hellowuzekai Update balance.md History

1 contributor

28 lines (21 sloc) | 1.13 KB

address

https://etherscan.io/address/0xB49E984A83d7A638E7F2889fc8328952BA951AbE#code

vuln

```
function () public payable {
               ...

                if(stageIndex<5 && stageMaxEthAmount>this.balance){
                 //   status = status*10+7;
                    //buys for rest of eth tokens in new prices
                    currS = stageDataStore[stageIndex] ;
                    amountToMint = this.balance*(currS.stagePrice);
                    b.stage = uint128(stageIndex);
                    b.amountOfEth =uint128(this.balance);
                    mintCoins(msg.sender,amountToMint);
                }
                ...
  }
```

In MillionCoin (MON) contract, there is a fallback function here that can cause an overflow.

After this judgment statement of "stageMaxEthAmount>this.balance", "this.balance" can still be increased with the "selfdestruct" function.

If we use the "selfdestruct(MON ADDRESS)" function in another contract to send some Ethereum to this contract after the "stageMaxEthAmount>this.balance", "this.balance" will increase, and "this.balance*(currS.stagePrice)" can cause an overflow.