智能合约安全审计报告

1. 概要

慢雾安全团队于 2021 年 04 月 28 日，收到 Lendoo 团队对 lendoo 系统安全审计的申请，根据项目特点慢雾安全团队制定如下审计方案。

慢雾安全团队将采用“白盒为主，黑灰为辅”的策略，以最贴近真实攻击的方式，对项目进行安全审计。

慢雾科技 DeFi 项目测试方法：

黑盒测试	站在外部从攻击者角度进行安全测试。
灰盒测试	通过脚本工具对代码模块进行安全测试，观察内部运行状态，挖掘弱点。
白盒测试	基于项目的源代码，进行脆弱性分析和漏洞挖掘。

慢雾科技 DeFi 漏洞风险等级：

严重漏洞	严重漏洞会对项目的安全造成重大影响，强烈建议修复严重漏洞。
高危漏洞	高危漏洞会影响项目的正常运行，强烈建议修复高危漏洞。
中危漏洞	中危漏洞会影响项目的运行，建议修复中危漏洞。
低危漏洞	低危漏洞可能在特定场景中会影响项目的业务操作，建议项目方自行评估和考虑这些问题是否需要修复。
弱点	理论上存在安全隐患，但工程上极难复现。
增强建议	编码或架构存在更好的实践方法。

2. 审计方法

慢雾安全团队智能合约安全审计流程包含两个步骤:

- 使用开源或内部自动化分析的工具对合约代码中常见的安全漏洞进行扫描和测试。
- 人工审计代码的安全问题，通过人工分析合约代码，发现代码中潜在的安全问题。

如下是合约代码审计过程中我们会重点审查的漏洞列表:

（其他未知安全漏洞不包含在本次审计责任范围）

- 重入攻击
- 重放攻击
- 重排攻击
- 短地址攻击
- 拒绝服务攻击
- 交易顺序依赖
- 条件竞争攻击
- 权限控制攻击
- 整数上溢/下溢攻击
- 时间戳依赖攻击
- Gas 使用，Gas 限制和循环
- 冗余的回调函数
- 不安全的接口使用
- 函数状态变量的显式可见性
- 逻辑缺陷
- 未声明的存储指针
- 算术精度误差
- tx.origin 身份验证
- 假充值漏洞
- 变量覆盖

3. 项目背景

3.1 项目介绍

审计合约文件：

项目源代码:

lendoo.zip: 9045ee538ba49599e6aefb933ba85e941a0bc903589672f6c1adc8f5f2fbe80c

3.2 审计合约结构

.
├── CETHToken.sol
├── CErc20.sol
├── CErc20Delegate.sol
├── CErc20Delegator.sol
├── CEther.sol
├── CToken.sol
├── CTokenInterfaces.sol
├── CarefulMath.sol
├── Comp.sol
├── Comptroller.sol
├── ComptrollerInterface.sol
├── ComptrollerStorage.sol
├── EIP20Interface.sol
├── EIP20NonStandardInterface.sol
├── ETHInterestRateModel.sol
├── ErrorReporter.sol
├── Exponential.sol
├── ExponentialNoError.sol
├── GovernorAlpha.sol
├── InterestRateModel.sol
├── InviterStorage.sol
├── JumpRateModelV2.sol
├── LendooPriceOracle.sol
├── PriceOracle.sol
├── PriceOracleProxy.sol

```
├── ReentrancyGuard.sol
├── SafeMath.sol
├── Timelock.sol
├── Unitroller.sol
└── WhitePaperInterestRateModel.sol
```

4. 代码概述

4.1 主要合约函数可见性分析

在审计过程中，慢雾安全团队对核心合约的可见性进行分析，结果如下:

CErc20			
Function Name	Visibility	Mutability	Modifiers
initialize	Public	can modify state	-
mint	External	can modify state	-
redeem	External	can modify state	-
redeemUnderlying	External	can modify state	-
borrow	External	can modify state	-
repayBorrow	External	can modify state	-
repayBorrowBehalf	External	can modify state	-
liquidateBorrow	External	can modify state	-
_addReserves	External	can modify state	-
getCashPrior	Internal	-	-
doTransferIn	Internal	can modify state	-
doTransferOut	Internal	can modify state	-

CToken			
Function Name	Visibility	Mutability	Modifiers
initialize	Public	can modify state	-
transferTokens	Internal	can modify state	-
transfer	External	can modify state	nonReentrant
transferFrom	External	can modify state	nonReentrant
approve	External	can modify state	-
allowance	External	-	-
balanceOf	External	-	-
balanceOfUnderlying	External	can modify state	-
getAccountSnapshot	External	-	-
getBlockNumber	Internal	-	-
borrowRatePerBlock	External	-	-
supplyRatePerBlock	External	-	-
totalBorrowsCurrent	External	can modify state	nonReentrant
borrowBalanceCurrent	External	can modify state	nonReentrant
borrowBalanceStored	Public	-	-
borrowBalanceStoredInternal	Internal	-	-
exchangeRateCurrent	Public	can modify state	nonReentrant
exchangeRateStored	Public	-	-
exchangeRateStoredInternal	Internal	-	-
getCash	External	-	-
accrueInterest	Public	can modify state	-
mintInternal	Internal	can modify state	-
mintFresh	Internal	can modify state	-

redeemInternal	Internal	can modify state	nonReentrant
redeemUnderlyingInternal	Internal	can modify state	nonReentrant
redeemFresh	Internal	can modify state	-
borrowInternal	Internal	can modify state	nonReentrant
borrowFresh	Internal	can modify state	-
repayBorrowInternal	Internal	can modify state	nonReentrant
repayBorrowBehalfInternal	Internal	can modify state	nonReentrant
repayBorrowFresh	Internal	can modify state	-
liquidateBorrowInternal	Internal	can modify state	nonReentrant
liquidateBorrowFresh	Internal	can modify state	-
seize	External	can modify state	nonReentrant
seizeInternal	Internal	can modify state	-
_setPendingAdmin	External	can modify state	-
_acceptAdmin	External	can modify state	-
_setComptroller	Public	can modify state	-
_setReserveFactor	External	can modify state	nonReentrant
_setReserveFactorFresh	Internal	can modify state	-
_addReservesInternal	Internal	can modify state	nonReentrant
_addReservesFresh	Internal	can modify state	-
_reduceReserves	External	can modify state	nonReentrant
_reduceReservesFresh	Internal	can modify state	-
_setInterestRateModel	Public	can modify state	-
_setInterestRateModelFresh	Internal	can modify state	-
getCashPrior	Internal	-	-
doTransferIn	Internal	can modify state	-

doTransferOut	Internal	can modify state	-

InterestRateModel			
Function Name	Visibility	Mutability	Modifiers
getBorrowRate	External	-	-
getSupplyRate	External	-	-

ComptrollerErrorReporter			
Function Name	Visibility	Mutability	Modifiers
fail	Internal	can modify state	-
failOpaque	Internal	can modify state	-

TokenErrorReporter			
Function Name	Visibility	Mutability	Modifiers
fail	Internal	can modify state	-
failOpaque	Internal	can modify state	-

Exponential			
Function Name	Visibility	Mutability	Modifiers
getExp	Internal	-	-
addExp	Internal	-	-
subExp	Internal	-	-
mulScalar	Internal	-	-
mulScalarTruncate	Internal	-	-

mulScalarTruncateAddUInt	Internal	-	-
divScalar	Internal	-	-
divScalarByExp	Internal	-	-
divScalarByExpTruncate	Internal	-	-
mulExp	Internal	-	-
mulExp	Internal	-	-
mulExp3	Internal	-	-
divExp	Internal	-	-
truncate	Internal	-	-
lessThanExp	Internal	-	-
lessThanOrEqualExp	Internal	-	-
greaterThanExp	Internal	-	-
isZeroExp	Internal	-	-

CarefulMath			
Function Name	Visibility	Mutability	Modifiers
mulUInt	Internal	-	-
divUInt	Internal	-	-
subUInt	Internal	-	-
addUInt	Internal	-	-
addThenSubUInt	Internal	-	-

CEther			
Function Name	Visibility	Mutability	Modifiers
constructor	Public	can modify state	CETHToken

mint	External	payable	-
redeem	External	can modify state	-
redeemUnderlying	External	can modify state	-
borrow	External	can modify state	-
repayBorrow	External	payable	-
repayBorrowBehalf	External	payable	-
liquidateBorrow	External	payable	-
	External	payable	-
getCashPrior	Internal	-	-
checkTransferIn	Internal	-	-
doTransferIn	Internal	can modify state	-
doTransferOut	Internal	can modify state	-
requireNoError	Internal	-	-

CETHToken			
Function Name	Visibility	Mutability	Modifiers
constructor	Internal	can modify state	-
transferTokens	Internal	can modify state	-
transfer	External	can modify state	nonReentrant
transferFrom	External	can modify state	nonReentrant
approve	External	can modify state	-
allowance	External	-	-
balanceOf	External	-	-
balanceOfUnderlying	External	can modify state	-
getAccountSnapshot	External	-	-

getBlockNumber	Internal	-	-
borrowRatePerBlock	External	-	-
supplyRatePerBlock	External	-	-
totalBorrowsCurrent	External	can modify state	nonReentrant
borrowBalanceCurrent	External	can modify state	nonReentrant
borrowBalanceStored	Public	-	-
borrowBalanceStoredInternal	Internal	-	-
exchangeRateCurrent	Public	can modify state	nonReentrant
exchangeRateStored	Public	-	-
exchangeRateStoredInternal	Internal	-	-
getCash	External	-	-
accrueInterest	Public	can modify state	-
mintInternal	Internal	can modify state	nonReentrant
mintFresh	Internal	can modify state	-
redeemInternal	Internal	can modify state	nonReentrant
redeemUnderlyingInternal	Internal	can modify state	nonReentrant
redeemFresh	Internal	can modify state	-
borrowInternal	Internal	can modify state	nonReentrant
borrowFresh	Internal	can modify state	-
repayBorrowInternal	Internal	can modify state	nonReentrant
repayBorrowBehalfInternal	Internal	can modify state	nonReentrant
repayBorrowFresh	Internal	can modify state	-
liquidateBorrowInternal	Internal	can modify state	nonReentrant
liquidateBorrowFresh	Internal	can modify state	-
seize	External	can modify state	nonReentrant

_setPendingAdmin	External	can modify state	-
_acceptAdmin	External	can modify state	-
_setComptroller	Public	can modify state	-
_setReserveFactor	External	can modify state	nonReentrant
_setReserveFactorFresh	Internal	can modify state	-
_reduceReserves	External	can modify state	nonReentrant
_reduceReservesFresh	Internal	can modify state	-
_setInterestRateModel	Public	can modify state	-
_setInterestRateModelFresh	Internal	can modify state	-
getCashPrior	Internal	-	-
checkTransferIn	Internal	-	-
doTransferIn	Internal	can modify state	-
doTransferOut	Internal	can modify state	-

Comptroller			
Function Name	Visibility	Mutability	Modifiers
constructor	Public	can modify state	-
getAssetsIn	External	-	-
checkMembership	External	-	-
enterMarkets	Public	can modify state	-
addToMarketInternal	Internal	can modify state	-
exitMarket	External	can modify state	-
mintAllowed	External	can modify state	-
mintVerify	External	can modify state	-
redeemAllowed	External	can modify state	-

redeemAllowedInternal	Internal	-	-
redeemVerify	External	can modify state	-
borrowAllowed	External	can modify state	-
borrowVerify	External	can modify state	-
repayBorrowAllowed	External	can modify state	-
repayBorrowVerify	External	can modify state	-
liquidateBorrowAllowed	External	can modify state	-
liquidateBorrowVerify	External	can modify state	-
seizeAllowed	External	can modify state	-
seizeVerify	External	can modify state	-
transferAllowed	External	can modify state	-
transferVerify	External	can modify state	-
getAccountLiquidity	Public	-	-
getAccountLiquidityInternal	Internal	-	-
getHypotheticalAccountLiquidity	Public	-	-
getHypotheticalAccountLiquidityInternal	Internal	-	-
liquidateCalculateSeizeTokens	External	-	-
_setPriceOracle	Public	can modify state	-
_setCloseFactor	External	can modify state	-
_setCollateralFactor	External	can modify state	-
_setLiquidationIncentive	External	can modify state	-
_supportMarket	External	can modify state	-
_addMarketInternal	Internal	can modify state	-
_setMarketBorrowCaps	External	can modify state	-
_setBorrowCapGuardian	External	can modify state	-

_setPauseGuardian	Public	can modify state	-
_setMintPaused	Public	can modify state	-
_setBorrowPaused	Public	can modify state	-
_setTransferPaused	Public	can modify state	-
_setSeizePaused	Public	can modify state	-
_become	Public	can modify state	-
adminOrInitializing	Internal	-	-
setCompSpeedInternal	Internal	can modify state	-
updateCompSupplyIndex	Internal	can modify state	-
updateCompBorrowIndex	Internal	can modify state	-
distributeSupplierComp	Internal	can modify state	-
distributeBorrowerComp	Internal	can modify state	-
updateContributorRewards	Public	can modify state	-
claim	Public	can modify state	-
claim	Public	can modify state	-
claim	Public	can modify state	-
grantCompInternal	Internal	can modify state	-
_grantComp	Public	can modify state	-
_setCompSpeed	Public	can modify state	-
_setContributorCompSpeed	Public	can modify state	-
getAllMarkets	Public	-	-
getBlockNumber	Public	-	-
getCompAddress	Public	-	-

Comptroller			
Function Name	Visibility	Mutability	Modifiers
getUnderlyingPrice	External	-	-

Unitroller			
Function Name	Visibility	Mutability	Modifiers
constructor	Public	can modify state	-
_setPendingImplementation	Public	can modify state	-
_acceptImplementation	Public	can modify state	-
_setPendingAdmin	Public	can modify state	-
_acceptAdmin	Public	can modify state	-
fallback	External	payable	-

ExponentialNoError			
Function Name	Visibility	Mutability	Modifiers
truncate	Internal	-	-
mul_ScalarTruncate	Internal	-	-
mul_ScalarTruncateAddUInt	Internal	-	-
lessThanExp	Internal	-	-
lessThanOrEqualExp	Internal	-	-
greaterThanExp	Internal	-	-
isZeroExp	Internal	-	-
safe224	Internal	-	-
safe32	Internal	-	-

add_	Internal	-	-
add_	Internal	-	-
add_	Internal	-	-
add_	Internal	-	-
sub_	Internal	-	-
sub_	Internal	-	-
sub_	Internal	-	-
sub_	Internal	-	-
mul_	Internal	-	-
mul_	Internal	-	-
mul_	Internal	-	-
mul_	Internal	-	-
mul_	Internal	-	-
mul_	Internal	-	-
mul_	Internal	-	-
mul_	Internal	-	-
mul_	Internal	-	-
div_	Internal	-	-
div_	Internal	-	-
div_	Internal	-	-
div_	Internal	-	-
div_	Internal	-	-
div_	Internal	-	-
div_	Internal	-	-
div_	Internal	-	-
fraction	Internal	-	-

GovernorAlpha			
Function Name	Visibility	Mutability	Modifiers
quorumVotes	Public	-	-
proposalThreshold	Public	-	-
proposalMaxOperations	Public	-	-
votingDelay	Public	-	-
votingPeriod	Public	can modify state	-
	Public	can modify state	-
propose	Public	can modify state	-
queue	Public	can modify state	-
_queueOrRevert	Internal	payable	-
execute	Public	can modify state	-
cancel	Public	-	-
getActions	Public	-	-
getReceipt	Public		-
state	Public	can modify state	-
castVote	Public	can modify state	-
castVoteBySig	Public	can modify state	-
_castVote	Internal	can modify state	-
__acceptAdmin	Public	can modify state	-
__abdicate	Public	can modify state	-
__queueSetTimelockPendingAdmin	Public	can modify state	-
__executeSetTimelockPendingAdmin	Public	-	-
add256	Internal	-	-

sub256	Internal	-	-
getChainId	Internal	-	-

TimelockInterface			
Function Name	Visibility	Mutability	Modifiers
delay	External	-	-
GRACE_PERIOD	External	-	-
acceptAdmin	External	can modify state	-
queuedTransactions	External	-	-
queueTransaction	External	can modify state	-
cancelTransaction	External	can modify state	-
executeTransaction	External	payable	-
LendooPriceOracle			
Function Name	Visibility	Mutability	Modifiers
constructor	Public	can modify state	-
fallback	External	payable	-
failOracle	Internal	can modify state	-
failOracleWithDetails	Internal	can modify state	-
_setPendingAnchor	Public	can modify state	-
_setPaused	Public	can modify state	-
_setPendingAnchorAdmin	Public	can modify state	-
_acceptAnchorAdmin	Public	can modify state	-
assetPrices	Public	-	-
getPrice	Public	-	-
setPrice	Public	can modify state	-

setPriceInternal	Internal	can modify state	-
setPriceStorageInternal	Internal	can modify state	-
calculateSwing	Internal	-	-
capToMax	Internal	-	-
setPrices	Public	can modify state	-

4.2 代码审计详情

4.2.1 低危漏洞

4.2.1.1 权限过大风险

lendoo 系统中的 admin 权限可以修改系统敏感参数，添加/移除价格预言机等。存在权限过大问题，建议管理员角色交与社区治理控制，以避免权限过大的风险。

修复状态：经与项目方沟通反馈后，项目方决定将权限转移至 timelcok 合约以避免权限过大的风险。但目前项目方暂未将权限转移至 Timelock。

5. 审计结果

5.1 总结

审计结论：低风险

审计编号：0X002104290002

审计时间：2021 年 04 月 29 日

审计团队 ：慢雾安全团队

审计总结 ：慢雾安全团队采用人工结合内部工具对代码进行分析。审计期间发现了 1 个问题。其中包含 1 个低危漏洞，由于目前项目各合约权限暂未移交给社区治理，因此项目仍存在权限过大的风险。

6. 声明

慢雾仅就本报告出具前已经发生或存在的事实出具本报告，并就此承担相应责任。对于出具以后发生或存在的事实，慢雾无法判断其智能合约安全状况，亦不对此承担责任。本报告所作的安全审计分析及其他内容，仅基于信息提供者截至本报告出具时向慢雾提供的文件和资料(简称“已提供资料”)。慢雾假设：已提供资料不存在缺失、被篡改、删减或隐瞒的情形。如已提供资料信息缺失、被篡改、删减、隐瞒或反映的情况与实际情况不符的，慢雾对由此而导致的损失和不利影响不承担任何责任。

慢雾科技
slow mist

官方网址

www.slowmist.com

电子邮箱

team@slowmist.com

微信公众号