HAECHI AUDIT

Zoo Farming

Smart Contract

Security Audit Report

May 7th, 2021

Overview

Project Summary

Target	Zoo Farming
Platform	Wanchain / Solidity
Codebase	Github Repositiory (https://github.com/ZooFarming/zoo-keeper-contracts)
Commit	860bdb99a616a7d0d278ba4d56b376062c1be4f0

Audit Summary

Delivery Date	May. 7, 2021 (Revised in Sep. 6, 2021)
Author	Jasper Lee
Version	1.1

Vulnerability Summary

Severety	**# of Findings**
Critical	0
Major	0
Medium	0
Minor	1
Infomational	0
Total	1

Key Findings

1. Bad Randomness in `NFTFactoryDelegate.randomNFT()` Minor Resolved

Description

Since the random value of `NFTFactoryDelegate.randomNFT()` is a sufficiently predictable value, there is a possibility that a malicious user cherry-picking items of the desired level and category.

NFTFactory/NFTFactoryDelegate.sol:L329-L336

```
329      function randomNFT(bool golden) private view returns (uint tokenId, uint level, uint category, uint item, uint random) {
330          uint totalSupply = IZooNFTMint(zooNFT).totalSupply();
331          tokenId = totalSupply + 1;
332          uint random1 = uint(keccak256(abi.encode(tokenId, msg.sender, blockhash(block.number - 1), block.coinbase, block.timestamp)));
333          uint random2 = uint(keccak256(abi.encode(random1)));
334          uint random3 = uint(keccak256(abi.encode(random2)));
335          uint random4 = uint(keccak256(abi.encode(random3)));
336          uint random5 = uint(keccak256(abi.encode(random4)));
```

Recommendation

Use a safe random number generator like Chainlink Verifiable Random Function.

- Although this is a vulnerability, We think it can be meaningless because its effectiveness against the cost of an attack is small.

Ackonwledgement

The Zoo Farming Team confirmed the vulnerability, and resolved the issue by using offchain oracle to provide random seed for every each NFT mint request.

Appendix A - Files in Scope

File	SHA-1 Hash
NFT/ZooNFT.sol	445c6b8a4fd5b353e422fe48da46c64c55637ac2
farming/ZooKeeperFarming.sol	d091345ceb5ab0052069fb0e735a886e7680cdc5
token/ZooToken.sol	3b3430045e3b8dbf3a8c1aa40105f2f098a9e424

Appendix B - Test Results

```
Contract: ZooNFT
  ✓ should success when set factory
  ✓ should failed when set factory without access
  ✓ should success when setURI
  ✓ should failed when setURI without access
  ✓ should success when getURI
  ✓ should empty when getURI without set
  ✓ should success when mint
  ✓ should failed when mint without access
  ✓ should success when getBoosting
  ✓ should 1e12 when getBoosting non-token
  ✓ should success when getTokenURI
  ✓ should failed when getTokenURI non token
  ✓ should success when getTokenInfo
  ✓ should 0 when getTokenInfo non token
  ✓ should success when setMultiNftURI
  ✓ should failed when setMultiNftURI without access

Contract: ZooToken
  ✓ should success when mint
  ✓ should failed when mint without permission
  ✓ should success when burn
  ✓ should failed when burn out of balance
  ✓ should success when transferOwner
  ✓ should failed when transferOwner without access

Contract: ZooKeeperFarming
  ✓ should success when transferOwner
  ✓ should failed when transferOwner without access
  ✓ should success when add pool
  ✓ should failed when add pool without access
  ✓ should success when update pool
  ✓ should failed when update pool without access
  ✓ should success when enable/disable dual farming
  ✓ should failed when enable/disable dual farming without access
  ✓ should success when deposit 0
  ✓ should success when deposit amount
  ✓ should success when pendingZoo
  ✓ should success when withdraw 0
  ✓ should success when withdraw amount
  ✓ should success when farming amount
  ✓ should success when multi pool farming 1
  ✓ should success when multi pool farming 2
  ✓ should success when deposit 0 with dual farming
  ✓ should success when deposit amount with dual farming
  ✓ should success when pendingZoo with dual farming
  ✓ should success when pendingWasp with dual farming
  ✓ should success when withdraw 0 with dual farming
  ✓ should success when withdraw amount with dual farming
  ✓ should success when deposit 0 with lock-time
  ✓ should success when deposit 0 with lock longer
  ✓ should success when deposit amount with lock-time
  ✓ should success when deposit amount with lock longer
  ✓ should success when deposit amount no-lock to lock
  ✓ should success when withdraw 0 with lock time
  ✓ should success when withdraw amount with lock time 1
  ✓ should success when withdraw amount with lock time 2
```

```
      ✓ should success when withdraw amount no-lock to lock 1
      ✓ should success when withdraw amount no-lock to lock 2
      ✓ should success when deposit 0 with NFT
      ✓ should success when deposit amount with NFT
      ✓ should success when deposit 0 no nft to nft
      ✓ should success when deposit amount no nft to nft
      ✓ should success when withdraw 0 with nft
      ✓ should success when withdraw 0 with nft
      ✓ deposit 0 with nft,lock-time,dual farming
      ✓ deposit amount with nft,lock-time,dual farming
      ✓ withdraw 0 with nft,lock-time,dual farming
      ✓ withdraw amount with nft,lock-time,dual farming
      ✓ team zoo test
      ✓ should success when owner emergencyWithdraw
      ✓ should failed when user emergencyWithdraw without access
```

File	% Stmts	% Branch	% Funcs	% Lines
NFT/ZooNFT.sol	100	85.71	100	100
farming/ZooKeeperFarming.sol	86.63	68.92	80	86.63
token/ZooToken.sol	100	100	100	100