Coinsult

Advanced Manual Smart Contract Audit

Project: Mobipad Fairlaunch

Website: https://mobipad.io

Low-Risk	Medium-Risk	High-Risk
3 low-risk code issues found	2 medium-risk code issues found	0 high-risk code issues found

Contract Address

0xEb79D22c3a15e51B34e444D507ff941F398D73C9

Disclaimer

Coinsult is not responsible if a project turns out to be a scam, rug-pull or honeypot. We only provide a detailed analysis for your own research.

Coinsult is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

The information provided in this audit is for informational purposes only and should not be considered investment advice. Coinsult does not endorse, recommend, support or suggest to invest in any project.

Coinsult can not be held responsible for when a project turns out to be a rug-pull, honeypot or scam.

Tokenomics

-

Source Code

Coinsult was comissioned by Mobipad Fairlaunch to perform an audit based on the following smart contract:

https://bscscan.com/address/0xEb79D22c3a15e51B34e444D507ff941F398D73C9#code

Fairlaunch Contract

Manual Code Review

In this audit report we will highlight all these issues:

🟢 Low-Risk

3 low-risk code
issues found

🟡 Medium-Risk

2 medium-risk code
issues found

🔴 High-Risk

0 high-risk code
issues found

The detailed report continues on the next page...

🟢 **Low-Risk:** Could be fixed, will not bring problems.

Too many digits

Literals with many digits are difficult to read and review.

```
uint256 private poolSupply = 24000000000000000000000000; // 24m Max token supply in fairlaunch [Pool
```

Recommendation

Use: Ether suffix, Time suffix, or The scientific notation

Exploit scenario

```
contract MyContract{
    uint 1_ether = 10000000000000000000;
}
```

While `1_ether` looks like `1 ether`, it is `10 ether`. As a result, it's likely to be used incorrectly.

🟢 **Low-Risk:** Could be fixed, will not bring problems.

Missing events arithmetic

Detect missing events for critical arithmetic parameters.

```
function setWithdrawalAddress(address payable _addr) external onlyOwner {
    WITHDRAWAL_ADDRESS = _addr;
}
```

Recommendation

Emit an event for critical parameter changes.

Exploit scenario

```
contract C {

  modifier onlyAdmin {
    if (msg.sender != owner) throw;
    _;
  }

  function updateOwner(address newOwner) onlyAdmin external {
    owner = newOwner;
  }
}
```

`updateOwner()` has no event, so it is difficult to track off-chain changes in the buy price.

🟢 **Low-Risk:** Could be fixed, will not bring problems.

Conformance to Solidity naming conventions

Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
bool private sale_enabled = false;

bool private claim_enabled = false;

bool private refund_enabled = false;
bool private refund_disabled_forever = false; // auto true when claim enabled

bool private vesting_1_enabled = false;
bool private vesting_2_enabled = false;
bool private vesting_3_enabled = false;

uint256 private vesting_1 = 20; // 20%
uint256 private vesting_2 = 40; // 40%
uint256 private vesting_3 = 40; // 40%
```

Recommendation

Follow the Solidity naming convention.

Rule exceptions

- Allow constant variable name/symbol/decimals to be lowercase (`ERC20`).
- Allow _ at the beginning of the `mixed_case` match for private variables and unused parameters.

🟡 **Medium-Risk:** Should be fixed, could bring problems.

referral_count can be greater than 1 for the same address (🟢 Acknowledged)

```
referral_count[referrer] = referral_count[referrer].add(1);
```

Recommendation

(🟢 Acknowledged) Using this configuration, the referral_count can be greater than 1 if the user contributes twice, using the same addresses. This will not directly have effects on the contract, but if you have social incentives concerning the referral count, people can abuse this by contributing low amounts with the same addresses to increase this number.

🟡 **Medium-Risk:** Should be fixed, could bring problems.

Unable to claim previous vest during vesting schedule 2 (🟢 Acknowledged)

```
function setVesting2Enabled(bool _enabled) external onlyOwner {
    if (_enabled == true) {
        vesting_1_enabled = false;
        vesting_3_enabled = false;
    }
    vesting_2_enabled = _enabled;
}
```

Recommendation

(🟢 Acknowledged) No need to disable previous vesting schedules when moving to a new vesting period. This allows investors who could not claim their vest during previous periods to still claim their bought tokens.

Owner privileges

⚠️ Owner can enable or disable the sale

⚠️ Owner can set claiming period enabled or disabled

⚠️ Owner can change the referral percentage without any constraints

Extra notes by the team

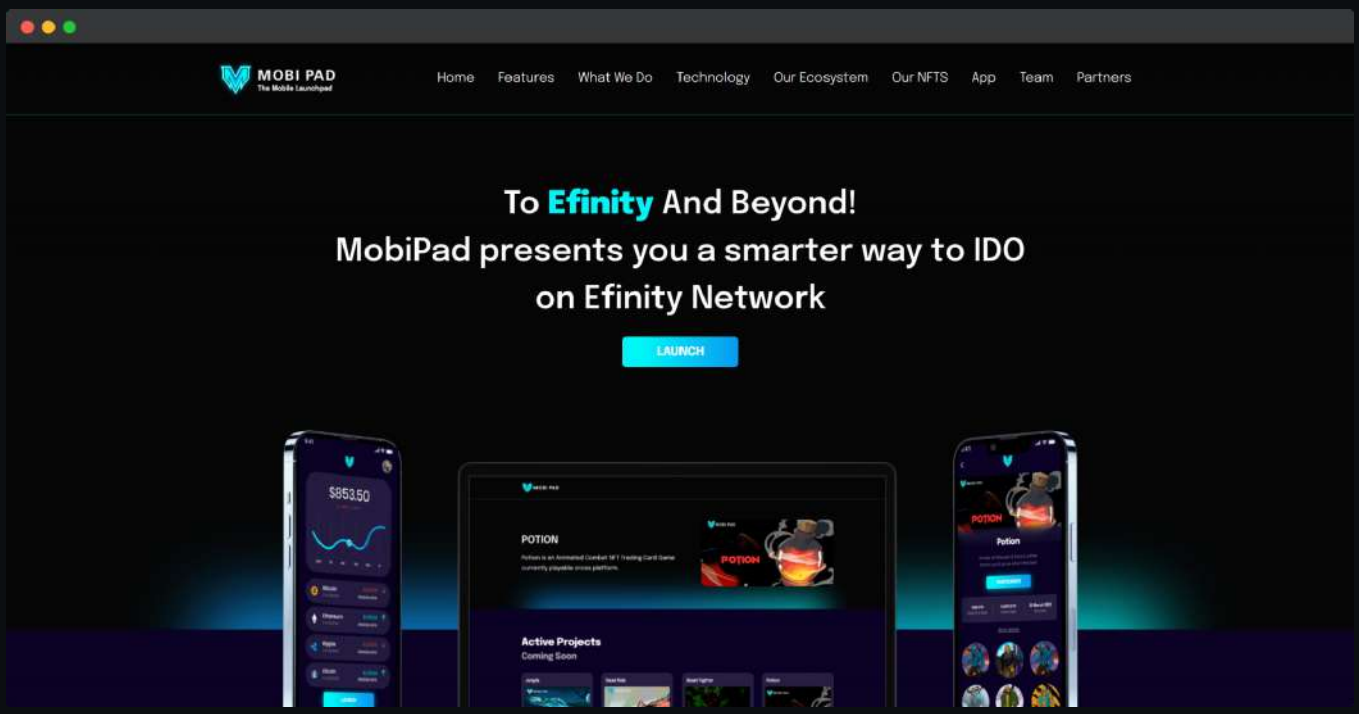
No notes

Contract Snapshot

```
contract MBPFairlaunch is Context, Ownable {
using SafeMath for uint256;

constructor() public {}

// Decimal is 18
uint256 private poolSupply = 24000000000000000000000000; // 24m Max token supply in fairlaunch [Pool
uint256 private totalBnbInvested = 0; // Total BNB in fairlaunch //same as address(this).balance

IMbpToken public MBP_CONTRACT;

function defineToken(address _mbpToken) external onlyOwner {
    MBP_CONTRACT = IMbpToken(_mbpToken);
}

bool private sale_enabled = false;

bool private claim_enabled = false;

bool private refund_enabled = false;
bool private refund_disabled_forever = false; // auto true when claim enabled

bool private vesting_1_enabled = false;
bool private vesting_2_enabled = false;
bool private vesting_3_enabled = false;

uint256 private vesting_1 = 20; // 20%
uint256 private vesting_2 = 40; // 40%
uint256 private vesting_3 = 40; // 40%

address payable WITHDRAWAL_ADDRESS =
    0x7578dFe7a8F2cb1B45B9758b4445F19E0Ae53b61;

function getPoolSupply() external view returns (uint256) {
    return poolSupply;
}
```

Website Review

Coinsult checks the website completely manually and looks for visual, technical and textual errors. We also look at the security, speed and accessibility of the website. In short, a complete check to see if the website meets the current standard of the web development industry.



- Mobile Friendly
- Does not contain jQuery errors
- SSL Secured
- No major spelling errors

Project Overview

KYC verified by Coinsult