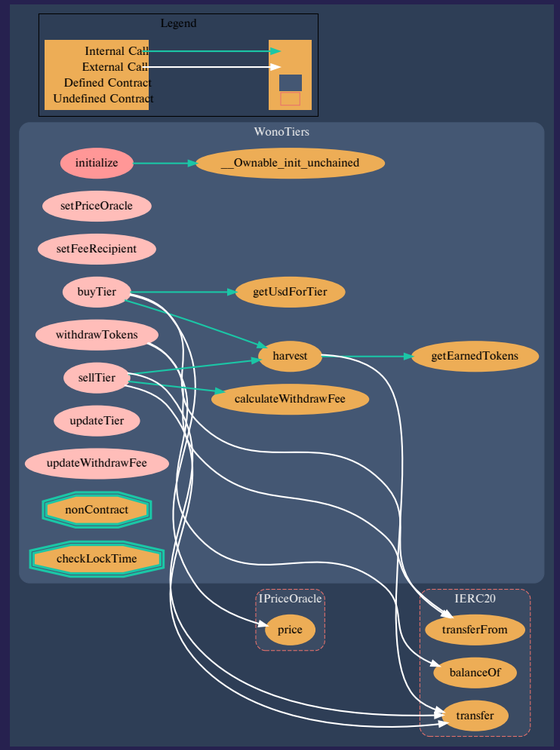
Pic. 1.5.
Timelock.sol

STRUCTURE OF CONTRACT

WONOTIERS.SOL

CONTRACT METHODS ANALYSIS:

- initialize(IERC20 _wonoTokenAddress, IPriceOracle _priceOracle, address _wonoFeeRecipient)
  Vulnerabilities not detected
- getEarnedTokens(address userAddress)
  Vulnerabilities not detected
- getUsdForTier(address userAddress, uint _tier)
  Vulnerabilities not detected
- setPriceOracle(IPriceOracle _priceOracle)
  Vulnerabilities not detected



Pic. 1.6.
WonoTiers.sol

- setFeeRecipient(address _ wonoFeeRecipient)
  Vulnerabilities not detected

PAYABLE

- buyTier(uint tier)
  Vulnerabilities not detected

wono tokens in, public

PAYABLE

- sellTier()
  Now fee tokens are deadlocked on the contract. Consider transfering them to fee recepient or implemeting a method to withdraw them

wono tokens out, public

PAYABLE

- harvest()
  Vulnerabilities not detected

wono tokens out, public

- updateTier(uint8 tierId, uint price, uint lockupTime, uint apr)
  Function should emit an event

- updateWithdrawFee(uint _key, uint _ percent)
  Function should emit an event

- calculateWithdrawFee(address _ userAddress, uint _amount)
  Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Solc version	Optimisation	Bytecode hash (SHA 256)
Sale	0.8.10	200	889389019d67d8ab0b4acc791cdbde390ee7865ac3cacc1921284b01ba614721
WonoTiers	0.8.10	200	d16d6b06c93f88c7cc6a5b14c00083e4fa48304e0e18b3f6e5d6e2e8067b960b

Get In Touch

info@smartstate.tech

smartstate.tech