智能合约安全审计报告

1. 概要

慢雾安全团队于 2021 年 03 月 22 日，收到 DeFiBOX 团队对 reward&mining 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）

- 溢出审计
- 权限漏洞审计
- 权限过大审计
- 硬编码地址安全
- 显现编码安全
- 异常校验审计
- 类型安全审计
- 性能优化审计
- 设计逻辑审计
- 拒绝服务审计
- 回滚攻击审计
- 重放攻击审计
- 假通知审计
- 假错误通知审计
- 假币审计
- 随机数安全审计
- 粉尘攻击安全审计
- 微分叉安全审计
- 排挤攻击安全审计
- 重入攻击安全审计

3. 项目背景

3.1 项目介绍

Reward&mining 是 DeFiBOX 推出的流动性挖矿合约。

审计合约文件：

项目源代码

审计初始版本：

SHA256(reward&mining.zip)=

b81add80ae0a07227b0fcae8d7e42bd1ca6c21ca05748c5528ecb4fce497d502

审计最终版本：

SHA256(reward-04-23.zip)=

07aa2760b52dfa1d820126396c18992dbf9ba9eaabfbcd4e08ef11eabcfe4630

SHA256(lpreward-2021-05-26.zip)=

e332b71c5c9c73b4ba837703423a616d3715ecdbc4dbdd5143f20ab142d6f967

3.2 项目结构

```
mining
├── CMakeLists.txt
├── README.txt
├── cmd.txt
├── include
|   ├── mining.hpp
|   ├── structs.hpp
|   └── utils.hpp
├── ricardian
```

```
|   └── mining.contracts.md
└── src
    ├── CMakeLists.txt
    └── mining.cpp
reward
├── CMakeLists.txt
├── README.txt
├── include
|   ├── defines.hpp
|   ├── lpreward.hpp
|   ├── structs.hpp
|   └── utils.hpp
├── ricardian
|   └── lpreward.contracts.md
└── src
    ├── CMakeLists.txt
    └── lpreward.cpp
```

3.3 项目架构

reward&mining 项目主要包含 2 个合约，主要功能是用户可通过存入代币或流动性凭证挖矿获得奖励。

4. 代码概述

4.1 主要合约地址

2021-04-23:

Contract Name	Code Hash(eosio.cdt v1.6.3)
reward	47f1e735de0639e9528129e8300871183a6f1c4e40d4d6bddbc0100bd3f9b30f
mining	01de5864d450d367a15ef65f956936edaf9304901af471e7aa3bfc038936d8d4

2021-05-26:

Contract Name	Code Hash(eosio.cdt v1.6.3)
lpreward	95b09878e717de150d88ed2b8fd8bd38cdf0b0a2ecab4dfc1d88c16fdfbfd5b9

4.2 主要合约函数权限分析

在审计过程中，慢雾安全团队对核心合约的可见函数进行权限分析，结果如下:

reward		
Function Name	Visibility	Authority
createpool	Public	ADMIN_ACCOUNT
removepool	Public	ADMIN_ACCOUNT
claimall	Public	owner
ontransfer	Notify	-
btokenchange	Notify	-

mining		
Function Name	Visibility	Authority
lendexchange	Public	LEND_CONTRACT
createpool	Public	ADMIN_ACCOUNT
mdfpoolwgt	Public	ADMIN_ACCOUNT
mdfpoolrf	Public	ADMIN_ACCOUNT
mdfpooltime	Public	ADMIN_ACCOUNT
removepool	Public	ADMIN_ACCOUNT
claimall	Public	owner
depositchange	Notify	-

4.3 代码审计详情

4.3.1 严重漏洞

4.3.1.1 假充值攻击漏洞

没有校验转账`to`参数，可通过“假通知”攻击造成“假充值”。

代码位置: lpreward.cpp

```
void lpreward::ontransfer(const name &from, const name &to, const asset &quantity, const string& memo,
const name& code) {
if (from == _self) {
return;
}
int16_t type = stoi(memo);
check(type == 1 || type == 2 || type == 3, "memo error");
lp_pools lppools(LPTOKEN_CONTRACT, LPTOKEN_CONTRACT.value);
```

修复状态: 已修复

4.3.2 低危漏洞

4.3.2.2 重入攻击风险

`ontransfer`未校验`from`为`lend.defi`，攻击者可能通过使用恶意合约频繁充值提现进行重入攻击，薅取挖矿奖励。

修复状态: 已修复

修复代码: lpreward.cpp

```
void lpreward::ontransfer(const name &from, const name &to, const asset &quantity, const string& memo,
const name& code) {
if (from != LEND_CONTRACT || to != _self) {
return;
}
int16_t type = stoi(memo);
check(type == 1 || type == 2 || type == 3, "memo error");
lp_pools lppools(LPTOKEN_CONTRACT, LPTOKEN_CONTRACT.value);
```

5. 审计结果

5.1 总结

审计结论：主网合约未多签

审计编号：0X002104270002

审计时间：2021 年 04 月 27 日

复审时间：2021 年 06 月 02 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 2 个问题。其中包含 1 个严重漏洞、0 个高危漏洞、0 个中危漏洞、1 个低危漏洞。经过与项目方沟通反馈确认审计过程中发现的风险均已修复或在可承受范围内。

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