callisto

Curate (CUR8) Token

Audit Report

Contents

Curate (CUR8) Token Security Audit Report

1. Summary

Curate (CUR8) Token smart contract security audit report performed by Callisto Security Audit Department

```
Symbol        : CUR8
Name          : Curate
Capped supply: 100,000,000
Decimals      : 8
Standard      : ERC20
```

2. In scope

- CUR8.

3. Findings

In total, **2 issues** were reported including:

- 2 low severity issues.

No critical security issues were found.

3.1. Known vulnerabilities of ERC-20 token

Severity: low

Description

1. It is possible to double withdrawal attack. More details here.
2. Lack of transaction handling mechanism issue. WARNING! This is a very common issue and it already caused millions of dollars losses for lots of token users! More details here.

Recommendation

Add the following code to the `transfer(_to address, ...)` function:

```
require( _to != address(this) );
```

3.2. Burn Mechanism

Severity: low

Description

Transfers to address 0 is used as a basic burn mechanism, however transfer to address zero can also be a result of a mistake by a user or a dapp, devs should take this issue into consideration

Code snippet

```
function transfer(address to, uint tokens) public returns (bool success) {
    balances[msg.sender] = safeSub(balances[msg.sender], tokens);
    balances[to] = safeAdd(balances[to], tokens);
    Transfer(msg.sender, to, tokens);
    return true;
}
```

```
function transferFrom(address from, address to, uint tokens) public returns (bool success)
     {
    balances[from] = safeSub(balances[from], tokens);
    allowed[from][msg.sender] = safeSub(allowed[from][msg.sender], tokens);
    balances[to] = safeAdd(balances[to], tokens);
    Transfer(from, to, tokens);
    return true;
}
```

```
function totalSupply() public constant returns (uint) {
    return _totalSupply  — balances[address(0)];
}
```

4. Conclusion

The audited smart contract can be deployed. Only low severity issues were found during the audit.

5. Revealing audit reports

https://gist.github.com/yuriy77k/5ad87c96038fe675464e03df5a2960a1

https://gist.github.com/yuriy77k/515f895dfb06b566c0a99478a333b0fd

https://gist.github.com/yuriy77k/90fd91fcf6b5f81094af0bfc74ba5054