DENTACOIN

ICORating

Smart Contract Security Audit.

28.08.2017 v0.8

Security

1. Error Level: ERC20 Short Address Attack can be performed on the Dentacoin.
   Check the **msg**.data.length for *Transfer*
   - @Note: This is due to an outdated solidity language version used.

2. Error Level: Contract allows to perform re-entrance attack on *sellDentacoinsAgainstEther* function. Thanks to *safeSub* that safe from the balance draining. We recommend to re-work the function.
   - @Note: Team are going to disable this function to increase security level of the contract. Function *sellDentacoinsAgainstEther* can be disabled by setting price to 0.
   - Warning Level: It would be better to use 'return' from the function instead of 'throw'. It avoids unnecessary gas burn. There is no flag that trading is disabled, user will need to analyze code to understand this.

3. Low Level: Contract executors (mines) can affect the receiver by transactions reordering *(#237 & #240)*
   !msg.sender.send(**gasForDCN**)

4. Warning Level: No chance to suspend & migrate the contract. It may be risky if something goes wrong due the an expected reasons

Code Analysis

1. Warning Level: Use ***revert*** instead of direct ***throw.*** Replace the conditions construction to more gas efficient **require** function:
   e.g if (newOwner == 0x0) throw; replace with require(newOrder == 0x0);
   This is due to old solidity language version used.
2. Warning Level: Check invalid address by ***address(0)*** instead of ***0x0***
3. Warning Level: It would be better if contract will be runnable without active eth balance on it, as it will cause client concerns, because owner is only one who can send additional funds to contract.

4. Low Level: All *SafeMath* functions not allow incoming params with 0 value
   ```
   assert(a == 0 || c / a == b);
   assert(b <= a);
   assert(c>=a && c>=b);
   ```
   All of this case assumes that 0 isn't possible to pass. It may broke some scenarios.
5. Low Level: Contract constructor is better to be payable, because contract cannot work without ether on balance.
6. Warning Level: Solidity language version is outdated, it is recommended to update source code using the latest version.

Testing Results

Contract: DentacoinToken

- ✓ need to have eth balance to work (474ms)
- ✓ should put 8000000000000 DentacoinToken in the first account (47ms)
- ✓ should transfer correctly from owner (279ms)
- ✓ should transfer correctly from participants (298ms)
- ✓ should transfer allowance correctly (523ms)
- ✓ should sell tokens correctly (377ms)
- ✓ should buy tokens correctly (635ms)