
# 智能合约安全审计报告

# 1. 概要

慢雾安全团队于 2021 年 02 月 18 日，收到 FilDA 团队对 FilDA 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

FilDA 是全球首个基于 HECO 的跨链借贷 DeFi 项目，首发 HUSD、HBTC、HT、等 H 系资产借贷功能，同时也是 HECO 首个公开平台各项 APY 数据，存借双向实时透明数据的借贷项目。FilDA 平台存借款总额高峰值突破 12 亿美元，FilDA 交易对深度超过 2000 万美金。FilDA 项目无募资，无预挖，致力于成为 HECO 首选的用户友好型的 DeFi 借贷平台。

**审计合约文件：**

项目源代码

审计初始版本：

https://github.com/fildaio/Quicksilver/tree/hardblock

commit: 4fd1b52f54b013dc4847327de31340b66c3dc294

审计最终版本：

https://github.com/fildaio/Quicksilver/compare/hardblock...cdljsj:patch-1

## 3.2 审计合约结构

```
├── DefaultHecoInterestModel.sol
├── HecoJumpInterestModel.sol
├── IPriceCollector.sol
├── Ownable.sol
├── QsConfig.sol
├── QsPriceOracle.sol
├── QsPriceOracleV2.sol
├── Qstroller.sol
├── QstrollerV1.sol
├── SToken.sol
```

```
├── compound
│   ├── CDaiDelegate.sol
│   ├── CErc20.sol
│   ├── CErc20Delegate.sol
│   ├── CErc20Delegator.sol
│   ├── CErc20Immutable.sol
│   ├── CEther.sol
│   ├── CToken.sol
│   ├── CTokenInterfaces.sol
│   ├── CarefulMath.sol
│   ├── Comptroller.sol
│   ├── ComptrollerG1.sol
│   ├── ComptrollerG2.sol
│   ├── ComptrollerG3.sol
│   ├── ComptrollerInterface.sol
│   ├── ComptrollerStorage.sol
│   ├── DAIInterestRateModelV2.sol
│   ├── EIP20Interface.sol
│   ├── EIP20NonStandardInterface.sol
│   ├── ErrorReporter.sol
│   ├── Exponential.sol
│   ├── Governance
│   │   ├── Comp.sol
│   │   └── GovernorAlpha.sol
│   ├── InterestRateModel.sol
│   ├── JumpRateModel.sol
│   ├── Lens
│   │   └── CompoundLens.sol
│   ├── Maximillion.sol
│   ├── Migrations.sol
│   ├── PriceOracle.sol
│   ├── PriceOracleProxy.sol
│   ├── Reservoir.sol
│   ├── SafeMath.sol
│   ├── SimplePriceOracle.sol
│   ├── Timelock.sol
│   ├── Unitroller.sol
│   └── WhitePaperInterestRateModel.sol
└── mock
    ├── ELAToken.sol
    ├── ETHToken.sol
    ├── HFILToken.sol
```

```
├── MockPriceOracle.sol
├── QsSimplePriceOracle.sol
└── TetherToken.sol
```

# 4. 代码概述

## 4.1 主要合约地址

| Contract Name | Contract Address |
| --- | --- |
| Filda HT | 0x824151251B38056d54A15E56B73c54ba44811aF8 |
| Filda ELA | 0x0AD0bee939E00C54f57f21FBec0fBa3cDA7DEF58 |
| Filda HFIL | 0x043aFB65e93500CE5BCbf5Bbb41FC1fDcE2B7518 |
| Filda HUSD | 0xB16Df14C53C4bcfF220F4314ebCe70183dD804c0 |
| Filda HPT | 0x749E0198f12559E7606987F8e7bD3AA1DE6d236E |
| Filda ETH | 0x033F8C30bb17B47f6f1f46F3A42Cc9771CCbCAAE |
| Filda HBTC | 0xF2a308d3Aea9bD16799A5984E20FDBfEf6c3F595 |
| Filda HDOT | 0xCca471B0d49c0d4835a5172Fd97ddDEA5C979100 |
| Filda HBCH | 0x09e3d97A7CFbB116B416Dae284f119c1eC3Bd5ea |
| Filda HLTC | 0x4937A83Dc1Fa982e435aeB0dB33C90937d54E424 |
| Filda USDT | 0xAab0C9561D5703e84867670Ac78f6b5b4b40A7c1 |
| Filda HBSV | 0x74F8D9B701bD4d8ee4ec812AF82C71EB67B9Ec75 |
| Filda HXTZ | 0xfEA846A1284554036aC3191B5dFd786C0F4Db611 |
| Filda pNEO | 0x92701DA6A28Ca70aA5Dfca2B8Ae2b4B8a22a0C11 |
| Filda AAVE | 0x73Fa2931e060F7d43eE554fd1De7F61115fE1751 |
| Filda UNI | 0xAc9E3AE0C188eb583785246Fef37AEF9ea159fb7 |
| Filda SNX | 0x88962975FDE8C7805fE0f38b7c91C18f4d55bb40 |
| Qstroller | 0xb74633f2022452f377403B638167b0A135DB096d |
| QsPriceOracle | 0x0a6a06003417dA7BCF1C2bdc27e2A30C38EfF4Ad |

## 4.2 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:

| SToken | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| seizeInternal | Internal | Can modify state | - |
| isNativeToken | Public | - | - |

| QsConfig | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| _setCompToken | Public | Can modify state | onlyOwner |
| _setSafetyVault | Public | Can modify state | onlyOwner |
| _setSafetyVaultRatio | Public | Can modify state | onlyOwner |
| _setCompSpeedGuardianPaused | Public | Can modify state | onlyOwner |
| calculateSeizeTokenAllocation | Public | - | - |

| Qstroller | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| _setQsConfig | Public | Can modify state | - |
| _setCompSpeeds | Public | Can modify state | - |
| refreshCompSpeeds | Public | Can modify state | - |
| refreshCompSpeedsInternal | Internal | Can modify state | - |
| getCompAddress | Public | - | - |
| calculateSeizeTokenAllocation | Public | - | - |
| transferComp | Internal | Can modify state | - |

| Unitroller | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| _setPendingImplementation | Public | Can modify state | - |
| _acceptImplementation | Public | Can modify state | - |
| _setPendingAdmin | Public | Can modify state | - |
| _acceptAdmin | Public | Can modify state | - |
| Fallback | External | Payable | - |

| Comptroller | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |

| | | | |
|---|---|---|---|
| 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 | - |
| _setMaxAssets | External | Can modify state | - |
| _setLiquidationIncentive | External | Can modify state | - |
| _supportMarket | External | Can modify state | - |
| _addMarketInternal | Internal | 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 | - | - |
| refreshCompSpeeds | Public | Can modify state | - |
| refreshCompSpeedsInternal | Internal | Can modify state | - |
| updateCompSupplyIndex | Internal | Can modify state | - |
| updateCompBorrowIndex | Internal | Can modify state | - |
| distributeSupplierComp | Internal | Can modify state | - |
| distributeBorrowerComp | Internal | Can modify state | - |
| transferComp | Internal | Can modify state | - |
| claimComp | Public | Can modify state | - |
| claimComp | Public | Can modify state | - |
| claimComp | Public | Can modify state | - |
| _setCompRate | Public | Can modify state | - |
| _addCompMarkets | Public | Can modify state | - |
| _addCompMarketInternal | Internal | Can modify state | - |
| _dropCompMarket | Public | Can modify state | - |
| getAllMarkets | Public | - | - |
| getBlockNumber | Public | - | - |
| getCompAddress | Public | - | - |

| CEther | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| 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 | - |
| fallback | External | Payable | - |
| getCashPrior | Internal | - | - |
| doTransferIn | Internal | Can modify state | - |
| doTransferOut | Internal | Can modify state | - |
| requireNoError | Internal | - | - |
| isNativeToken | Public | - | - |

| 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 | 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 |
| 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 | - |

| QsPriceOracle | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| getUnderlyingPrice | Public | - | - |
| setUnderlyingPrice | Public | Can modify state | onlyAdmin |
| setDirectPrice | Public | Can modify state | onlyAdmin |
| setDirectPrice | Public | Can modify state | onlyAdmin |
| assetPrices | External | - | - |
| compareStrings | Internal | - | - |
| transferPriceAdmin | Public | Can modify state | onlyAdmin |

| QsPriceOracleV2 | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| getUnderlyingPrice | Public | - | - |
| setUnderlyingPrice | Public | Can modify state | onlyPriceAdmin |
| isValidPrice | Public | - | - |
| setDirectPrice | Public | Can modify state | onlyPriceAdmin whenNotPaused |
| setDirectPrice | Public | Can modify state | onlyPriceAdmin whenNotPaused |
| setPrice | Private | Can modify state | onlyPriceAdmin |
| setDirectPriceWithForce | Public | Can modify state | onlyPriceAdmin |
| assetPrices | External | - | - |
| addPriceAdmin | Public | Can modify state | onlyGovernance |

| | | | |
|---|---|---|---|
| removePriceAdmin | Public | Can modify state | onlyGovernance |
| setPaused | Public | Can modify state | onlyGovernance |
| setErrorHappened | Public | Can modify state | onlyGovernance |
| transferGovernance | Public | Can modify state | onlyGovernance |

| HecoJumpInterestModel | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| utilizationRate | Public | - | - |
| getBorrowRate | Public | - | - |
| getSupplyRate | Public | - | - |

| DefaultHecoInterestModel | | | |
|---|---|---|---|
| Function Name | Visibility | Mutability | Modifiers |
| utilizationRate | Public | - | - |
| getBorrowRate | Public | - | - |
| getSupplyRate | Public | - | - |

## 4.3 代码审计详情

## 4.3.1 低危漏洞

### 4.3.1.1 权限过大风险

在 SToken、Qstroller、QsPriceOracle 等合约中存在管理员角色，管理员可以对项目的利率模型、暂停机制等敏感参数进行任意修改，这将导致管理员权限过大的风险。

修复建议：建议将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。

#### 4.3.1.2 价格事件记录错误

在 QsPriceOracle 合约中，Admin 在调用 setDirectPrice 和 setDirectPrice 函数进行喂价时，使用 PricePosted 进行事件记录，但记录 previousPriceMantissa 时使用的是更新过后的 prices[_asset]，导致先前价格记录错误。

修复建议：增加一个变量记录更新前价格。

**代码位置：**QsPriceOracle.sol

```
    function setDirectPrice(address _asset, uint _price) public onlyAdmin {
        prices[_asset] = _price;
        emit PricePosted(_asset, prices[_asset], _price, _price);
    }

    function setDirectPrice(address[] memory _assets, uint[] memory _prices) public onlyAdmin {
        require(_assets.length > 0, "At least one asset price is required");
        require(_assets.length == _prices.length, "Assets and prices are not match");

        for (uint i = 0; i < _assets.length; i++) {
            prices[_assets[i]] = _prices[i];
            emit PricePosted(_assets[i], prices[_assets[i]], _prices[i], _prices[i]);
        }
    }
```

修复状态：已修复。

### 4.3.2 增强建议

#### 4.3.2.1 部分代码冗余

QsPriceOracle 合约中的 compareStrings 函数并未被使用。

修复建议：建议移除此冗余函数。

**代码位置：**QsPriceOracle.sol

```
function compareStrings(string memory a, string memory b) internal pure returns (bool) {
    return (keccak256(abi.encodePacked((a))) == keccak256(abi.encodePacked((b))));
}
```

**修复状态：**已修复。

# 5. 审计结果

## 5.1 总结

审计结论 ：低风险

审计编号 ：0X002102260002

审计时间 ：2021 年 02 月 26 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 3 个问题。其中包含 2 个低危漏洞，并提出了 1 点增强建议。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

慢雾科技
slow mist

**官方网址**

www.slowmist.com

**电子邮箱**

team@slowmist.com

**微信公众号**