ACMD 审计报告

Version 1.0.0

报告编号：2021062000011015

灵踪安全发布

2021年6月20日

01. 介绍

本报告包含了灵踪安全在ACMD团队要求下对ACMD项目代码进行审计的结果。

项目通证名：

ACMD

项目通证所在的区块链链上地址：

暂无

审计代码所在的Github仓库地址：

暂无

审计代码在Github中的commit编号：

暂无

合约所在的区块链链上地址：

暂无

审计代码文件及目录结构：

开始审计时的13个代码文件名及对应的SHA-256哈希值为：

```
ACMDToken.sol:
0xacfddfc2e8b10449adef244095394b5fccd60de1d82c431376faaa79840d1dc9

ArchimedesBank.sol:
0x95ce66eba73b6906e37cbde5b42ab9b540b3cea1940d346d879eac81ea6af081

GovernorAlpha.sol:
0x1f7d835375dd60b20f49f87cf7408a9e6cb4fbbdb47824e360c5aa28328ad690

MdxswapSpellV1.sol:
0x7797d50f64e4b55faf2187332568f934d1aebb540433bf29857238a843fb9ae9

Mining.sol:
0x42d2f8409fd8210351e898c21849bc7d7f3ed4e918442146cabf4fe0568aedd8

PriceOracleProxy.sol:
0x10e30561d112cf076fd0fca7d79f38ad02bdf572da9bdd31c0189f019939b134

ProxyOracle.sol:
0x6af6de027bdcfcbc050881a9c591e0e0c58b8da824e6bf23029605efc7eb42a0

SafeBoxChannels.sol:
0x9b5c65030a36b3e3527849ec04bacbd4be224876cefacbc541c0e63bf61f5b5f
```

```
SafeBoxHTChannels.sol:
0x1b1c1a9f8e3109ec6ce712f6e610b499225d23640ebf379a07ca0dcf233804c5

Timelock.sol:
0x9821bb4d9e5a92c66e706bc8839eb8e31212cd96aa68adf75a452bd81befd8d0

TransparentUpgradeableProxyImpl.sol:
0xb20f13a60729112cb7da85810611bf12c30165a19922c297065748fbb438781d

WERC20.sol:
0xb689fedfde9b173e7e70404ca5cebbe5cb733b162382e2ee45826373cfb1458c

WMasterChef.sol:
0xdf18ec8a0ea680455fb3fffe567de092b2b9ac7b54704da89ebb6e4c6b86da0c
```

审计代码的文件名及目录结构为：

```
contracts/
├── ACMDToken.sol
├── ArchimedesBank.sol
├── GovernorAlpha.sol
├── MdxswapSpellv1.sol
├── Mining.sol
├── PriceOracleProxy.sol
├── ProxyOracle.sol
├── SafeBoxChannels.sol
├── SafeBoxHTChannels.sol
├── Timelock.sol
├── TransparentUpgradeableProxyImpl.sol
├── WERC20.sol
└── WMasterChef.sol
```

本次审计的目的是为了审阅ACMD项目基于Solidity语言编写的杠杆挖矿协议，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ACMD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。

一 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。

一 审计方式

审计ACMD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。

灵踪安全审计的流程如下：

1. 背景研究。灵踪安全团队会阅读项目介绍、白皮书、合约源码等一切ACMD团队所提供的相关材料及信息，以确保灵踪安全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ACMD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。此步骤包括两部分：
   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。

一 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。

一 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：

项目代码文件

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ACMD团队进行了沟通和确认。

一 审计结论

经过审计，当前发现的风险数量为：致命风险：0，高危风险：0，中度风险：1，低风险：0。

结论：当前合约代码审计发现风险。

02. 灵踪安全介绍

灵踪安全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。灵踪安全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

本项目为一个杠杆挖矿协议，用户可以提供资产获取利息，也可以贷出资产用于杠杆挖矿，还可以执行清算获取超额抵押资产。

04. 审计代码的主要功能

所审计的代码主要实现了下列功能：

- 通证发行。通证名称：ACMD；发行数量：10亿枚，无增发和燃烧功能。
- 预言机。主要为项目提供特定资产的价格参考。
- 机枪池。将用户提供的资产投资于第三方平台获利。
- 杠杆借贷。用户可提供资产，出借资产或者执行清算。

注意：由于协议将资产投资到了第三方平台，因此存在由于第三方平台出现问题而遭受损失的可能。

05. 本审计的主要工作

在审计过程中，灵踪安全与项目方密切合作，主要完成了下列工作：

- 审计了通证发行情况
- 审计是否正确运用了价格预言机
- 审计了合约的实现逻辑是否正确
- 审计了其它安全问题

06. 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
- 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，Gas 限制和循环
- 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
- 设计缺陷
- 潜在后门
- 代币发行
- 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

07. 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：

致命 风险及隐患需要立刻解决。

高危 风险及隐患将引发风险及问题，必须解决。

中度 风险及隐患可能导致潜在风险，最终仍然需要解决。

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。

08. 本审计关注的风险重点

根据所审计代码的功能及应用场景，我们着重审查了下列功能中可能潜藏的风险。

- 通证发行

我们检查了通证发行是否有不合规的增发接口，以保护投资者的利益和系统的稳定运行。

经审查此功能暂未发现明显风险。

- 价格获取机制

我们重点检查了合约的价格获取机制是否存在安全隐患。

经审查此功能暂未发现明显风险。

- 合约迁移与升级

我们重点检查了合约是否可升级或迁移，以提示项目方相关风险。

经审查此功能发现风险，细节请参看“11. 问题详述”。

- 其它

经审查其它功能暂未发现明显风险。

09. 基于风险等级的问题列表

A. 致命风险

- 无

B. 高危风险

- 无

C. 中度风险

- ArchimedesBank.sol、Mining.sol，SafeBoxChannels.sol、SafeBoxHTChannels.sol

合约升级

D. 低风险

- 无

10. 基于合约文件的问题列表

- ArchimedesBank.sol、Mining.sol，SafeBoxChannels.sol、SafeBoxHTChannels.sol

合约升级：中度风险

11. 问题详述

- 合约升级：中度风险

问题位置及描述：

部分合约（`ArchimedesBank`、`Mining`，`SafeBoxChannels`与`SafeBoxHTChannels`采用了委托/代理模式，因此可以升级合约。

修改建议：

建议对新升级的合约必须进行安全审计，以防止出现数据或者逻辑错误。

项目方反馈：采取可升级的委托/代理模式是为了更好的容错及功能拓展，以便在出现预期之外的情况时及时应对处理。同时项目方会谨慎处理升级需求，在升级之前审计新的合约。

12. 增强建议

- 无