smart state

> Smart
Contract
Audit #

blocsport.one

Nov 03
2021

TABLE OF CONTENTS

Table of contents 3

Methodology 4

Stucture of contact AuctionHouse.sol 5

Verification check sums 9

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

AUCTIONHOUSE.SOL

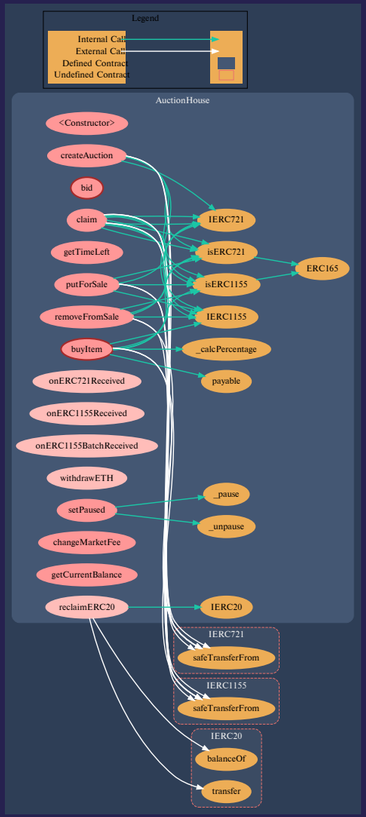
CONTRACT METHODS ANALYSIS:

PAYABLE

- createAuction(
  address nftContract,
  uint256 nftID,
  uint256 startPrice
)

  Vulnerabilities not detected

NFT in, public



Pic. 1.1.
AuctionHouse.sol

PAYABLE

- bid(uint256 auctionId)
  Vulnerabilities not detected

ETH in, public

PAYABLE

- claim(uint256 auctionId)
  First case in if else statement should emit an event.

NFT out, ETH out, public

- getTimeLeft(uint256 auctionId)
  Vulnerabilities not detected

PAYABLE

- putForSale(
  address nftContract,
  uint256 nftID,
  uint256 price,
  uint256 saleDurationInSeconds
)
  Vulnerabilities not detected

NFT out, ETH out, public

PAYABLE

- removeFromSale(uint256 saleID)
  Vulnerabilities not detected

NFT out, public

PAYABLE

- buyItem(uint256 saleID)
  Vulnerabilities not detected

ETH in, NFT out, public

- onERC721Received(
  address,
  address,
  uint256,
  bytes memory
)
  Vulnerabilities not detected

- onERC1155Received(
  address,
  address,
  uint256,
  uint256,
  bytes memory
)
  Vulnerabilities not detected

- onERC1155BatchReceived(
  address,
  address,
  uint256[] memory,
  uint256[] memory,
  bytes memory
)
  Vulnerabilities not detected

PAYABLE

- withdrawETH(uint256 amount)
  Vulnerabilities not detected

ETH out, onlyOwner

PAYABLE

- reclaimERC20(address _tokenContract)
  Vulnerabilities not detected

ERC20 out, onlyOwner

- changeMarketFee(uint256 _marketFee)
  Recommended to add limits for market fee

- isERC721(address contractAddr)
  Vulnerabilities not detected

- isERC1155(address contractAddr)
  Vulnerabilities not detected

- _calcPercentage(uint256 amount, uint256 basisPoints)
  Vulnerabilities not detected

- getCurrentBalance()
  Vulnerabilities not detected

VERIFICATION CHECK SUMS

Contract Name	Solc version	Optimisation	Bytecode hash (SHA 256)
AuctionHouse	0.8.3	200	6fea339291c725cfc89b37128 06fa7305e14cbc767768359f abd1187d232b685

Get In Touch

info@smartstate.tech

smartstate.tech