0x Guard

Smart contracts security assessment

Final report

Tariff: Top

Tonpound Lending

March 2023

0xguard.com

hello@0xguard.com

Contents

Introduction

The report has been prepared for **Tonpound Lending**.

The code is available in Github repo tonpound/tonpound-lending-smart-contracts and was audited after the commit d8f0988.

The Tonpound lending is a fork of Compound protocol. Only changes made to commit a303a325 were audited.

Update. Recheck was done after the commit f96dfc2.

Name	Tonpound Lending
Audit date	2023-03-22 - 2023-03-31
Language	Solidity
Platform	Ethereum

Contracts checked

Name	Address
CToken	
TonpoundPriceOracle	
WhitePaperInterestRateModel	
Unitroller	
Reservoir	
Maximillion	
BaseJumpRateModelV2	
CDaiDelegate	
CErc20	
CErc20Delegate	
CErc20Delegator	

CErc20Immutable

CEther

CTokenInterfaces

Comptroller

ComptrollerStorage

CpTonDelegate

DAIInterestRateModelV3

ErrorReporter

ExponentialNoError

InterestRateModel

JumpRateModel

JumpRateModelV2

Procedure

We perform our audit according to the following procedure:

Automated analysis

- Scanning the project's smart contracts with several publicly available automated Solidity analysis tools
- Manual verification (reject or confirm) all the issues found by the tools

Manual audit

- Manually analyze smart contracts for security vulnerabilities
- Smart contracts' logic check

Known vulnerabilities checked

Title	Check result
Unencrypted Private Data On-Chain	passed
Code With No Effects	passed
Message call with hardcoded gas amount	passed
Typographical Error	passed
DoS With Block Gas Limit	passed
Presence of unused variables	passed
Incorrect Inheritance Order	passed
Requirement Violation	passed
Weak Sources of Randomness from Chain Attributes	passed
Shadowing State Variables	passed
Incorrect Constructor Name	passed
Block values as a proxy for time	passed
Authorization through tx.origin	passed
DoS with Failed Call	passed
Delegatecall to Untrusted Callee	passed
Use of Deprecated Solidity Functions	passed
Assert Violation	passed
State Variable Default Visibility	passed
Reentrancy	passed
Unprotected SELFDESTRUCT Instruction	passed
Unprotected Ether Withdrawal	passed
Unchecked Call Return Value	passed

Floating Pragma	passed
Outdated Compiler Version	passed
Integer Overflow and Underflow	passed
Function Default Visibility	passed

Classification of issue severity

High severity High severity issues can cause a significant or full loss of funds, change of contract ownership, major interference with contract logic. Such issues require immediate attention.

Medium severity Medium severity issues do not pose an immediate risk, but can be detrimental to the client's reputation if exploited. Medium severity issues may lead to a contract failure and can be fixed by modifying the contract state or redeployment. Such issues require attention.

Low severity Low severity issues do not cause significant destruction to the contract's functionality. Such issues are recommended to be taken into consideration.

Issues

High severity issues

No issues were found

Medium severity issues

1. Wrong authorization check (CToken)

Status: Fixed

The changes made to the Compound protocol include that the protocol rewards should go to a Treasury contract. To claim rewards the Treasury should have rights to claim rewards, but the rewards can be claimed only by the admin.

```
    function _reduceReservesFresh(uint reduceAmount) internal returns (uint) {
        // totalReserves - reduceAmount
        uint totalReservesNew;

        // Check caller is admin
        if (msg.sender != admin) {
            revert ReduceReservesAdminCheck();
        }
        ...
    }
```

Recommendation: Change the authorization check to be callable only by the Treasury.

Low severity issues

1. Use fallback price from pair (TonpoundPriceOracle)

Status: Fixed

If price form Chainlink oracle is not fresh, a price from pair TWAP can be used as a fallback.

Recommendation: Implement fallback price for getting price from the Chainlink oracles.

Conclusion

Tonpound Lending CToken, TonpoundPriceOracle, WhitePaperInterestRateModel, Unitroller, Reservoir, Maximillion, BaseJumpRateModelV2, CDaiDelegate, CErc20, CErc20Delegate, CErc20Delegator, CErc20Immutable, CEther, CTokenInterfaces, Comptroller, ComptrollerStorage, CpTonDelegate, DAIInterestRateModelV3, ErrorReporter, ExponentialNoError, InterestRateModel, JumpRateModel, JumpRateModelV2 contracts were audited. 1 medium, 1 low severity issues were found.
1 medium, 1 low severity issues have been fixed in the update.

The Tonpound is a fork of Compound protocol. Only changes to the original code were audited.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without 0xGuard prior written consent.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts 0xGuard to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.
OxGuard retains exclusive publishing rights for the results of this audit on its website and social networks.

0x Guard