smart state

> Smart
Contract
Audit #

smart state

Oct 13
2021

TABLE OF CONTENTS

Table of contents 3

Methodology 4

Stucture of contact Contract.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

CONTRACT.SOL

CHECK SUMMARY:

No need for constructor in this contract

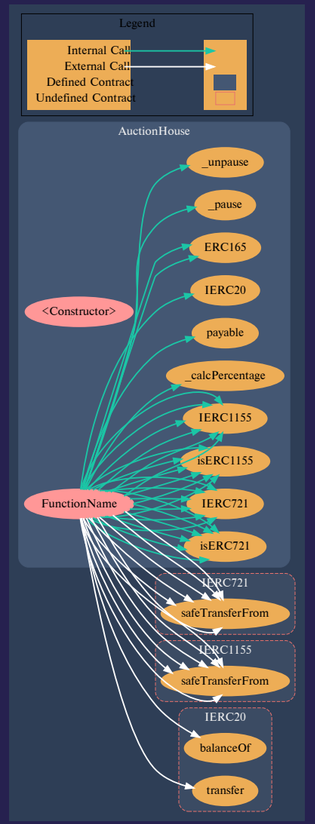
CONTRACT METHODS ANALYSIS:

PAYABLE

- FunctionName(
  a,
  b,
  c
)

  Function can be declared external.

NFT in, public



Pic. 1.1.
Contract.sol

PAYABLE

- FunctionName()

In case funds can be not returned to the previous bidder he will become winner of auction. If attacker bids from malicious contracts which revers on receiving eth, he will become winner. Recommended to add NonReetrant modifier

ETH in, public

PAYABLE

- FunctionName()

Refcommended to add if else if instead of 2 if at lines 172 and 175 + lines 188 and 192 in order to avoid bugs. Function can be declared external. Recommended to add NonReentrant modifier. First case in if else statement should emit an event.

NFT out, ETH out, public

- FunctionName()

Function can be declared external.

PAYABLE

- FunctionName(
  a,
  b,
  c,
  d
)

Function can be declared external

NFT out, ETH out, public

PAYABLE

- FunctionName()

Refcommended to add if else if instead of 2 if at lines 269 and 273 in order to avoid logical bugs

NFT out, public

PAYABLE

- FunctionName()

  Function can be declared external. Recommended to put sl.sold = true before transfer eth in order to avoid potential reentrancy. Recommended to add NonReentrant modifier.

ETH in, NFT out, public

- FunctionName(
  a,
  b,
  c,
  d
)

  Vulnerabilities not detected

- FunctionName(
  a,
  b,
  c,
  d,
  e
)

  Vulnerabilities not detected

- FunctionName(
  a,
  b,
  c,
  d,
  e
)

  Vulnerabilities not detected

PAYABLE

- FunctionName()
  Vulnerabilities not detected

ETH out, onlyOwner

PAYABLE

- FunctionName()
  Vulnerabilities not detected

ERC20 out, onlyOwner

- FunctionName()
  Recommended to add limits for market fee

- FunctionName()
  Vulnerabilities not detected

- FunctionName()
  Vulnerabilities not detected

- FunctionName()
  Vulnerabilities not detected

- FunctionName()
  Function can be declared external

VERIFICATION CHECK SUMS

Contract Name	Solc version	Optimisation	Bytecode hash (SHA 256)
Contract	0.8.3	200	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Get In Touch

info@smartstate.tech

smartstate.tech