

近日，FAIRWIN 智能合约存在漏洞这一问题引起各方关注，FAIRWIN 作为近日以太坊链上交易量最高的资金盘模式应用，在以太坊链上还存在大量类似的克隆盘，如果存在隐藏漏洞会给公链带来较大风向，因此成都链安安全人员对FAIRWIN智能合约展开了深度分析，分析结果如下：

通过对FAIRWIN合约代码进行审计，我们发现其合约存在一个remedy()接口，如果合约owner没有通过close()关闭接口时，该接口可以被任意用户调用，并且可以通过这个接口伪造投注数据，实现“无中生有”，在不使用任何资金的情况下伪造了充值记录，之后攻击者便可以享受分红，或者通过userWithdraw()将余额全部提出。

Transaction Hash: 0xfd0a7be6e4ced944c46d15c26140f61cedcd499821622b2a316a70f514262f35

Status: Success

Block: 8239759 (390008 Block Confirmations)

Timestamp: 60 days 17 hrs ago (Jul-28-2019 02:55:12 PM +UTC)

From: 0xcb104fa25a1a46040dbab9f554ff564ce325668b

To: Contract 0x01eacc3ae59ee7fbbc191d63e8e1ccfdac11628c

Value: 0 Ether (\$0.00)

Transaction Fee: 0.000208475 Ether (\$0.03)

Gas Limit: 41,695

Gas Used by Transaction: 41,695 (100%)

Gas Price: 0.000000005 Ether (5 Gwei)

Nonce: 2121 (Position: 46)

Input Data: Function: closeAct(), MethodID: 0x0649df31

```
function remedy(address userAddress ,uint freezeAmount,string inviteCode,string beInvitedCode ,uint freeAmount,uint times) public {
    require(actStu == 0,"this action was closed");
    freezeAmount = freezeAmount * ethWei;
    freeAmount = freeAmount * ethWei;
    uint level =util.getlevel(freezeAmount);
    uint lineLevel = util.getLineLevel(freezeAmount + freeAmount);
    if(beginTime==1 && freezeAmount > 0){
        Invest memory invest = Invest(userAddress,freezeAmount,now, inviteCode, beInvitedCode ,1,1,times);
        invests.push(invest);
    }
}
```

通过链上记录，我们发现项目方已于2019年7月28日(合约上线第二天)通过closeAct()关闭了该接口。通过成都链安Beosin-AML系统分析项目方所有的交易记录，我

Transaction Hash: [0xff446de94a6f269bb5b3d6ffda6de0a657a5c93ac02b7d056ed27936a4ee9ea](#)

Status: Success

Block: [8291285](#) 338996 Block Confirmations

Timestamp: ⌚ 52 days 19 hrs ago (Aug-05-2019 02:54:51 PM +UTC)

From: [0x3017cdca109d03414ad54e6d6bcd226948fd104a](#)

To: [Contract 0x01eacc3ae59ee78bc191d63e8e1cddac11628c](#)
↳ TRANSFER 9 Ether From 0x01eacc3ae59ee78bc19... To => 0x3017cdca109d03414ad...

Value: 0 Ether (\$0.00)

Transaction Fee: 0.00131244 Ether (\$0.22)

Gas Limit: 158,486

Gas Used by Transaction: 131,244 (82.81%)

Gas Price: 0.00000001 Ether (10 Gwei)

Nonce: Position 28 68

Input Data:
Function: userWithdraw(address userAddress)
MethodID: 0xa8cef00f
[0]: 00000000000000000000000000000000000000000000000000000000000000003017cdca109d03414ad54e6d6bcd226948fd104a

通过进一步分析其合约部署情况发现，在项目方关闭actStu的前一天，也就是2019年7月27日，项目方刚刚部署FAIRWIN合约，在短短一天时间不到之内，项目合约之内便无中生有了5000多个ETH。
7月29日，以太坊浏览器显示合约进行了开源。

Transactions Internal Txns Erc20 Token Txns **Contract** Events Analytics Comments

Code Read Contract Write Contract

✔ Contract Source Code Verified (Exact Match) ⚠

Contract Name: FairWin Optimization Enabled: No with 200 runs

Compiler Version: v0.4.24+commit.e67f0147 Other Settings: default evmVersion, None license

Contract Source Code (Solidity) Similar Outline Sol2Uml NEW ⌕ 🔄

```
1 /**  
2  *Submitted for verification at Etherscan.io on 2019-07-29  
3  */  
4  
5 pragma solidity ^0.4.24;  
6  
7 contract UtilFairWin {  
8  
9     /* fairwin.me */  
10  
11     function getRecommendScaleByLevelandTim(uint level,uint times) public view returns(uint);  
12     function compareStr (string _str,string str) public view returns(bool);  
13     function getLineLevel(uint value) public view returns(uint);  
14     function getScByLevel(uint level) public view returns(uint);  
15     function getFireScByLevel(uint level) public view returns(uint);
```