callisto

XCOYNZ Token Audit Report.

Contents

1. Summary

XCOYNZ token smart contract security audit report performed by Callisto Security Audit Department

2. In scope

- CustomAdmin.sol github commit hash e4535fb03b4621919fba7798a0721111f35f634b.

3. Findings

In total, **3 issues** were reported including:

- 3 low severity issues.

No critical security issues were found.

3.1. Underflow in Transfer function

Severity: low

Description

- If the tokenOwner input not correct value the underflow occurs, in this case the requires in `transfer` function will not work, but transfer will reverted due using SafeMath in the function `_transfer`.
- The values of timestamps must be updated. (23 Jan 2019).

Code snippet

https://github.com/xcoynz/XCZ-Token-Smart_Contract/blob/e4535fb03b4621919fba7798a0721111f35f634b/XCOYNZ%20T
L380

3.2. Owner Privileges

Severity: low

Description

1. The contact code is not guaranteed that the owner will burn tokens after crowdsale, which is not good for investors.
2. The tokenOwner can bypass the restrictions in `transfer` function using functions `approve` and `transferFrom` instead.

Code snippet

https://github.com/xcoynz/XCZ-Token-Smart_Contract/blob/e4535fb03b4621919fba7798a0721111f35f634b/XCOYNZ%20T
L389

https://github.com/xcoynz/XCZ-Token-Smart_Contract/blob/e4535fb03b4621919fba7798a0721111f35f634b/XCOYNZ%20T
L375

https://github.com/xcoynz/XCZ-Token-Smart_Contract/blob/e4535fb03b4621919fba7798a0721111f35f634b/XCOYNZ%20T

https://github.com/xcoynz/XCZ-Token-Smart_Contract/blob/e4535fb03b4621919fba7798a0721111f35f634b/XCOYNZ%20T

3.3. 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 into a function `transfer(address _to, ... )` following code:

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

4. Conclusion

No critical security issues were found in the audited smart contract. But investors have to pay attention to high privileges of token Owner whose could manipulate ICO process.

5. Revealing audit reports

https://gist.github.com/yuriy77k/e01d4429a4a4e62f37b9cc0990eabd2e

https://gist.github.com/yuriy77k/9f2f707f0ba330597ae3ac8e674568be

https://gist.github.com/yuriy77k/df49590bde2835e5f25a327f9f492f6b