Security Audit Report

Bndswap_BND smart contract

Audit Team：IOSIRO security team

Official Web：https://iosiro.com

Email: hello@iosiro.com

Audit Date：April 25, 2021

BND Smart Contract Security Audit Report

1. Overview

On April 24, 2021 the security team of IOSIRO security received the security audit request of the **Bndswap project**. The team will conduct a report on the **BND smart contract** from April 24, 2021 to April 25, 2021. During the audit process, the security audit experts of IOSIRO security team communicate with the relevant interface people of the Bndswap project, maintain information symmetry, conduct security audits under controllable operational risks, and try to avoid project generation and operation during the test process. Cause risks.
Through communicate and feedback with Bndswap project party, it is confirmed that the loopholes and risks found in the audit process have been repaired or within the acceptable range.

The result of this BND smart contract security audit: passed.

Audit Report MD5：0X002104250001

2. Background

2.1 Project Description

- Project name: Bndswap
- official website: https://Bndswap.com
- Contract type: DeFi Token contract
- Code language: Solidity

2.2 Audit Range

Bndswap official chain token contract :

0x0Fe5EA4b0179Cd4AB5bE142D41fd63A1a78fa552

2.3 Security Audit List

The security experts of IOSIRO security team conduct security audits on the security audit list within the agreement, The scope of this smart contract security audit does not include new attack methods that may appear in the future, does not include the code after contract upgrades or tampering, and is not included in the subsequent cross-country, does not include cross-chain deployment, does not include project front-end code security and project platform server security.

This smart contract security audit list includes the following:

- Integer overflow
- Reentry attack
- Floating point numbers and numerical precision
- Default visibility
- Tx.origin authentication
- Wrong constructor
- Return value not verified
- Insecure random numbers
- Timestamp dependency
- Transaction order is dependent
- Delegatecall
- Call
- Denial of service
- Logic design flaws
- Fake recharge vulnerability
- Short address attack
- Uninitialized storage pointer
- Additional token issuance
- Frozen account bypass
- Access control
- Gas usage

3. Contract Structure Analysis

3.1 Directory Structure

```
└── Bndswap
    Farm.sol
    lp.sol
    MDX-USDT-LP.sol
    TimelockController.sol
```

3.2 token contract

Contract

token

ERC20Burnable

- burn(uint256 amount)
- burnFrom(address account, uint256 amount)

ERC20

- name()
- symbol()
- decimals()
- totalSupply()

- balanceOf(address account)
- transfer(address recipient, uint256 amount)
- allowance(address owner, address spender)
- approve(address spender, uint256 amount)
- transferFrom(address sender, address recipient, uint256 amount)
- increaseAllowance(address spender, uint256 addedValue)
- decreaseAllowance(address spender, uint256 subtractedValue)
- _transfer(address sender, address recipient, uint256 amount)
- _mint(address account, uint256 amount)
- _burn(address account, uint256 amount)
- _approve(address owner, address spender, uint256 amount)
- *setupDecimals(uint8 decimals*)
- _beforeTokenTransfer(address from, address to, uint256 amount)

Context

- _msgSender()
- _msgData()

Ownable

- owner()
- renounceOwnership()
- transferOwnership(address newOwner)

Operator

- operator()
- isOperator()
- transferOperator(address newOperator_)
- *transferOperator(address newOperator*)

Interface

IERC20

- totalSupply()
- balanceOf(address account)
- transfer(address recipient, uint256 amount)
- allowance(address owner, address spender)
- approve(address spender, uint256 amount)
- transferFrom(address sender, address recipient, uint256 amount)

Library

Address

- isContract(address account)
- sendValue(address payable recipient, uint256 amount)functionCall(address target, bytes memory data)
- functionCall(address target, bytes memory data, string memory errorMessage)
- functionCallWithValue(address target, bytes memory data, uint256 value)
- functionCallWithValue(address target, bytes memory data, uint256 value, string memory
- errorMessage)
- _functionCallWithValue(address target, bytes memory data, uint256 weiValue, string
- memory errorMessage)

SafeMath

3.3 lp contract

Contract

Context

- _msgSender()
- _msgData()

Ownable

- owner()
- renounceOwnership()
- transferOwnership(address newOwner)

LPTokenWrapper

- totalSupply()
- balanceOf(address account)
- stake(uint256 amount)
- withdraw(uint256 amount)

LPTokenSharePool

- setStartTime(uint256 starttime_)
- updateReward(address account)
- lastTimeRewardApplicable()
- rewardPerToken()
- earned(address account)
- stake(uint256 amount)
- withdraw(uint256 amount)
- exit()
- getReward()

Interface

IERC20

- totalSupply()
- balanceOf(address account)
- transfer(address recipient, uint256 amount)
- allowance(address owner, address spender)
- approve(address spender, uint256 amount)
- transferFrom(address sender, address recipient, uint256 amount)

Library

Address

- isContract(address account)
- sendValue(address payable recipient, uint256 amount)
- functionCall(address target, bytes memory data)
- functionCall(address target, bytes memory data, string memory errorMessage)
- functionCallWithValue(address target, bytes memory data, uint256 value)
- functionCallWithValue(address target, bytes memory data, uint256 value, string memory
- errorMessage)

- _functionCallWithValue(address target, bytes memory data, uint256 weiValue, string
- memory errorMessage)

Math

SafeMath

SafeERC20

3.4 Farm contract

Contract

Context

- _msgSender()
- _msgData()

ERC20

- name()
- symbol()
- decimals()
- totalSupply()
- balanceOf(address account)
- transfer(address recipient, uint256 amount)
- allowance(address owner, address spender)
- approve(address spender, uint256 amount)
- transferFrom(address sender, address recipient, uint256 amount)
- increaseAllowance(address spender, uint256 addedValue)
- decreaseAllowance(address spender, uint256 subtractedValue)
- _transfer(address sender, address recipient, uint256 amount)
- _mint(address account, uint256 amount)
- _burn(address account, uint256 amount)
- _approve(address owner, address spender, uint256 amount)
- *setupDecimals(uint8 decimals*)
- _beforeTokenTransfer(address from, address to, uint256 amount)

Ownable

- owner()
- renounceOwnership()
- transferOwnership(address newOwner)

Farm

- poolLength()
- add(uint256 _allocPoint,IERC20 _want,bool _withUpdate,address _strat)
- stakedWantTokens(uint256 _pid, address _user)
- stake(uint256 _pid, uint256 _wantAmt)withdraw(uint256 _pid, uint256 _wantAmt)
- withdrawAll(uint256 _pid)
- massUpdatePools()
- updatePool(uint256 _pid)
- emergencyWithdraw(uint256 _pid)
- inCaseTokensGetStuck(address _token, uint256 _amount)

Interface

IERC20

- totalSupply()
- balanceOf(address account)
- transfer(address recipient, uint256 amount)
- allowance(address owner, address spender)
- approve(address spender, uint256 amount)
- transferFrom(address sender, address recipient, uint256 amount)

IStrategy

- wantLockedTotal()
- sharesTotal()
- earn()
- deposit(address _userAddress, uint256 _wantAmt)
- withdraw(address _userAddress, uint256 _wantAmt)
- inCaseTokensGetStuck(address _token,uint256 _amount,address _to)

Library

Address

- isContract(address account)
- sendValue(address payable recipient, uint256 amount)
- functionCall(address target, bytes memory data)
- functionCall(address target, bytes memory data, string memory errorMessage)
- functionCallWithValue(address target, bytes memory data, uint256 value)
- functionCallWithValue(address target, bytes memory data, uint256 value, string memory
- errorMessage)
- _functionCallWithValue(address target, bytes memory data, uint256 weiValue, string
- memory errorMessage)

EnumerableSet

- _add(Set storage set, bytes32 value)
- _remove(Set storage set, bytes32 value)
- _contains(Set storage set, bytes32 value)
- _length(Set storage set)
- _at(Set storage set, uint256 index)
- add(Bytes32Set storage set, bytes32 value)
- remove(Bytes32Set storage set, bytes32 value)
- contains(Bytes32Set storage set, bytes32 value)
- length(Bytes32Set storage set)
- at(Bytes32Set storage set, uint256 index)
- add(AddressSet storage set, address value)
- remove(AddressSet storage set, address value)
- contains(AddressSet storage set, address value)length(AddressSet storage set)
- at(AddressSet storage set, uint256 index)
- add(UintSet storage set, uint256 value)
- remove(UintSet storage set, uint256 value)
- contains(UintSet storage set, uint256 value)
- length(UintSet storage set)
- at(UintSet storage set, uint256 index)

SafeMath

SafeERC20

3.5 TimelockController contract

Contract

Context

- _msgSender()
- _msgData()

AccessControl

- hasRole(bytes32 role, address account)
- getRoleMemberCount(bytes32 role)
- getRoleMember(bytes32 role, uint256 index)
- getRoleAdmin(bytes32 role)
- grantRole(bytes32 role, address account)
- revokeRole(bytes32 role, address account)
- renounceRole(bytes32 role, address account)
- _setupRole(bytes32 role, address account)
- _setRoleAdmin(bytes32 role, bytes32 adminRole)
- _grantRole(bytes32 role, address account)
- _revokeRole(bytes32 role, address account)

Ownable

- owner()
- renounceOwnership()
- transferOwnership(address newOwner)

LPTokenWrapper

- totalSupply()
- balanceOf(address account)
- stake(uint256 amount)
- withdraw(uint256 amount)

LPTokenSharePool

- setStartTime(uint256 starttime_)
- updateReward(address account)
- lastTimeRewardApplicable()
- rewardPerToken()
- earned(address account)
- stake(uint256 amount)
- withdraw(uint256 amount)
- exit()getReward()

TimelockController

- isOperationPending(bytes32 id)
- isOperationReady(bytes32 id)
- isOperationDone(bytes32 id)
- getTimestamp(bytes32 id)
- getMinDelay()
- hashOperation(address target,uint256 value,bytes calldata data,bytes32

- predecessor,bytes32 salt)
- hashOperationBatch(address[] calldata targets,uint256[] calldata values,bytes[] calldata
- datas,bytes32 predecessor,bytes32 salt)
- schedule(address target,uint256 value,bytes calldata data,bytes32 predecessor,bytes32
- salt,uint256 delay)
- scheduleBatch(address[] calldata targets,uint256[] calldata values,bytes[] calldata
- datas,bytes32 predecessor,bytes32 salt,uint256 delay)
- _schedule(bytes32 id, uint256 delay)
- cancel(bytes32 id)
- execute(address target,uint256 value,bytes calldata data,bytes32 predecessor,bytes32 salt)
- executeBatch(address[] calldata targets,uint256[] calldata values,bytes[] calldata
- datas,bytes32 predecessor,bytes32 salt)
- _beforeCall(bytes32 predecessor)
- _afterCall(bytes32 id)
- _call(bytes32 id,uint256 index,address target,uint256 value,bytes calldata data)
- updateMinDelay(uint256 newDelay)
- updateMinDelayReduced(uint256 newDelay)
- setDevWalletAddress(address payable _devWalletAddress)
- scheduleSet(address _autofarmAddress,uint256 _pid,uint256 _allocPoint,bool
- _withUpdate,bytes32 predecessor,bytes32 salt)
- executeSet(address _autofarmAddress,uint256 _pid,uint256 _allocPoint,bool
- _withUpdate,bytes32 predecessor,bytes32 salt)
- withdrawBNB()
- withdrawBEP20(address _tokenAddress)
- add(address _autofarmAddress,address _want,bool _withUpdate,address _strat)
- earn(address _stratAddress)
- farm(address _stratAddress)
- pause(address _stratAddress)
- unpause(address _stratAddress)
- rebalance(address _stratAddress,uint256 _borrowRate,uint256 _borrowDepth)
- deleverageOnce(address _stratAddress)
- wrapBNB(address _stratAddress)
- noTimeLockFunc1(address _stratAddress)
- noTimeLockFunc2(address _stratAddress)
- noTimeLockFunc3(address _stratAddress)

Interface

IERC20

- totalSupply()
- balanceOf(address account)
- transfer(address recipient, uint256 amount)
- allowance(address owner, address spender)approve(address spender, uint256 amount)
- transferFrom(address sender, address recipient, uint256 amount)

IAutoFarm

- add(uint256 _allocPoint,address _want,bool _withUpdate,address _strat)
- set(uint256 _pid,uint256 _allocPoint,bool _withUpdate)

IStrategy

- earn()
- farm()
- pause()
- unpause()
- rebalance(uint256 _borrowRate, uint256 _borrowDepth)
- deleverageOnce()
- wrapBNB()
- noTimeLockFunc1()
- noTimeLockFunc2()
- noTimeLockFunc3()

Library

Address

- isContract(address account)
- sendValue(address payable recipient, uint256 amount)
- functionCall(address target, bytes memory data)
- functionCall(address target, bytes memory data, string memory errorMessage)
- functionCallWithValue(address target, bytes memory data, uint256 value)
- functionCallWithValue(address target, bytes memory data, uint256 value, string memory
- errorMessage)
- _functionCallWithValue(address target, bytes memory data, uint256 weiValue, string
- memory errorMessage)

EnumerableSet

- _add(Set storage set, bytes32 value)
- _remove(Set storage set, bytes32 value)
- _contains(Set storage set, bytes32 value)
- _length(Set storage set)
- _at(Set storage set, uint256 index)
- add(Bytes32Set storage set, bytes32 value)
- remove(Bytes32Set storage set, bytes32 value)
- contains(Bytes32Set storage set, bytes32 value)
- length(Bytes32Set storage set)
- at(Bytes32Set storage set, uint256 index)
- add(AddressSet storage set, address value)
- remove(AddressSet storage set, address value)
- contains(AddressSet storage set, address value)
- length(AddressSet storage set)
- at(AddressSet storage set, uint256 index)
- add(UintSet storage set, uint256 value)
- remove(UintSet storage set, uint256 value)
- contains(UintSet storage set, uint256 value)
- length(UintSet storage set)at(UintSet storage set, uint256 index)

SafeMath

SafeERC20

3.6 MDX-USDT-LP contract

Contract

Context

_msgSender()

_msgData()

ERC20

- name()
- symbol()
- decimals()
- totalSupply()
- balanceOf(address account)
- transfer(address recipient, uint256 amount)
- allowance(address owner, address spender)
- approve(address spender, uint256 amount)
- transferFrom(address sender, address recipient, uint256 amount)
- increaseAllowance(address spender, uint256 addedValue)
- decreaseAllowance(address spender, uint256 subtractedValue)
- _transfer(address sender, address recipient, uint256 amount)
- _mint(address account, uint256 amount)
- _burn(address account, uint256 amount)
- _approve(address owner, address spender, uint256 amount)
- *setupDecimals(uint8 decimals*)
- _beforeTokenTransfer(address from, address to, uint256 amount)

Ownable

- owner()
- renounceOwnership()
- transferOwnership(address newOwner)

Pausable

- paused()
- _pause()
- _unpause()

StratX

- deposit(address _userAddress, uint256 _wantAmt)
- farm()
- _farm()
- withdraw(address _userAddress, uint256 _wantAmt)
- earn()
- buyBack(uint256 _earnedAmt)
- distributeFees(uint256 _earnedAmt)
- convertDustToEarned()
- pause()unpause()
- setEntranceFeeFactor(uint256 _entranceFeeFactor)
- setControllerFee(uint256 _controllerFee)
- setbuyBackRate(uint256 _buyBackRate)

- setGov(address _govAddress)
- setOnlyGov(bool _onlyGov)
- setRewardsMigratorAddress(address _rewardsMigratorAddress)
- inCaseTokensGetStuck(address _token,uint256 _amount,address _to)

Interface

IERC20

- totalSupply()
- balanceOf(address account)
- transfer(address recipient, uint256 amount)
- allowance(address owner, address spender)
- approve(address spender, uint256 amount)
- transferFrom(address sender, address recipient, uint256 amount)

IPancakeswapFarm

- poolLength()
- userInfo()
- getMultiplier(uint256 _from, uint256 _to)
- pendingCake(uint256 _pid, address _user)
- deposit(uint256 _pid, uint256 _amount)
- withdraw(uint256 _pid, uint256 _amount)
- enterStaking(uint256 _amount)
- leaveStaking(uint256 _amount)
- emergencyWithdraw(uint256 _pid)

IPancakeRouter01

- factory()
- WETH()
- addLiquidity(address tokenA,address tokenB,uint256 amountADesired,uint256
- amountBDesired,uint256 amountAMin,uint256 amountBMin,address to,uint256 deadline)
- addLiquidityETH(address token,uint256 amountTokenDesired,uint256
- amountTokenMin,uint256 amountETHMin,address to,uint256 deadline)
- removeLiquidity(address tokenA,address tokenB,uint256 liquidity,uint256
- amountAMin,uint256 amountBMin,address to,uint256 deadline)
- removeLiquidityETH(address token,uint256 liquidity,uint256 amountTokenMin,uint256
- amountETHMin,address to,uint256 deadline)
- removeLiquidityWithPermit(address tokenA,address tokenB,uint256 liquidity,uint256
- amountAMin,uint256 amountBMin,address to,uint256 deadline,bool approveMax,uint8
- v,bytes32 r,bytes32 s)
- removeLiquidityETHWithPermit(address token,uint256 liquidity,uint256
- amountTokenMin,uint256 amountETHMin,address to,uint256 deadline,bool
- approveMax,uint8 v,bytes32 r,bytes32 s)
- swapExactTokensForTokens(uint256 amountIn,uint256 amountOutMin,address[] calldata
- path,address to,uint256 deadline)
- swapTokensForExactTokens(uint256 amountOut,uint256 amountInMax,address[] calldata
- path,address to,uint256 deadline)swapExactETHForTokens(uint256 amountOutMin,address[] calldata path,address to,uint256
- deadline)

- swapTokensForExactETH(uint256 amountOut,uint256 amountInMax,address[] calldata
- path,address to,uint256 deadline)
- swapExactTokensForETH(uint256 amountIn,uint256 amountOutMin,address[] calldata
- path,address to,uint256 deadline)
- swapETHForExactTokens(uint256 amountOut,address[] calldata path,address to,uint256
- deadline)
- quote(uint256 amountA,uint256 reserveA,uint256 reserveB)
- getAmountOut(uint256 amountIn,uint256 reserveIn,uint256 reserveOut)
- getAmountIn(uint256 amountOut,uint256 reserveIn,uint256 reserveOut)
- getAmountsOut(uint256 amountIn, address[] calldata path)
- getAmountsIn(uint256 amountOut, address[] calldata path)

IPancakeRouter02

- removeLiquidityETHSupportingFeeOnTransferTokens(address token,uint256
- liquidity,uint256 amountTokenMin,uint256 amountETHMin,address to,uint256 deadline)
- removeLiquidityETHWithPermitSupportingFeeOnTransferTokens(address token,uint256
- liquidity,uint256 amountTokenMin,uint256 amountETHMin,address to,uint256 deadline,bool
- approveMax,uint8 v,bytes32 r,bytes32 s)
- swapExactTokensForTokensSupportingFeeOnTransferTokens(uint256 amountIn,uint256
- amountOutMin,address[] calldata path,address to,uint256 deadline)
- swapExactETHForTokensSupportingFeeOnTransferTokens(uint256 amountOutMin,address[]
- calldata path,address to,uint256 deadline)
- swapExactTokensForETHSupportingFeeOnTransferTokens(uint256 amountIn,uint256
- amountOutMin,address[] calldata path,address to,uint256 deadline)

Library

Address

- isContract(address account)
- sendValue(address payable recipient, uint256 amount)
- functionCall(address target, bytes memory data)
- functionCall(address target, bytes memory data, string memory errorMessage)
- functionCallWithValue(address target, bytes memory data, uint256 value)
- functionCallWithValue(address target, bytes memory data, uint256 value, string memory
- errorMessage)
- _functionCallWithValue(address target, bytes memory data, uint256 weiValue, string
- memory errorMessage)

EnumerableSet

- _add(Set storage set, bytes32 value)
- _remove(Set storage set, bytes32 value)
- _contains(Set storage set, bytes32 value)
- _length(Set storage set)
- _at(Set storage set, uint256 index)
- add(Bytes32Set storage set, bytes32 value)
- remove(Bytes32Set storage set, bytes32 value)
- contains(Bytes32Set storage set, bytes32 value)
- length(Bytes32Set storage set)
- at(Bytes32Set storage set, uint256 index)

- add(AddressSet storage set, address value)
- remove(AddressSet storage set, address value)
- contains(AddressSet storage set, address value)
- length(AddressSet storage set)
- at(AddressSet storage set, uint256 index)
- add(UintSet storage set, uint256 value)
- remove(UintSet storage set, uint256 value)
- contains(UintSet storage set, uint256 value)
- length(UintSet storage set)
- at(UintSet storage set, uint256 index)

SafeMath

SafeERC20

4. Audit Details

4.1 Vulnerabilities Distribution

Vulnerabilities in this security audit are distributed by risk level, as follows：

This smart contract security audit has:
0 high-risk vulnerabilities,
0 medium-risk vulnerabilities,
0 low-risk vulnerabilities, and 21 passed, **with a high security level.**

4.2 Vulnerabilities Details

A security audit was conducted on the smart contract within the agreement, and no security vulnerabilities that could be directly exploited and generated security problems were found, and the security audit was passed.

4.3 Other Risks

Related issues and risks have been communicated with the official confirmation, the risks have been repaired or within the tolerable range, there are no serious risk issues.

5. Vulnerability assessment criteria

Disclaimer：

IOSIRO security team only issues a report and assumes corresponding responsibilities for the facts that occurred or existed before the issuance of this report, Since the facts that occurred after the issuance of the report cannot determine the security status of the smart contract, it is not responsible for this.
IOSIRO security team conducts security audits on the security audit items in the project agreement, and is not responsible for the project background and other circumstances, The subsequent on-chain deployment and operation methods of the project party are beyond the scope of this audit.

This report only conducts a security audit based on the information provided by the information provider to IOSIRO security at the time the report is issued, If the information of this project is concealed or the situation reflected is inconsistent with the actual situation, IOSIRO security team shall not be liable for any losses and adverse effects caused thereby.

iosiro

Security Audit Report

Audit Team：IOSIRO security team

Official Web：https://iosiro.com

Email: hello@iosiro.com

Audit Date：April 25, 2021