smart state

Web3 security
easier than ever

1inch NETWORK

1inch

Dec 09

2022

TABLE OF CONTENTS

METHODOLOGY

MAIN TESTS LIST:

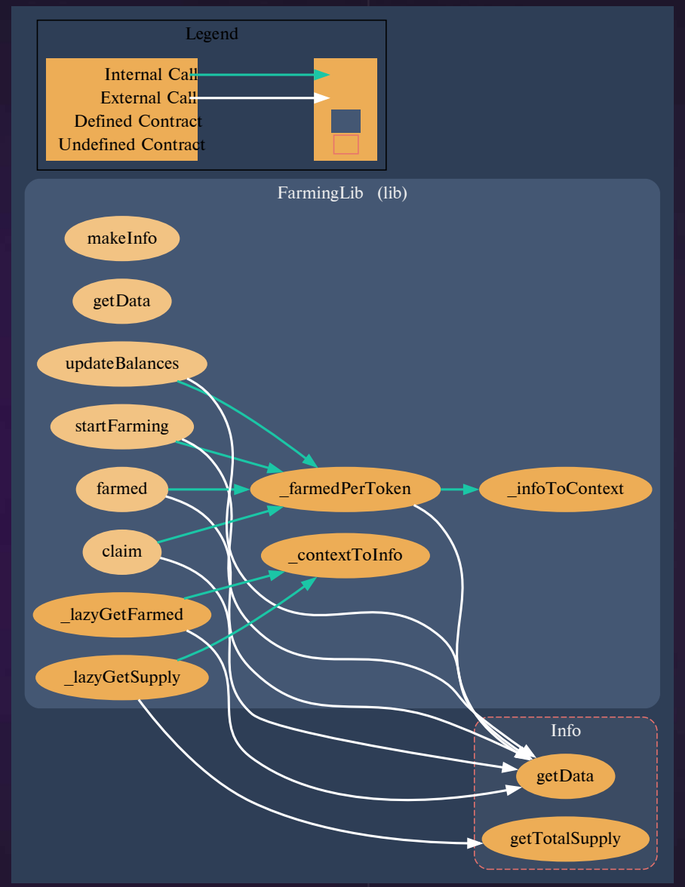
- Best code practices
- ERC20/BEP20 compliance (if applicable)
- FA2 compliance (if applicable)
- Logical bugs
- General Denial Of Service(DOS)
- Locked ether
- Private data leaks
- Using components with known vulns
- Weak PRNG
- Unused vars
- Unchecked call return method
- Code with no effects
- Pool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

FARMINGLIB.SOL

CONTRACT METHODS ANALYSIS:

- makeInfo(function() internal view returns(uint256) getTotalSupply, Data storage data)
  Vulnerabilities not detected
- getData(Info memory self)
  Vulnerabilities not detected
- startFarming(Info memory self, uint256 amount, uint256 period)
  Vulnerabilities not detected
- farmed(Info memory self, address account, uint256 balance)
  Vulnerabilities not detected
- claim(Info memory self, address account, uint256 balance)
  Vulnerabilities not detected



Pic. 1.1
FarmingLib.sol

- updateBalances(Info memory self, address from, address to, uint256 amount)
  Vulnerabilities not detected
- _farmedPerToken(Info memory self)
  Vulnerabilities not detected
- _lazyGetSupply(bytes32 context)
  Vulnerabilities not detected
- _lazyGetFarmed(bytes32 context, uint256 checkpoint)
  Vulnerabilities not detected
- _contextToInfo(bytes32 context)
  Vulnerabilities not detected
- _infoToContext(Info memory self)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

FARMINGPOD.SOL

CONTRACT METHODS ANALYSIS:

- totalSupply()
  Vulnerabilities not detected

- getFarmInfo()
  Vulnerabilities not detected

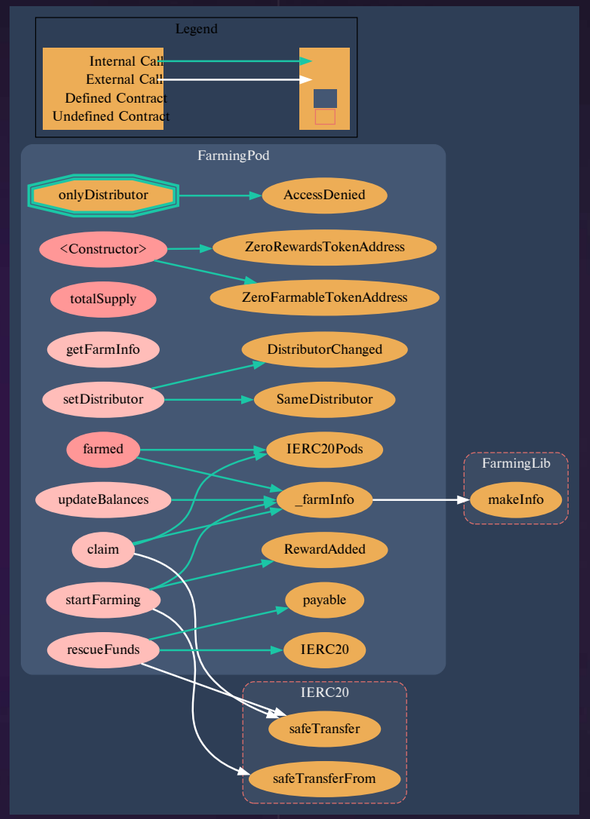
- setDistributor(address distributor_)
  Vulnerabilities not detected

TOKEN FLOW

- startFarming(uint256 amount, uint256 period)
  Vulnerabilities not detected

Tokens in, onlyDistributor

- farmed(address account)
  Vulnerabilities not detected



Pic. 1.2
FarmingPod.sol

TOKEN FLOW

- claim()
  Vulnerabilities not detected

Tokens out, public

- updateBalances(address from, address to, uint256 amount)
  Vulnerabilities not detected

TOKEN FLOW

- rescueFunds(IERC20 token, uint256 amount)
  Vulnerabilities not detected

ETH out, Tokens out, onlyDistributor

- _farmInfo()
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

FARMINGPOOL.SOL

CONTRACT METHODS ANALYSIS:

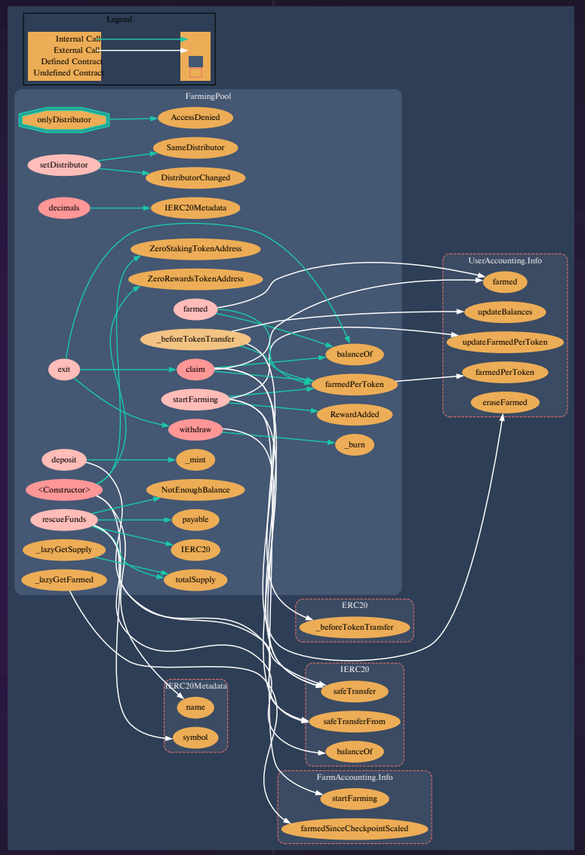
- setDistributor(address distributor_)
  Vulnerabilities not detected

TOKEN FLOW

- startFarming(uint256 amount, uint256 period)
  Vulnerabilities not detected

Tokens in, onlyDistributor

- decimals()
  Vulnerabilities not detected
- farmedPerToken()
  Vulnerabilities not detected
- farmed(address account)
  Vulnerabilities not detected



Pic. 1.3
FarmingPool.sol

TOKEN FLOW

- deposit(uint256 amount)
  Vulnerabilities not detected

Tokens in, public

TOKEN FLOW

- withdraw(uint256 amount)
  Vulnerabilities not detected

Tokens out, public

TOKEN FLOW

- claim()
  Vulnerabilities not detected

Tokens out, public

- exit()
  Vulnerabilities not detected

TOKEN FLOW

- rescueFunds(IERC20 token, uint256 amount)
  Vulnerabilities not detected

ETH out, Tokens out, onlyDistributor

- _beforeTokenTransfer(address from, address to, uint256 amount)
  Vulnerabilities not detected
- _lazyGetSupply(bytes32 /* context */)
  Vulnerabilities not detected
- _lazyGetFarmed(bytes32 /* context */, uint256 checkpoint)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

MULTIFARMINGPOD.SOL

CONTRACT METHODS ANALYSIS:

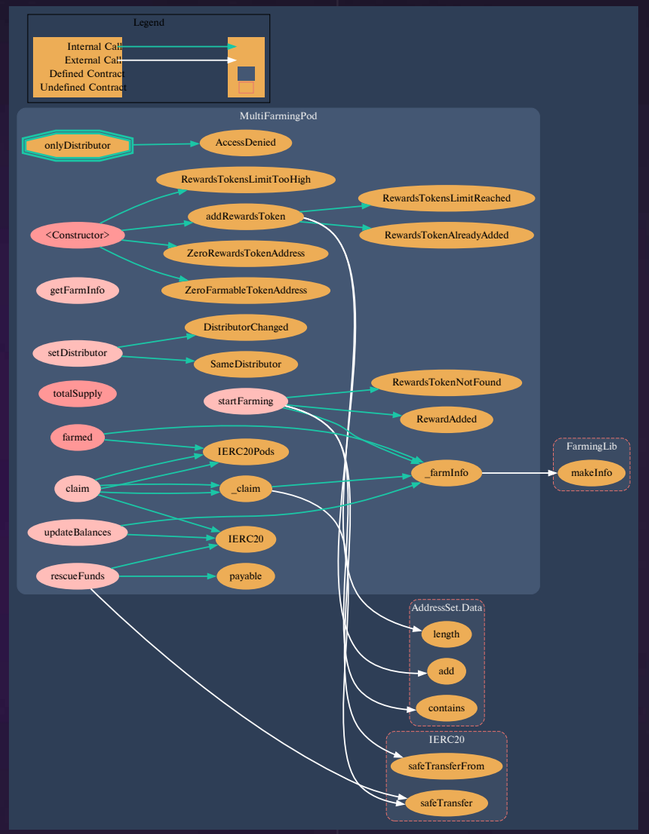
- getFarmInfo(IERC20 rewardsToken)
  Vulnerabilities not detected
- setDistributor(address distributor_)
  Vulnerabilities not detected
- addRewardsToken(IERC20 rewardsToken)
  Vulnerabilities not detected

TOKEN FLOW

- startFarming(IERC20 rewardsToken, uint256 amount, uint256 period)
  Vulnerabilities not detected

Tokens in, onlyDistributor

- totalSupply()
  Vulnerabilities not detected



Pic. 1.4
MultiFarmingPod.sol

- farmed(IERC20 rewardsToken, address account)
  Vulnerabilities not detected

TOKEN FLOW

- claim(IERC20 rewardsToken)
  Vulnerabilities not detected

Tokens out, public

- claim()
  Vulnerabilities not detected

- updateBalances(address from, address to, uint256 amount)
  Vulnerabilities not detected

- rescueFunds(IERC20 token, uint256 amount)
  Vulnerabilities not detected

TOKEN FLOW

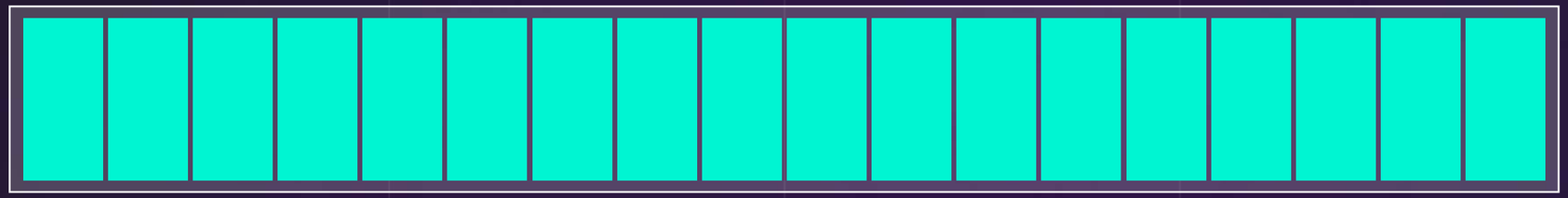
- rescueFunds(IERC20 token, uint256 amount)
  Vulnerabilities not detected

ETH out, Tokens out, onlyDistributor

VERIFICATION CHECK SUMS

Contract Name	Solc version	Optimization	Bytecode hash (SHA 256)
FarmingLib.sol	0.8.12	200	0a908f44419c5cc40698b4f9a2a4a502bf4adeac0b96a84c6f6b869632eedb27
FarmingPod.sol	0.8.12	200	caad7964a77ec51e33ba9f8e22edbcca35d2afc09b8b11bbbf1c4d5829d55b5f
FarmingPool.sol	0.8.12	200	8f517779503d8211c377c2fa9bb6531a5a05934d5eee91a699bea54b34b409f9
MultiFarmingPod.sol	0.8.12	200	3bc88098e3fb82e7e484e20e98eb0fe23cd8be59da1f47cdc8cc07f6c13dbb3f

PROJECT EVALUATION



10/10

GET IN TOUCH

info@smartstate.tech
smartstate.tech

View this report on smartstate.tech