callisto

Asure Token Audit

Report

Contents

Asure Token Security Audit Report

1. Summary

Asure Token smart contract security audit report performed by Callisto Security Audit Department

2. In scope

Commit hash 50cfbe81c88ba9be85419cc191298872435c4615.

- TestAsureBonusesCrowdsale.sol.
- TestToken.so.
- AsureBonusesCrowdsale.sol.
- AsureBounty.sol.
- AsureCrowdsale.sol.
- AsureCrowdsaleDeployer.sol.
- AsureToken.sol.
- Migrations.sol.

3. Findings

In total, **7 issues** were reported including:

- 2 low severity issues.
- 5 owner privileges (ability of owner to manipulate contract, may be risky for investors).

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. Array Size

Severity: low

Description

In `drop` function member of `AsureBounty` contract, `recipients` and `values` arrays length should be checked if they are the same length.

Code snippet

https://github.com/AsureNetwork/crowdsale/blob/50cfbe81c88ba9be85419cc191298872435c4615/packages/crowdsale/contracts/AsureBounty.sol#L16

3.3. Inconsistencies with Asure Token Generation Event.

Severity: owner privileges

Description

1. According to the whitepaper, specified parameters of soft cup and hard cap, but in code we can't see these functions.
2. According to the [whitepaper] the Asure Team and Advisors will receive their tokens over two years after the start of the second phase, but in constructor of AsureCrowdsaleDeployer contract we can't see the Teams and Advisor vesting parameters.
3. According to the [whitepaper] the minimum Contribution is $ 100 (ETH equivalent), but we can't see this parameter in code.

The contract is managed manually by the owner which is not good for investors.

3.4. Owner Privileges

Severity: owner privileges

Description

The contract owner allow himself to:

1. update bonus rate, bonus time, crowdsale time and default rate before crowdsale opened.
2. withdraw ETH and tokens funds before the end of sales.

The contract is managed manually by the owner which is not good for investors.

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/451e55756c987ff65ec9c365d60f03b5

https://gist.github.com/yuriy77k/5680e6009da2c5485b39e7135561088b

https://gist.github.com/yuriy77k/0102e9e8cc41043bf2e1a56e92ee1531