smart state

new generation of
smart contract audit

Sheesha Finance

Jul 09

2022

TABLE OF CONTENTS

METHODOLOGY

MAIN TESTS LIST:

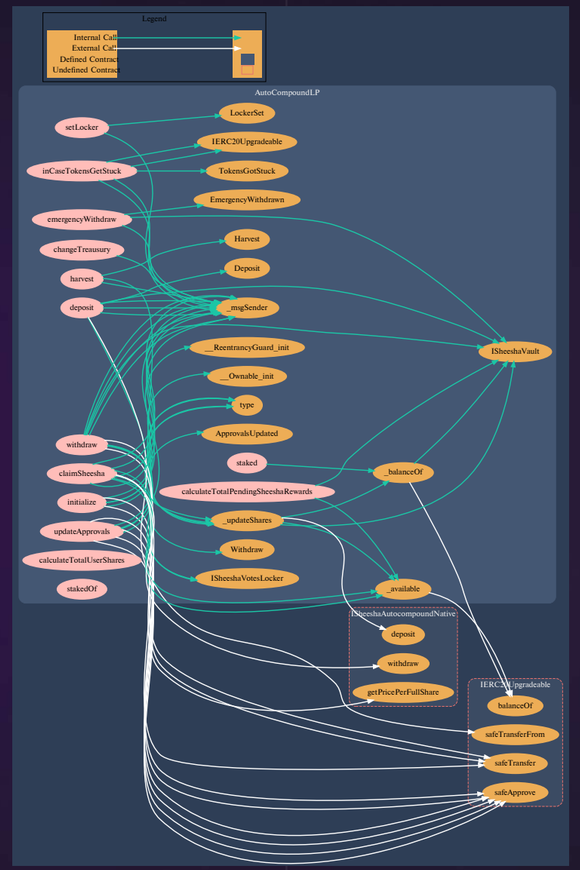
- Best code practices
- ERC20/BEP20 compliance (if applicable)
- FA2 compliance (if applicable)
- Logical bugs
- General Denial Of Service(DOS)
- Locked ether
- Private data leaks
- Using components with known vulns
- Weak PRNG
- Unused vars
- Unchecked call return method
- Code with no effects
- Pool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

AUTOCOMPOUNDLP.SOL

CONTRACT METHODS ANALYSIS:

- initialize(IERC20Upgradeable _sheesha,IERC20Upgradeable _lp,ISheeshaVault _sheeshaVaultLP,ISheeshaAutocompoundNative _autoCompoundNative,address _treasury)
  Vulnerabilities not detected
- updateApprovals()
  Vulnerabilities not detected
- changeTreausury(address _treasury)
  Vulnerabilities not detected
- setLocker(address _locker)
  Vulnerabilities not detected
- emergencyWithdraw()
  Vulnerabilities not detected



Pic. 1.1
AutoCompoundLP.sol

TOKEN FLOW

- inCaseTokensGetStuck(address _token)
  Vulnerabilities not detected

Tokens out, onlyOwner

TOKEN FLOW

- deposit(uint256 _amount)
  Vulnerabilities not detected

Tokens in, public

- harvest()
  Vulnerabilities not detected

TOKEN FLOW

- withdraw(uint256 _amount)
  Vulnerabilities not detected

Tokens out, public

TOKEN FLOW

- claimSheesha(uint256 _shares)
  Vulnerabilities not detected

Tokens out, public

- calculateTotalPendingSheeshaRewards()
  Vulnerabilities not detected

- calculateTotalUserShares(address _user)
  Vulnerabilities not detected

- staked()
  Vulnerabilities not detected

- stakedOf(address member)
  Vulnerabilities not detected

- _available()
  Vulnerabilities not detected

- _balanceOf()
  Vulnerabilities not detected

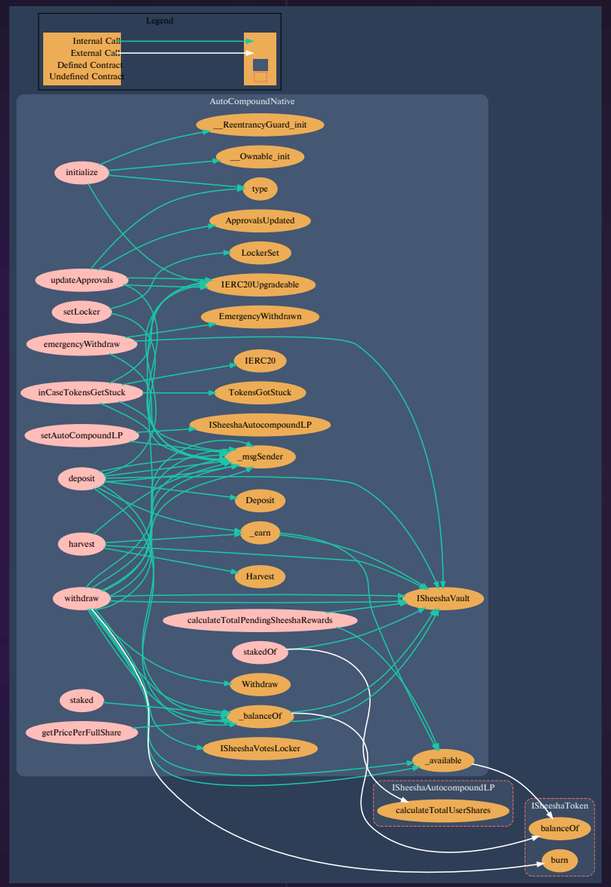
- _updateShares()
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

AUTOCOMPOUNDNATIVE.SOL

CONTRACT METHODS ANALYSIS:

- initialize(ISheeshaToken _sheesha, ISheeshaVault _sheeshaVault)
  Vulnerabilities not detected
- updateApprovals()
  Vulnerabilities not detected
- setLocker(address _locker)
  Vulnerabilities not detected
- setAutoCompoundLP(address _autoCompoundLP)
  Vulnerabilities not detected



Pic. 1.2
AutoCompoundNative.sol

- emergencyWithdraw()
  Vulnerabilities not detected

TOKEN FLOW

- inCaseTokensGetStuck(address _token)
  Vulnerabilities not detected

Tokens out, onlyOwner

TOKEN FLOW

- deposit(uint256 _amount)
  Vulnerabilities not detected

Tokens in, public

- harvest()
  Vulnerabilities not detected

TOKEN FLOW

- withdraw(uint256 _shares)
  Vulnerabilities not detected

Tokens out, public

- calculateTotalPendingSheeshaRewards()
  Vulnerabilities not detected

- getPricePerFullShare()
  Vulnerabilities not detected

- staked()
  Vulnerabilities not detected

- stakedOf(address member)
  Vulnerabilities not detected

- _available()
  Vulnerabilities not detected

- _balanceOf()
  Vulnerabilities not detected

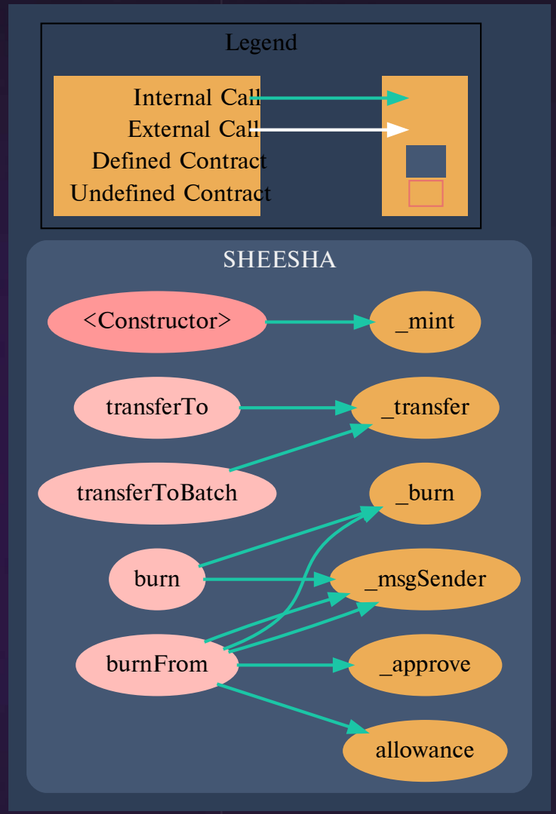
- _earn()
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

SHEESHA.SOL

CONTRACT METHODS ANALYSIS:

- transferTo(address _dest, uint256 _amount)
  Vulnerabilities not detected
- transferToBatch(address[] calldata _dest,uint256[] calldata _amount)
  Vulnerabilities not detected
- burn(uint256 amount)
  Vulnerabilities not detected
- burnFrom(address account, uint256 amount)
  Vulnerabilities not detected



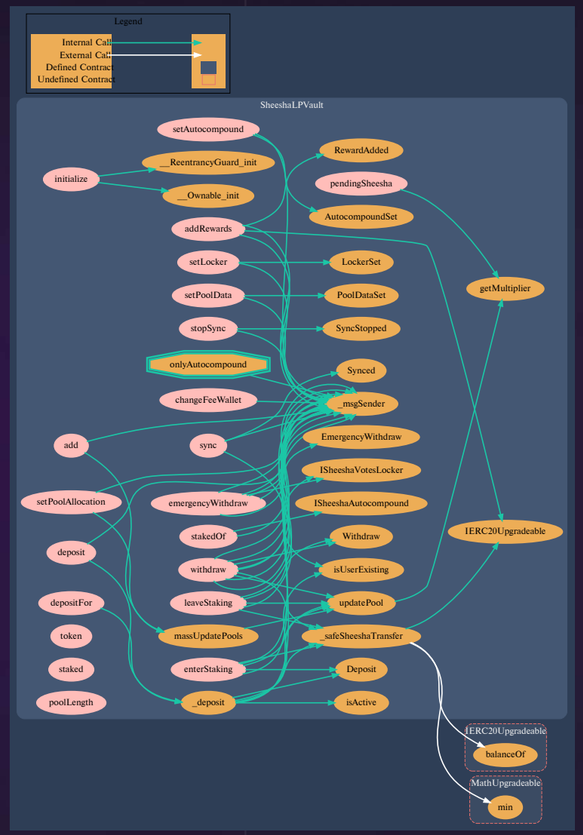
Pic. 1.3
SHEESHA.sol

STRUCTURE OF CONTRACT

SHEESHALPVAULT.SOL

CONTRACT METHODS ANALYSIS:

- initialize(IERC20Upgradeable _sheesha, address _feeWallet, uint256 _startBlock, uint256 _sheeshaPerBlock, uint256 _lpRewards)
  Vulnerabilities not detected
- changeFeeWallet(address _feeWallet)
  Vulnerabilities not detected
- setAutocompound(address _autoCompound)
  Vulnerabilities not detected
- setLocker(address _locker)
  Vulnerabilities not detected



Pic. 1.4
SheeshaLPVault.sol

- add(uint256 _allocPoint, IERC20Upgradeable _lpToken, bool _withUpdate)
  Vulnerabilities not detected

TOKEN FLOW

- addRewards(uint256 _amount)
  Vulnerabilities not detected

Tokens in, public

- setPoolAllocation(uint256 _pid, uint256 _allocPoint, bool _withUpdate)
  Vulnerabilities not detected

- setPoolData(uint256 _blockNumber, uint256 _accSheeshaPerShare)
  Vulnerabilities not detected

- sync(address[] calldata _addr, uint256[] calldata _amount, uint256[] calldata _rewardDebt)
  Vulnerabilities not detected

- stopSync()
  Vulnerabilities not detected

TOKEN FLOW

- enterStaking(uint256 _amount)
  Vulnerabilities not detected

Tokens in, only autoCompound

TOKEN FLOW

- leaveStaking(uint256 _amount)
  Vulnerabilities not detected

Tokens out, only autoCompound

TOKEN FLOW

- deposit(uint256 _pid, uint256 _amount)
  Vulnerabilities not detected

Tokens in, public

TOKEN FLOW

- depositFor(address _depositFor, uint256 _pid, uint256 _amount)
  Vulnerabilities not detected

Tokens in, public

TOKEN FLOW

- withdraw(uint256 _pid, uint256 _amount)
  Vulnerabilities not detected

Tokens out, public

TOKEN FLOW

- emergencyWithdraw(uint256 _pid)
  Vulnerabilities not detected

Tokens out, public

- pendingSheesha(uint256 _pid, address _user)
  Vulnerabilities not detected

- token()
  Vulnerabilities not detected
- staked()
  Vulnerabilities not detected
- stakedOf(address member)
  Vulnerabilities not detected
- poolLength()
  Vulnerabilities not detected
- massUpdatePools()
  Vulnerabilities not detected
- updatePool(uint256 _pid)
  Vulnerabilities not detected
- getMultiplier(uint256 _from, uint256 _to)
  Vulnerabilities not detected
- isUserExisting(address _who)
  Vulnerabilities not detected

- `isActive(uint256 _pid, address _user)`
  Vulnerabilities not detected

- `_deposit(address _depositFor, uint256 _pid, uint256 _amount)`
  Vulnerabilities not detected

- `_safeSheeshaTransfer(address _to, uint256 _amount)`
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

SHEESHASHVAULT.SOL

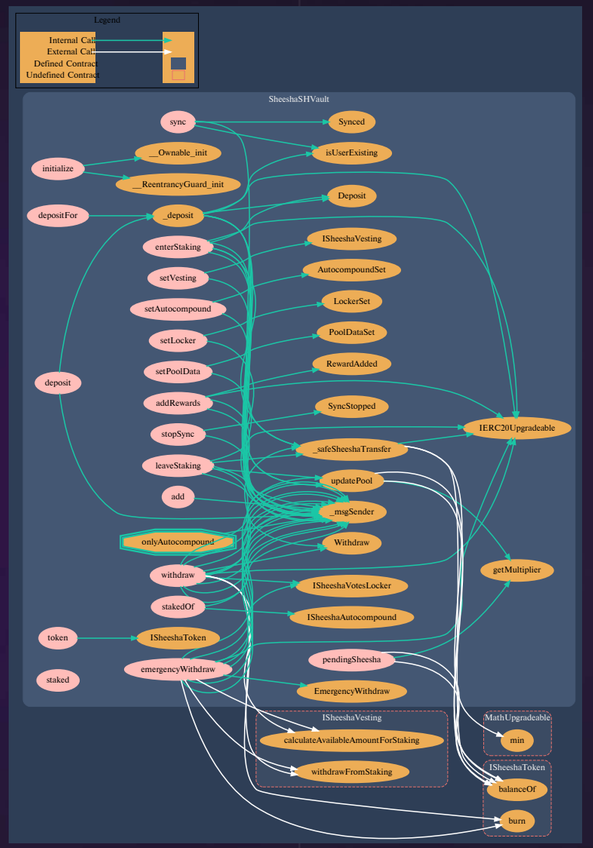
CONTRACT METHODS ANALYSIS:

- initialize(ISheeshaToken _sheesha, uint256 _startBlock, uint256 _sheeshaPerBlock, uint256 _tokenRewards)
  Vulnerabilities not detected

- setVesting(address _vesting)
  Vulnerabilities not detected

- setAutocompound(address _autoCompound)
  Vulnerabilities not detected

- setLocker(address _locker)
  Vulnerabilities not detected



Pic. 1.5
SheeshaSHVault.sol

- add(IERC20 _token)
  Vulnerabilities not detected

- addRewards(uint256 _amount)
  Vulnerabilities not detected

- setPoolData(uint256 _blockNumber, uint256 _accSheeshaPerShare)
  Vulnerabilities not detected

- sync(address[] calldata _addr, uint256[] calldata _amount, uint256[] calldata _rewardDebt)
  Vulnerabilities not detected

TOKEN FLOW

- enterStaking(uint256 _amount)
  Vulnerabilities not detected

Tokens in, only autoCompound

TOKEN FLOW

- leaveStaking(uint256 _amount)
  Vulnerabilities not detected

Tokens out, only autoCompound

TOKEN FLOW

- deposit(uint256 _pid, uint256 _amount)
  Vulnerabilities not detected

Tokens in, public

TOKEN FLOW

- depositFor(address _depositFor, uint256 _pid, uint256 _amount)
  Vulnerabilities not detected

Tokens in, public

TOKEN FLOW

- withdraw(uint256 _pid, uint256 _amount)
  Vulnerabilities not detected

Tokens out, public

TOKEN FLOW

- emergencyWithdraw(uint256 _pid)
  Vulnerabilities not detected

Tokens out, public

- pendingSheesha(uint256 _pid, address _user)
  Vulnerabilities not detected
- token()
  Vulnerabilities not detected
- staked()
  Vulnerabilities not detected
- stakedOf(address member)
  Vulnerabilities not detected
- updatePool(uint256 _pid)
  Vulnerabilities not detected
- getMultiplier(uint256 _from, uint256 _to)
  Vulnerabilities not detected
- isUserExisting(address _who)
  Vulnerabilities not detected
- _deposit(address _depositFor, uint256 _pid, uint256 _amount)
  Vulnerabilities not detected
- _safeSheeshaTransfer(address _to, uint256 _amount)
  Vulnerabilities not detected

STRUCTURE OF CONTRACT

VESTING.SOL

CONTRACT METHODS ANALYSIS:

- addRecipients(address[] calldata _recipients, uint256[] calldata _amount, VestingType _vestingType)
  Vulnerabilities not detected

TOKEN FLOW

- withdrawFromVesting()
  Vulnerabilities not detected

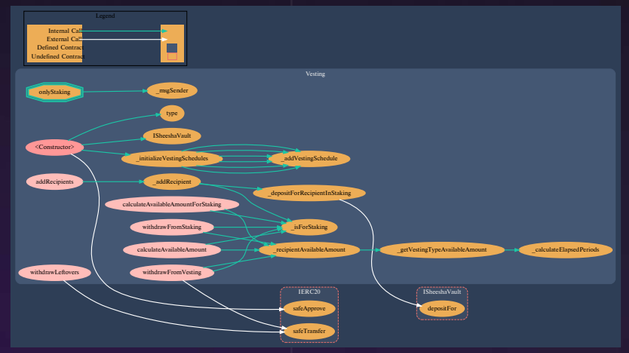
Tokens out, public

- withdrawFromStaking(address recipient, uint256 amount)
  Vulnerabilities not detected

TOKEN FLOW

- withdrawLeftovers(VestingType _type, address recipient)
  Vulnerabilities not detected

Tokens out, onlyOwner



Pic. 1.6
Vesting.sol

- calculateAvailableAmount(address _recipient)
  Vulnerabilities not detected

- calculateAvailableAmountForStaking(address _recipient)
  Vulnerabilities not detected

- _initializeVestingSchedules()
  Vulnerabilities not detected

- _addVestingSchedule(VestingType _type, VestingSchedule memory _schedule)
  Vulnerabilities not detected

- _addRecipient(address _recipient, uint256 _amount, VestingType _vestingType)
  Vulnerabilities not detected

- _depositForRecipientInStaking(address _recipient, uint256 _amount)
  Vulnerabilities not detected

- _isForStaking(VestingType _type)
  Vulnerabilities not detected

- _recipientAvailableAmount(address _recipient, uint256 index)
  Vulnerabilities not detected

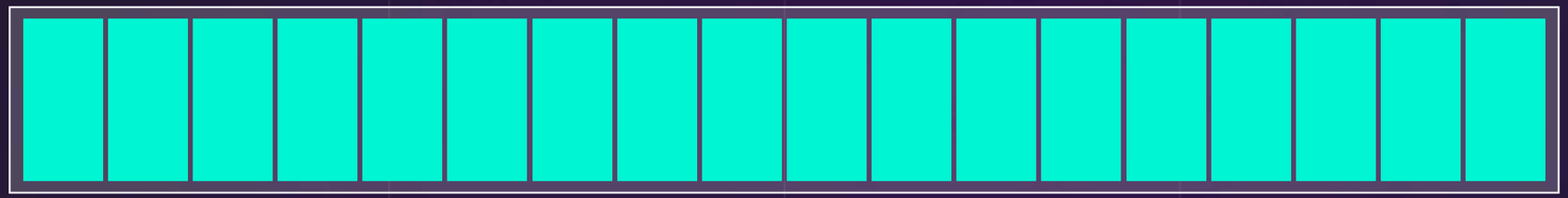
- _getVestingTypeAvailableAmount(VestingSchedule memory _vestingSchedule, uint256 _amount)
  Vulnerabilities not detected

- _calculateElapsedPeriods()
  Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Bytecode hash (SHA 256)
AutoCompoundLP.sol	fbd4aeeb31b863257d98f64ed5ea5e7eb1d0f38264652ecc71edaed3311b7341
AutoCompoundNative.sol	06de91773f44ca6761f8a7eb5b7b59ab366fd2c0711e87acca0c9ea542bcaeb6
SHEESHA.sol	86c1a07434832fb1a3b43884acd92f6d2adc8b85f300296ce4b85ae82bf46039
SheeshaLPVault.sol	b6ac64c1a1731519ed1e065e113bbd92714637b380914e7623a97335de3c66a5
SheeshaSHVault.sol	65f293ff86da28dffa074f725b9dc3bd67eebde67add19044675bbc38324c9c1
Vesting.sol	348be5f7644896fb7681f3da2e2a0a50299afe46cc5cd83ee0d4e9498c7d952a

PROJECT EVALUATION



10/10

smart state

GET IN TOUCH

info@smartstate.tech
smartstate.tech

View this report on smartstate.tech