

main

...

SC-RCVD / Vulnerabilities / Doftcoin.md



MRdoulestar update DSC

History

1 contributor

30 lines (20 sloc) | 922 Bytes

...

Doftcoin

<https://etherscan.io/address/0x2eb9cc28c34c6d427aac9f259ee5c4b33f1c4448#code>

Etherscan

Eth: \$2,699.40 (+2.11%) | 10 Gwei

Token Doftcoin

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

Overview (ERC-20)

Max Total Supply:	5,010,647.18858225 DFC
Holders:	36
Transfers:	99

Profile Summary

Contract:	0x2eb9cc28c34c6d427aac9f259ee5c4b33f1c4448
Decimals:	18
Official Site:	https://doft.com/
Social Profiles:	Twitter Facebook Instagram YouTube LinkedIn Medium

Transfers Holders Info Contract Analytics Comments

A total of 99 transactions found

Figure 1. Doftcoin Token Information

Integer Overflow

```
function mintToken(address _target, uint256 _mintedAmount) onlyOwner {
    require (_target != 0x0);

    //ownership will be given to ICO after creation
    balanceOf[_target] += _mintedAmount;
    _totalSupply += _mintedAmount;
    Transfer(0, this, _mintedAmount);
    Transfer(this, _target, _mintedAmount);
}
```

The Integer Overflow vulnerability in mintToken function similar to CVE-2018-11812. This vulnerability allows owner to add token to users. However, the unlimited value can change balance of user to zero (balanceOf[_target] += _mintedAmount;).

Exploit

The screenshot displays the Remix IDE interface. On the left, the Solidity code for the `Doftcoin` contract is visible, with the `mintToken` function highlighted. The function takes an address `_target` and a uint256 `_mintedAmount` as arguments. The right-hand sidebar shows the 'Doftcoin at 0xbbf...732db (memory)' instance. The `mintToken` function is being called with `_target` set to `0x14723a09acff6d2a60dcd7aa4af308fddc1` and `_mintedAmount` set to `5000`. The 'transact' button is highlighted. Below the code editor, the debug console shows the transaction details: `From: 0xca35b7d915458e540ade6068df2f44e8fa733c To: Doftcoin.mintToken(address,uint256) 0xbbf...732db value: 0 wei data: 0x79c...fec79 logs: 2 hash: 0xae6...12508`. The console also shows the state of the contract after the transaction, with `balanceOf` for the target address being `0` and `uint256: balance 5000`.

*Figure 2. The Result of mintToken() to target account.

This screenshot shows the same Remix IDE interface as Figure 2, but with a different target account. The `mintToken` function is called with `_target` set to `0x14723a09acff6d2a60dcd7aa4af308fddc1` and `_mintedAmount` set to `11579208923731619542357098500868790`. The 'transact' button is highlighted. The debug console shows the transaction details: `From: 0xca35b7d915458e540ade6068df2f44e8fa733c To: Doftcoin.mintToken(address,uint256) 0xbbf...732db value: 0 wei data: 0x79c...fec79 logs: 2 hash: 0x2da...d6922`. The console also shows the state of the contract after the transaction, with `balanceOf` for the target address being `0` and `uint256: balance 1`.

*Figure 3. The Result of mintToken() to attack target account!