CYBERSEC CONTRACT AUDIT REPORT
ALOHA - CTDSEC.com

Introduction

During February of 2021, Aloha engaged CTDSec to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. Aloha provided CTDSec with access to their code repository and whitepaper.

Disclaimer

The audit makes no statements or warranties about utility of the code, safety of the code, suitability of the business model, regulatory regime for the business model, or any other statements about fitness of the contracts to purpose, or their bugfree status. The audit documentation is for discussion purposes only.

I always recommend having a bug bounty program opened to detect future bugs.

Coverage

Target Code and Revision

For this audit, we performed research, investigation, and review of the Aloha contract followed by issue reporting, along with mitigation and remediation instructions outlined in this report. The following code files are considered in-scope for the review:

- Alohasale.sol - MD5: E542CE1FD2B6DA60980BA21E5F4EDD85

Attacks made to the contract

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices.

Correctness of the protocol implementation [Result OK]

User funds are secure on the blockchain and cannot be transferred without user permission [Result OK]

Vulnerabilities within each component as well as secure interaction between the network components [Result OK]

Correctly passing requests to the network core [Result OK]

Data privacy, data leaking, and information integrity [Result OK]

Susceptible to reentrancy attack [Result OK]

Key management implementation: secure private key storage and proper management of encryption and signing keys [Result OK]

Handling large volumes of network traffic [Result OK]

Resistance to DDoS and similar attacks [Result OK]

Aligning incentives with the rest of the network [Result OK]

Any attack that impacts funds, such as draining or manipulating of funds [Result OK]

Mismanagement of funds via transactions [Result OK]

Inappropriate permissions and excess authority [Result OK]

Special token issuance model [Result OK]

Vulnerabilities

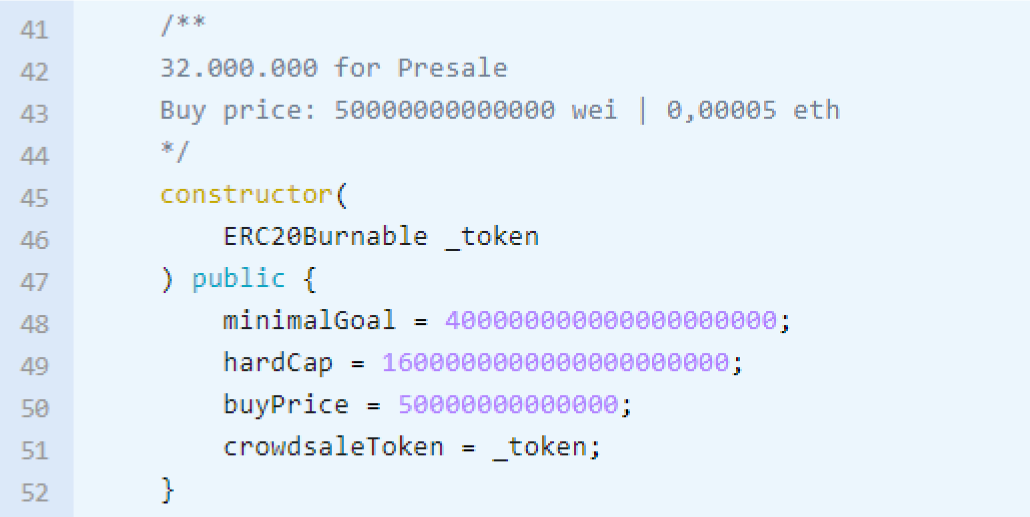
ISSUES

HIGH

Token economics aren’t correctly applied.

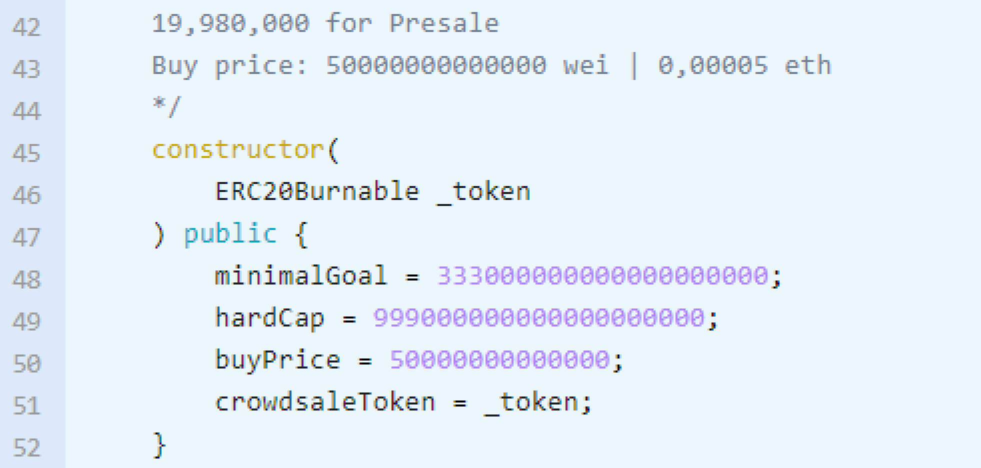
Reviewing the project economics we saw that token economics aren’t correctly applied.

Location:



```
    /**
    32.000.000 for Presale
    Buy price: 50000000000000 wei | 0,00005 eth
    */
    constructor(
        ERC20Burnable _token
    ) public {
        minimalGoal = 400000000000000000000;
        hardCap = 1600000000000000000000;
        buyPrice = 50000000000000;
        crowdsaleToken = _token;
    }
```

Team update: Team modified the contract and applied the correct token economics.



```
    19,980,000 for Presale
    Buy price: 50000000000000 wei | 0,00005 eth
    */
    constructor(
        ERC20Burnable _token
    ) public {
        minimalGoal = 333000000000000000000;
        hardCap = 999000000000000000000;
        buyPrice = 50000000000000;
        crowdsaleToken = _token;
    }
```

Summary of the Audit

The contract is safe and now is also correctly applied according to token economics.

After reviewing the contract we came to the conclusion that is safe to deploy.