Openmeta
审计报告

版本：1.0.0

报告编号：2022030800011019

Fairyproof 发布

2022 年 3 月 8 日

01. 介绍

本报告包含了Fairyproof对Openmeta项目代码进行审计的结果。

审计开始时间：

2022年3月4日

审计结束时间：

2022年3月7日

审计代码所在的Github仓库地址：

https://github.com/openmeta-finance/contracts

审计开始时代码在Github中的commit编号：

d8749545140dc1559222ae55bb80190e18ab17d1

审计结束时代码在Github中的commit编号：

498da778c2562623f18175b574de785267d127fe

审计代码文件及目录结构：

审计代码的文件名及目录结构为：

```
contracts/
├── OpenmetaController.sol
├── OpenmetaNFT.sol
├── OpenmetaTrade.sol
├── interface
|   ├── IERCToken.sol
|   ├── IMnftController.sol
|   ├── IOpenmetaController.sol
|   └── IOpenmetaTrade.sol
├── libraries
|   └── TransferHelper.sol
└── utils
    ├── BlockTimestamp.sol
    └── Validation.sol

3 directories, 10 files
```

本次审计的目的是为了审阅Openmeta项目基于Solidity语言编写的NFT拍卖平台，发现潜在的安全隐患，研究其设计、架构，并试图找到可能存在的漏洞。

我们全面阅读了Openmeta团队提交的上述代码，并仔细审阅了上述代码中可能出现问题的方方面面，对上述合约代码给出了全面、综合的改进意见及评审结果。

本次审计仅针对授权方指定版本的代码、安装包及其它授权方提供的素材展开，其结论仅对相应版本的应用适用，一旦相关代码、配置、运营环境等发生变化，相应结论将不再适用。

— 免责声明

截至本报告发布之日，本报告所阐述的内容仅反映审计团队对当前所审计的代码安全进展及状况的理解。任何人在接触或使用与本报告相关的服务、产品、协议、平台、或任何物品时，自行承担一切可能产生的冲突、损失、利益及风险，本报告的审计团队概不负责。

本审计不涉及审计代码的编译器及任何超出代码编程语言的领域。如果所审计的代码为智能合约，则合约由引用链下信息或资源所导致的风险及责任不在本审计覆盖的范围之内。

本审计无法详尽查看每一个细节，也无法穷尽每一种可能，因此本报告的审计团队鼓励本项目的开发团队及任何相关利益方对所审计代码进行任何后续的测试及审计。

对任何第三方使用本报告中所提及或涉及的软件、源码、软件库、产品、服务、信息等一切事物所产生的冲突、损失、利益及风险，本审计团队不保证、不承诺也不承担任何责任。

本报告的内容、获取方式、使用以及任何其所涉及的服务或资源都不能作为任何形式的投资、税务、法律、监管及建议等的依据，也不产生相关的责任。

— 审计方式

审计Openmeta项目的源代码是为了能清晰地理解该项目的实现方式及运行原理。审计团队对项目代码进行了深入的研究、分析和测试，并收集了详尽的数据。审计团队会在本报告中会详细列举所发现的每个问题、问题所在的源码位置、问题产生的根源以及对问题的描述，并对问题给出相应的改进建议。

Fairyproof审计的流程如下：

1. 背景研究。Fairyproof团队会阅读项目介绍、白皮书、合约源码等一切Openmeta团队所提供的相关材料及信息，以确保Fairyproof团队理解项目的规模、范围及功能。
2. 自动化检测。此步骤主要用自动化工具扫描源码，找到常见的潜在漏洞。
3. 人工审阅项目代码。此步骤由工程师逐行阅读代码，找到潜在的漏洞。
4. 逻辑校对。此步骤审计工程师将对代码的理解与Openmeta团队提供的材料及信息相比较，检查代码的实现是否符合项目的定义及白皮书等信息中的描述。
5. 测试用例检测。此步骤包括三部分：
   i. 测试用例设计。审计工程师将根据前述步骤对项目背景的理解及合约代码的理解，针对项目可能的执行逻辑及方式设计测试用例。
   ii. 测试范围分析。该步骤会详细检查所设计的测试用例是否覆盖了合约代码的所有逻辑分支，并判断测试用例执行后，合约代码的逻辑是否能得到充分的执行及检查
   iii. 符号执行。该步骤将运行测试用例以测试代码所有可能的执行路径。
6. 优化审查。该流程将根据合约的应用场景、调用方式及业界最新的研究成果从可维护性、安全性及可操作性等方面审查项目代码。

— 报告结构

本报告列举的每个问题都被设置了一个安全级别，这些安全级别根据其对项目的影响及安全隐患的大小而定。我们对每个问题都给出了相应的改进建议。为了便于读者阅读，我们分别按主题内容和安全级别这两种方式罗列了所有的问题，并提出了全面增强安全性的建议。

— 引用文档

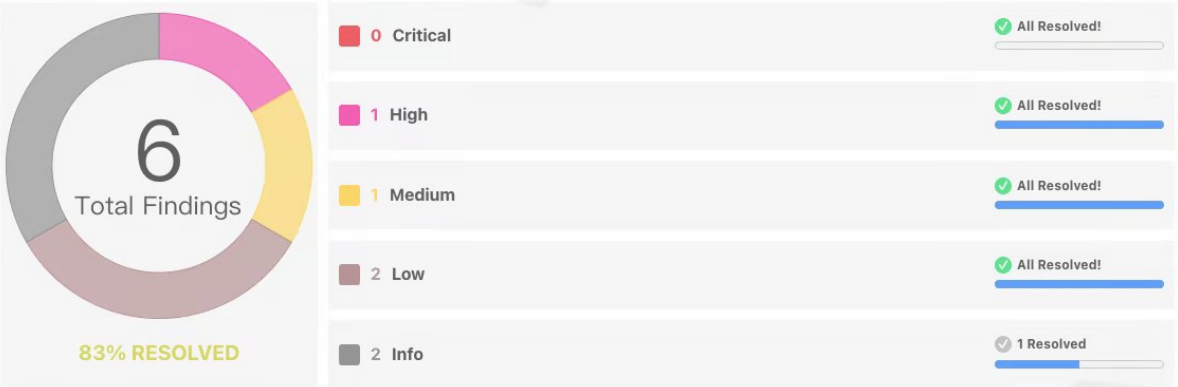
在审阅过程中，我们参考了与项目相关的文档以加深对项目逻辑、功能及应用的理解。本次报告参阅的文档资料如下：

https://nft.openmeta.finance/

上述文档被视为本项目代码实现及功能的定义。当我们认为代码实现与文档定义有分歧时，我们及时咨询并与Openmeta团队进行了沟通和确认。

— 审计结果

审计编号	审计团队	审计时间	审计结果
2022030800011019	Fairyproof Security Team	2022.03.04 - 2022.03.07	信息



审计结论：

Fairyproof团队综合使用了自动化工具和人工方式审计了本项目。在审计过程中，发现了 1个高风险、1个中风险、2个低风险和2个信息等级风险，修复了其中的1个高风险、1个中风险、2个低风险和1个信息等级风险，确认了其中1个信息等级风险。

02. Fairyproof介绍

Fairyproof是一家领先的区块链技术公司，公司为行业企业提供安全审计和咨询方面的服务。Fairyproof研发了自己的一系列合约编写和安全审计标准，为众多客户提供了周到、严谨的服务。

03. 项目介绍

Openmeta为一NFT拍卖平台。

04. 审计代码的主要功能

被审计合约的主要功能为NFT的发行与拍卖，细节如下：

`OpenmetaNFT.sol` 为ERC-1155协议的NFT发行合约

`OpenmetaController.sol` 为控制器合约，控制NFT的发行与管理员签名。

`OpenmetaTrade.sol` 为NFT拍卖平台，兼容ERC-721与ERC-1155。用户可以拍卖自己的NFT，从平台支持的通证中选定一种来定价。其它用户可以支付相应的价格购买该NFT。

注：合约平台的线下中心化程序部分不在本次审计的范围内。

05. 风险种类

当前审计采用智能工具静态分析和人工审计相结合的方法，从以下多个风险种类方面对项目代码进行了全方位的审计。

- 重入攻击
- 重放攻击
- 重排攻击
- 矿工特权
- 回滚攻击
- 注入攻击
- 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
- 冗余的回调函数
- 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
- 参数设置
- 设计缺陷
- 潜在后门
- 通证发行
- 管理权限
- 代理升级
- 委托调用插槽共享
- 用户资金安全
- 迁移管理
- 代码优化
- 其它分类

06. 风险分级

本报告中的每个问题都被设置了一个安全等级，程度由高到低排列如下：

Critical/致命 风险及隐患需要立刻解决。

High/高危 风险及隐患将引发风险及问题，必须解决。

Medium/中 风险及隐患可能导致潜在风险，最终仍然需要解决。

Minor/低 风险及隐患主要指各类处理不当或者会引发警告信息的细节，这类问题可以暂时搁置，但建议最终解决。

Informational/信息 一般不会引起风险问题，主要是代码的改进与优化。

07. 基于风险等级的问题列表

编号	标题	分类	等级	状态
FP-1	竞拍模式时，购买者不用支付费用	设计缺陷	高风险	✓已修复
FP-2	竞拍模式时，NFT未铸造时购买会导致流拍	设计缺陷	中风险	✓已修复
FP-3	maxFeeLimit设置未进行限制	参数设置	低风险	✓已修复
FP-4	合约中未验证支付价格	设计缺陷	低风险	✓已修复
FP-5	部分代码未发挥作用	代码优化	信息	✓已修复
FP-6	未使用的导入接口	代码优化	信息	已确认

08. 问题详述

[FP-1] 竞拍模式时，购买者不用支付费用 高风险 ✓已修复

风险分类：设计缺陷

描述：

`OpenmetaTrade.sol`，`performOrder`函数，设计有使用`ETH`进行支付的场景。然而在拍卖模式时，限定只有`OpenmetaController`合约的签名者才能调用，见`modifier checkOrderCaller`。此时，支付消耗的是`msg.sender`也就是签名者的资金，当签名者的资金足够时，NFT购买者将购买成功而签名者支付购买费用。

建议：

使用`WETH`代币进行购买而不直接使用`ETH`购买。

状态：

已修复。增加一个验证条件`require(!isOriginToken, "auctions do not support chain-based coins");`，强制支付资产为ERC-20相关资产。

[FP-2] 竞拍时NFT未铸造时购买会导致流拍 中风险 ✓已修复

风险分类：设计缺陷

描述：

`OpenmetaTrade.sol`，`performOrder`函数，会调用`getOrderUserBalance`函数验证用户的支付代币数量及拍卖者的NFT数量是否足够。当拍卖者的ERC-1155 NFT不存在时，不进行实际拍卖，因此会流拍。然而根据设计，拍卖者可以拍卖属于它的暂未上链的NFT，此时应该`mint`一个相应的NFT然后再进行拍卖。

建议：

只有当NFT已经发行时才检查拍卖者的NFT余额。

状态：

已修复。增加类似如下判断条件：`if ((_dealOrder.minted && nftBalance < _makerOrder.quantity) || amountBalance < _dealOrder.dealAmount)`

[FP-3] maxFeeLimit设置未进行限制 低风险 √已修复

风险分类：参数设置

描述：

`OpenmetaController.sol`，`setMaxFeeLimit`函数，未对函数参数`_maxFeeLimit`的取值进行限制，当超过适当的取值范围时，用户无法进行拍卖活动。

建议：

设定为一个适当的值。

状态：

已修复。增加类似如下限制条件：

```
require(
    _maxFeeLimit >= feeRate && _maxFeeLimit < BASE_ROUND,
    "verification fee limit failed"
);
```

[FP-4] 合约中未验证支付价格 低风险 √已修复

风险分类：设计缺陷

描述：

`OpenmetaTrade.sol`，`performOrder`函数，未对用户支付的费用和出售者的定价进行比较，依赖于线下中心化程序进行判断。

建议：

合约内也作相应的判断。

状态：

已修复。增加类似如下限制条件：

```
uint256 dealAmount = _makerOrder.price * _makerOrder.quantity;
require(_dealOrder.dealAmount >= dealAmount, "order deal amount verification failed");
```

[FP-5] 部分代码未发挥作用 信息 √已修复

风险分类：代码优化

描述：

`OpenmetaController.sol`，`getMaximumFee`及`checkFeeAmount`函数，存在无效的精度提升代码片断：

```
maximumFee = _amount * (maxFeeLimit * BASE_ROUND) / 10000 / BASE_ROUND;
authorFee = _amount * (_authorProtocolFee * BASE_ROUND) / 10000 / BASE_ROUND;
txFee = _amount * (feeRate * BASE_ROUND) / 10000 / BASE_ROUND;
```

这里，代码里乘上一个`BASE_ROUND`然后再除于一个`BASE_ROUND`没有意义，无法获得精度提升。

建议：

简化相应的代码。

状态：

已修复。修改后的部分代码片断如下：

```
uint256 public constant BASE_ROUND = 10000;
maximumFee = _amount * maxFeeLimit / BASE_ROUND;
```

[FP-6] 未使用的导入接口 信息 已确认

风险分类：代码优化

描述：

`interface`目录下，定义了`IMnftController.sol`接口及其它相关接口。`IMnftController.sol`并未使用，并且其它接口对应的合约并未显式的在定义处实现它。

建议：

统一定义的外部接口文件，非继承合约引用它，继承合约实现它，防止漏掉部分功能；仅引用不实现的接口建议在合约内部定义。

状态：

已确认，在未来会进行进一步代码优化。

09. 增强建议

- 无

Appendix

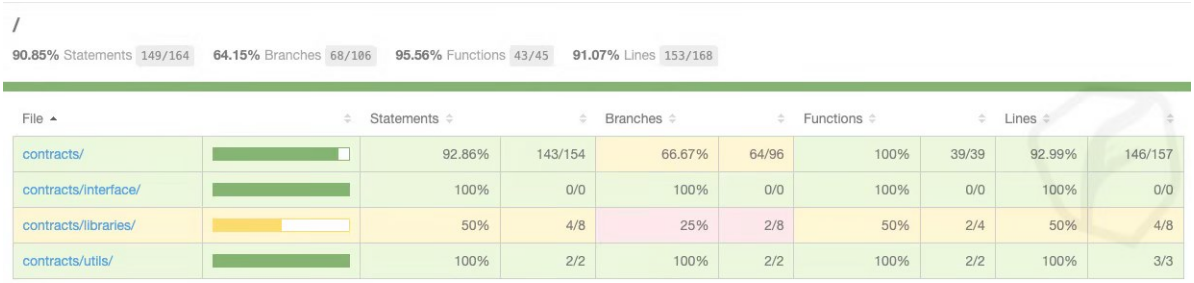
所审计文件的SHA-256哈希值:

```
contracts/OpenmetaController.sol:
0x4f53964474b08c964a28953550d5d3fef7485f6649b0f21ce311f4105af75bd7

contracts/OpenmetaNFT.sol:
0x9658ebddf0b2f1ed6036c2a4c19e115524df6d125b0160907dd6b9603e128e91

contracts/OpenmetaTrade.sol:
0x733a3bb69ef289328f2e8af5835fda278cb50763288fd11d1f250e4ce8e72579

contracts/interface/IERCToken.sol:
0xc7b798f9b0a0660cf79fd6f33a6f4172b79142ad8d2269744cae52ab70c3516e

contracts/interface/IMnftController.sol:
0xeda179b24e31a22e6d7d6948ac0b24d20f10472a94d2e7b85d71758cd23df59b

contracts/interface/IOpenmetaController.sol:
0xe03f90b69532e7b48f0f30652c09855dcd64fb8b2205240d2a383df8e9972e40

contracts/interface/IOpenmetaTrade.sol:
0xf41f9f58d97478dd3d7545ec972b4f5b64cfc7f5633584efee928da8927fff13

contracts/libraries/TransferHelper.sol:
0x10e90a45583a37c724469636c3f72891b05df8758bcced41e7428e0a16d739c8

contracts/utils/BlockTimestamp.sol:
0x49ed703773e14bdff4b91e2e3c6725b113a9f98a274a85fc4b662a4e8387279b

contracts/utils/Validation.sol:
0x21adc5caeba350fa5504f8cdfe192043eea2d8e814762dd5dc1e0ecb924c71f7
```

单元测试结果:

```
44 passing (6s)

----------------------------|----------|----------|----------|----------|----------
------|
File                        |  % Stmts | % Branch |  % Funcs |  % Lines |Uncovered
Lines |
----------------------------|----------|----------|----------|----------|----------
------|
 contracts/                 |    92.86 |    66.67 |      100 |    92.99 |
       |
  Mock20.sol                |      100 |      100 |      100 |      100 |
       |
  OpenmetaController.sol    |      100 |    85.71 |      100 |      100 |
       |
  OpenmetaNFT.sol           |      100 |      100 |      100 |      100 |
       |
```

```
  OpenmetaTrade.sol       |    86.25 |    58.82 |      100 |    86.42 |...
303,304,325 |
 contracts/interface/     |      100 |      100 |      100 |      100 |
       |
  IERCToken.sol           |      100 |      100 |      100 |      100 |
       |
  IMnftController.sol     |      100 |      100 |      100 |      100 |
       |
  IOpenmetaController.sol |      100 |      100 |      100 |      100 |
       |
  IOpenmetaTrade.sol      |      100 |      100 |      100 |      100 |
       |
 contracts/libraries/     |       50 |       25 |       50 |       50 |
       |
  TransferHelper.sol      |       50 |       25 |       50 |       50 |
 11,12,37,38 |
 contracts/utils/         |      100 |      100 |      100 |      100 |
       |
  BlockTimestamp.sol      |      100 |      100 |      100 |      100 |
       |
  Validation.sol          |      100 |      100 |      100 |      100 |
       |
--------------------------|----------|----------|----------|----------|----------
------|
All files                 |    90.85 |    64.15 |    95.56 |    91.07 |
       |
--------------------------|----------|----------|----------|----------|----------
------|
```



FAIRYPROOF

https://medium.com/@FairyproofT

https://twitter.com/FairyproofT

https://www.linkedin.com/company/fairyproof-tech

https://t.me/Fairyproof_tech

Reddit: https://www.reddit.com/user/FairyproofTech