POKESWAP
智能合约安全审计
最终报告

北京长亭科技有限公司
2020年10月27日

版权声明

目录

1. 服务声明

本次审计仅针对所涉及区块链智能合约项目技术层面的安全性，对项目的法律、经济、政治以及其他目的、效力与行为不评价、不负责。

2. 服务摘要

经POKESWAP对本智能合约源码安全审计项目授权，北京长亭科技有限公司安全服务组于2020年10月16日 至 2020年10月23日，对合同与协议中的受审范围进行了安全审计，并于2020年10月27日基于初审中提出的安全问题进行了复审，确认初审中提出的非低危安全问题均已修复，安全审计结果为【通过】。

依照POKESWAP与北京长亭科技有限公司关于安全审计的协议，
初审版本为:commit 97623d6483874f61b69d3877bd5a327487b08125
复审版本为:commit ba4ad3c72c118a2b184b1e81887bf95a38d2dc29

3. 安全检测项

No.	类型	检测项	检测结果
1.	类型与关键字	数据类型	通过
2.		函数类型	通过
3.		引用类型	通过
4.		类型转换及使用	通过
5.	权限控制	函数及变量可见性设置	通过
6.		Owner权限控制	通过
7.		中继合约权限控制	通过
8.	拒绝服务	非预期回滚	通过
9.		手续费超限	通过

No.	类型	检测项	检测结果
10.	逻辑表达与控制	签名验证	通过
11.		算数精度	通过
12.		随机数生成	通过
13.		运算符使用	通过
14.		内外部函数调用	通过
15.		逻辑执行顺序	通过
16.		返回值校验	通过
17.		重放攻击	通过
18.		重排攻击	通过
19.		错误处理	通过
20.	外部实体依赖与交互	交易顺序依赖	通过
21.		时间戳依赖	通过
22.		预言机使用	通过
23.		外部合约使用/引用	通过
24.		多继承合约执行顺序	通过
25.		短地址攻击	通过
26.	特殊检查项	非预期ETH	通过

No.	类型	检测项	检测结果
27.		未初始化的存储指针	通过
28.		同名变量作用域	通过
29.		编译器版本	通过
30.		敏感信息泄露	通过
31.		CEI编码规范	通过
32.	优化项	手续费优化	通过
33.		安全组件使用	通过
34.		冗余逻辑	通过
35.		善用修饰符与语法糖	通过
36.		规范命名	通过
37.		拼写	通过
38.		合理注释	通过

4. 低危安全问题

4.1 BallsBar中收益轻微减少

漏洞成因

在PokeRouter.sol中，Swap交易量的0.05%会换成Balls，并转入BallsBar中，作为BallsBar的质押奖励。

代码如下:

contracts/PokeRouter.sol, L260-L285:

```
    function _toBuyPlatToken(address _sender,address _token, uint _amount ,address[] memory path) inter
nal {
        ...
            uint[] memory amounts = PokeLibrary.getAmountsOut(factory, _amount, path);
        ...
        TransferHelper.safeTransfer( ballsToken, stakingAddress, IERC20(ballsToken).balanceOf(address(thi
s)));
    }
```

但在换成Balls时会额外收取转换量0.25%的手续费。

消耗手续费的代码如下:

contracts/PokeRouter.sol, L260-L285:

```
function getAmountOut(uint amountIn, uint reserveIn, uint reserveOut) internal pure returns (uint amoun
tOut) {
        ...
        uint amountInWithFee = amountIn.mul(9975);
        uint numerator = amountInWithFee.mul(reserveOut);
        uint denominator = reserveIn.mul(10000).add(amountInWithFee);
        amountOut = numerator / denominator;
    }
```

由于这部分手续费消耗，BallsBar中的收益将减少0.25%.

漏洞危害

BallsBar中的总收益减少0.25%。

利用条件

无利用门槛。

修复建议

实现一个不需要手续费的getAmountOut方法，该方法仅用于合约内部的无损货币转换。

5. 致谢

在贵公司的大力配合下，本次安全深度检测得以顺利完成。北京长亭科技有限公司区块链安全服务组向POKESWAP所有参与并提供支持的部门及个人表示深深感谢。

北京长亭科技有限公司
CEO 陈宇森