Chemix Launchpad-V2 Smart Contract Security Auditing Final Report

BEIJING CHAITIN FUTURE
TECHNOLOGY Co.,Ltd.
Jan 5, 2022

Copyright Notice

Table of contents

1. DisClaimer 4
2. Summary 4
3. Project Version 5
4. Description 5
5. Critical severity 6
6. Heigh Severity 8
7. Medium Severity 10
8. Low Severity 12
9. Optimization Suggestion 17
10. Acknowledgements 17

1. Disclaimer

Except for discussion purposes only, this audit makes no statements or warranties about the utility of the code, safety of the code, suitability of the business model, regulatory regime for the business model, or any other statements about the fitness of the contracts to purpose, or their bug-free status.

2. Summary

Chemix Ecology Committee has authorized this contract security audit project. The blockchain security team of Beijing Chaitin Future Technology Co., Ltd. has conducted a security audit from Dec 6, 2021 to Dec 13, 2021 for the scope defined in the contract and agreement with Chemix Ecology Committee. The audit process was carried out in strict accordance with the scope specified in the contract and agreement.

This audit of the Chemix Launchpad contract source code mainly uses manual audit methods. In addition to the Chaitin Future Technology security audit checklist items, the code logic is also analyzed line by line.

According to the “National Blockchain Vulnerability Database - Blockchain Vulnerability Scoring System”, the nature of vulnerabilities is unintentional, unpredicted security risks. At the same time, the audit should analyze the vulnerability from two dimensions: the degree of impact and the complexity of exploitation.

Impact degree is defined according to the three dimensions of confidentiality impact (C), integrity impact (I) and availability impact (A);

The complexity of exploitation is defined according to the three dimensions of attack vector (AV), attack complexity (AC) and authentication (AU).

For practical reasons, we categorize blockchain vulnerabilities to the following four levels of risk, reflecting its severity: Critical, High, Medium and Low.

	Critical Impact	High Impact	Medium Impact	Low Impact
Low Complexity	Critical	High	Medium	Low
Medium Complexity	Critical	Medium	Medium	Low
High Complexity	High	Low	Low	N/A
Extreme Complexity	Low	N/A	N/A	N/A

The target version contract security audit found a total of **Critical 0**、**High 1** 、**Medium 0** 、**Low 0**。

- Inconsistent calculation of the final settlement price[**High**][**Fixed**]

3. Project Version

According to the audit scope defined in the contract and agreement with the Chemix Ecology Committee.

Audited version:

https://github.com/QIAN-Protocol/LaunchpadV2/commit/84b626aae5db5cb19b443cd4f330c015cd33133a

Final Audited version:

https://github.com/Chemix-Eco/LaunchpadV2/commit/3e9c3fd616739a6868a724004f325eca18c8e3b1

4. Description

This smart contract provides a range of financial services for both DeFi investors and subscribers, including the whole process of token auction, issuance/subscription eligibility verification and other functional services.

5. Heigh Severity

5.1. Inconsistent calculation of the final settlement price

Overview

There is an inconsistency in the calculation of the price when auction tokens are deposited by the auction token issuer and when users withdraw their auction tokens. This problem will cause the amount of auction tokens in the contract pool to be insufficient for later users to withdraw auction tokens when the amount of auction tokens being tapped does not reach total_amount.

BasicBatchAuction.sol:L252-L254

```
function totalTokensCommitted() public view returns (uint256) {
        return totalCommitments.mul(_unit).div(clearingPrice());
   }
```

BasicBatchAuction.sol:L235-L250

```
function tokensClaimable(address account)
        public
        view
        returns (uint256 claimerCommitment){
```

```
        if (commitments[account] == 0) return 0;
        uint256 unclaimedTokens = IERC20(auctionToken).balanceOf(address(this));
        claimerCommitment = commitments[account].mul(totalAmount).div(
            totalCommitments
        );
        //totalAmount
        //
        claimerCommitment = claimerCommitment.sub(claimed[account]);
        if (claimerCommitment > unclaimedTokens) {
            claimerCommitment = unclaimedTokens;
        }
    }
```

Impact

The issue can lead to unintended financial losses as later comers have no auction tokens to withdraw. Early risers might get their auction tokens back at a lower price.

Exploit

The issue occurs when the token's auction volume does not reach total_amount after the auction ends.

Recommendation

It is recommended to use a uniform price settlement method.

Repair results

Repaired.

6. Optimization Suggestion

6.1 “Initializable” has the risk of reentrancy,

It is recommended to add the ReentrancyGuard mechanism for initializable.

6.2 Possibility of fee evasion through div accuracy defects

Pay attention to the issue of screening the very high value of the Payment Tokens.

6.3 PriceDrop's division without SafeMath

Using SafeMath for PriceDrop's division

6.4 Add ReentrancyGuard modifier for auction tokens

The auction tokens should also add ReentrancyGuard modifier.

6.5 Improve the naming convention of internal functions

Internal functions and variables should be prefixed with "_".

6.6 Set parameter carefully for Dutch auction to avoid Dos

The time of the auction should not be too short and the PriceDrop should not be too high.

6.7 Precision issue of PriceDrop DIV

PriceDrop DIV may cause the final transaction price to be high and affect other parts.

6.8 Project security relies on KYC

Project security relies on KYC auditors reviewing the project, so it is recommended to build a checklist.

6.9 Be careful with proxy contracts

The proxy contract mechanism should be wary of the undisciplined ‘selfdestruct()’ or ‘delegatecall()’ method in future version updates.On the other hand, it is recommended to call the initialization method in the depoly of the proxy contract using the ‘constructor()’.

7. Acknowledgements

With the great cooperation of your company, this security audit was successfully completed. The Blockchain Security Team of Beijing Chaitin Future Technology Co., Ltd. expresses its gratitude to all the departments and individuals of Chemix Ecology Committee who participated and provided support.

Beijing Chaitin Future Technology Co., Ltd
CEO Yusen Chen