慢雾科技
SLOWMIST

智能合约安全审计报告

[2021]

目录

1 前言

2 审计方法

3 项目概要

3.1 项目介绍

3.2 漏洞信息

4 审计详情

4.1 合约基础信息

4.2 函数可见性分析

4.3 漏洞详情

5 审计结果

6 声明

1 前言

慢雾安全团队于2021.05.06，收到O3 swap团队对O3 swap智能合约安全审计的申请，慢雾安全团队根据项目特点制定如下审计方案。

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。

慢雾科技项目测试方法：

测试方法	说明
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。

慢雾科技漏洞风险等级：

漏洞等级	说明
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慢雾安全团队会重点审查的漏洞列表:

（其他未知的安全漏洞及审计项不包含在本次审计责任范围）

- 重入漏洞
- 重放漏洞
- 重排漏洞
- 短地址漏洞
- 拒绝服务漏洞
- 交易顺序依赖漏洞
- 条件竞争漏洞
- 权限控制漏洞
- 整数上溢/下溢漏洞
- 时间戳依赖漏洞
- 未声明的存储指针漏洞
- 算术精度误差漏洞
- tx.origin身份验证漏洞
- 假充值漏洞
- 变量覆盖漏洞
- Gas优化审计
- 恶意 Event 事件审计
- 冗余的回调函数
- 不安全的外部调用审计

- 函数状态变量可见性审计
- 业务逻辑缺陷审计
- 变量声明及作用域审计

3 项目概要

3.1 项目介绍

O3 Swap是由O3 Labs构建的专有跨链聚合协议。 O3 Swap的使命是为消费者提供基于加密货币的金融服务，使他们能够在O3钱包内交换或“交换”各种数字资产。这种设计的好处可以归因于资产存储和保护的分散模型固有的高级别安全性。该平台还提供“跨链”兑换以进行交易结算，而无需考虑典型的隔离式区块链网络的局限性。术语“跨链”本身源自这样一个事实，即交换是在两个或多个单独的区块链网络之间旅行之后执行的。通过跨链交换，初始资产和目标资产被部署在两个隔离的区块链上，否则它们是不可通信的。鉴于去中心化金融协议（DeFi）的先进发展以及借贷，交换，衍生品等市场的日趋成熟，O3 Swap协议与其相关的去中心化钱包软件合作，提供了一站式汇总和交换消费者平台，并为开发人员提供访问开放，分布式，无限和安全的交易环境的权限。

审计初始文件信息

Github：

https://github.com/O3Labs/o3swap-aggregator-contracts

commit: c46ed522534fdfc279344a4945e9159241f2c9bf

Github:

https://github.com/O3Labs/o3swap-contracts

commit: 53c009e09ece07328a3a566262dbc4f8a1697478

修复文件信息

Github：

https://github.com/O3Labs/o3swap-aggregator-contracts

commit: ee0b0c395ce165c163449d5db36f83d673a5ef08

Github:

https://github.com/O3Labs/o3swap-contracts

commit: 57884e1ae1d3c7d08b7fc3c61339532d1d9791f0

3.2 漏洞信息

如下是本次审计发现的漏洞及漏洞的修复状态信息：

NO	标题	漏洞类型	漏洞等级	漏洞状态
N1	未检查 pair 是否存在	其它	建议	已修复
N2	权限过大问题	权限控制攻击	中	已修复

4 审计详情

4.1 合约基础信息

如下是合约主网地址：

目前代码还未部署到主网。

4.2 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函数可见性进行分析，结果如下：

Context			
Function Name	Visibility	Mutability	Modifiers

Context			
_msgSender	internal	-	-
_msgData	internal	-	-

Ownable			
Function Name	Visibility	Mutability	Modifiers
_msgSender	internal	-	-
_msgData	internal	-	-
constructor	internal	can modify state	-
owner	public	-	-
renounceOwnership	public	can modify state	onlyOwner
transferOwnership	public	can modify state	onlyOwner

O3SwapBSCPancakeBridge			
Function Name	Visibility	Mutability	Modifiers
constructor	internal	can modify state	-
owner	public	-	-
renounceOwnership	public	can modify state	onlyOwner
transferOwnership	public	can modify state	onlyOwner
_msgSender	internal	-	-
_msgData	internal	-	-
constructor	public	can modify state	-

O3SwapBSCPancakeBridge			
swapExactTokensForTokensSupportingFeeOnTransferTokens	external	can modify state	ensure
swapExactTokensForTokensSupportingFeeOnTransferTokensCrossChain	external	payable	ensure
_swapExactTokensForTokensSupportingFeeOnTransferTokens	internal	can modify state	-
swapExactETHForTokensSupportingFeeOnTransferTokens	external	payable	ensure
swapExactETHForTokensSupportingFeeOnTransferTokensCrossChain	external	payable	ensure
_swapExactETHForTokensSupportingFeeOnTransferTokens	internal	can modify state	-
swapExactTokensForETHSupportingFeeOnTransferTokens	external	can modify state	ensure
_swapExactTokensForETHSupportingFeeOnTransferTokens	internal	can modify state	-
_swapSupportingFeeOnTransferTokens	internal	can modify state	-
_cross	internal	can modify state	-
receive	external	payable	-
setPolySwapperId	external	can modify state	onlyOwner
collect	external	can modify state	-
setAggregatorFee	external	can modify state	onlyOwner
setPancakeFactory	external	can modify state	onlyOwner
setPolySwapper	external	can modify state	onlyOwner
setWBNB	external	can modify state	onlyOwner

ReentrancyGuard			

ReentrancyGuard			
Function Name	Visibility	Mutability	Modifiers
constructor	internal	can modify state	-

O3Staking			
Function Name	Visibility	Mutability	Modifiers
constructor	internal	can modify state	-
constructor	internal	can modify state	-
owner	public	-	-
renounceOwnership	public	can modify state	onlyOwner
transferOwnership	public	can modify state	onlyOwner
_msgSender	internal	-	-
_msgData	internal	-	-
constructor	public	can modify state	-
getTotalProfit	external	-	-
getStakingAmount	external	-	-
getSharePerBlock	external	-	-
setStakingToke	external	can modify state	onlyOwner,*logs*
setSharePerBlock	external	can modify state	onlyOwner,*logs*
setStartUnstakeBlockIndex	external	can modify state	onlyOwner,*logs*
setStartClaimBlockIndex	external	can modify state	onlyOwner,*logs*

O3Staking			
stake	external	can modify state	nonReentrant,*logs*
unstake	external	can modify state	nonReentrant,*logs*
claimProfit	external	can modify state	nonReentrant,*logs*
_getTotalProfit	internal	can modify state	-
_updateUserStakingRecord	internal	can modify state	-
_settleCurrentUserProfit	internal	-	-
_updateUnitProfitState	internal	can modify state	-
_updateUnitProfit	internal	can modify state	-
pauseStaking	external	can modify state	onlyOwner,*logs*
unpauseStaking	external	can modify state	onlyOwner,*logs*
pauseUnstake	external	can modify state	onlyOwner,*logs*
unpauseUnstake	external	can modify state	onlyOwner,*logs*
pauseClaimProfit	external	can modify state	onlyOwner,*logs*
unpauseClaimProfit	external	can modify state	onlyOwner,*logs*
collect	external	can modify state	nonReentrant,onlyOwner,*logs*
_pushToken	internal	can modify state	-
_pushShareToken	internal	can modify state	-
_pullToken	internal	can modify state	-

O3SwapETHUniswapBridge			

O3SwapETHUniswapBridge			
Function Name	Visibility	Mutability	Modifiers
constructor	internal	can modify state	-
owner	public	-	-
renounceOwnership	public	can modify state	onlyOwner
transferOwnership	public	can modify state	onlyOwner
_msgSender	internal	-	-
_msgData	internal	-	-
constructor	public	can modify state	-
swapExactTokensForTokensSupportingFeeOnTransferTokens	external	can modify state	ensure
swapExactTokensForTokensSupportingFeeOnTransferTokensCrossChain	external	payable	ensure
_swapExactTokensForTokensSupportingFeeOnTransferTokens	internal	can modify state	-
swapExactETHForTokensSupportingFeeOnTransferTokens	external	payable	ensure
swapExactETHForTokensSupportingFeeOnTransferTokensCrossChain	external	payable	ensure
_swapExactETHForTokensSupportingFeeOnTransferTokens	internal	can modify state	-
swapExactTokensForETHSupportingFeeOnTransferTokens	external	can modify state	ensure
_swapExactTokensForETHSupportingFeeOnTransferTokens	internal	can modify state	-
_swapSupportingFeeOnTransferTokens	internal	can modify state	-
_cross	internal	can modify state	-

O3SwapETHUniswapBridge			
receive	external	payable	-
setPolySwapperId	external	can modify state	onlyOwner
collect	external	can modify state	-
setAggregatorFee	external	can modify state	onlyOwner
setUniswapFactory	external	can modify state	onlyOwner
setPolySwapper	external	can modify state	onlyOwner
setWETH	external	can modify state	onlyOwner

O3SwapHecoMdexBridge			
Function Name	Visibility	Mutability	Modifiers
constructor	internal	can modify state	-
owner	public	-	-
renounceOwnership	public	can modify state	onlyOwner
transferOwnership	public	can modify state	onlyOwner
_msgSender	internal	-	-
_msgData	internal	-	-
constructor	public	can modify state	-
swapExactTokensForTokensSupportingFeeOnTransferTokens	external	can modify state	ensure
swapExactTokensForTokensSupportingFeeOnTransferTokensCrossChain	external	payable	ensure
_swapExactTokensForTokensSupportingFeeOnTransferTokens	internal	can modify state	-

O3SwapHecoMdexBridge			
swapExactETHForTokensSupportingFeeOnTransferTokens	external	payable	ensure
swapExactETHForTokensSupportingFeeOnTransferTokensCrossChain	external	payable	ensure
_swapExactETHForTokensSupportingFeeOnTransferTokens	internal	can modify state	-
swapExactTokensForETHSupportingFeeOnTransferTokens	external	can modify state	ensure
_swapExactTokensForETHSupportingFeeOnTransferTokens	internal	can modify state	-
_swapSupportingFeeOnTransferTokens	internal	can modify state	-
_cross	internal	can modify state	-
receive	external	payable	-
setPolySwapperId	external	can modify state	onlyOwner
collect	external	can modify state	-
setAggregatorFee	external	can modify state	onlyOwner
setMdexFactory	external	can modify state	onlyOwner
setPolySwapper	external	can modify state	onlyOwner
setWHT	external	can modify state	onlyOwner

ERC20			
Function Name	Visibility	Mutability	Modifiers
totalSupply	external	-	-
balanceOf	external	-	-

ERC20			
transfer	external	can modify state	-
allowance	external	-	-
approve	external	can modify state	-
transferFrom	external	can modify state	-
_msgSender	internal	-	-
_msgData	internal	-	-
constructor	public	can modify state	-
name	public	-	-
symbol	public	-	-
decimals	public	-	-
totalSupply	public	-	-
balanceOf	public	-	-
transfer	public	can modify state	-
allowance	public	-	-
approve	public	can modify state	-
transferFrom	public	can modify state	-
increaseAllowance	public	can modify state	-
decreaseAllowance	public	can modify state	-
_transfer	internal	can modify state	-
_mint	internal	can modify state	-

ERC20			
_burn	internal	can modify state	-
_approve	internal	can modify state	-
_setupDecimals	internal	can modify state	-
_beforeTokenTransfer	internal	can modify state	-

O3			
Function Name	Visibility	Mutability	Modifiers
constructor	internal	can modify state	-
getUnlockFactor	external	-	-
getUnlockBlockGap	external	-	-
totalUnlocked	external	-	-
unlockedOf	external	-	-
lockedOf	external	-	-
getStaked	external	-	-
getUnlockSpeed	external	-	-
claimableUnlocked	external	-	-
setUnlockFactor	external	can modify state	-
setUnlockBlockGap	external	can modify state	-
stake	external	can modify state	-
unstake	external	can modify state	-

O3			
claimUnlocked	external	can modify state	-
setAuthorizedMintCaller	external	can modify state	-
removeAuthorizedMintCaller	external	can modify state	-
mintUnlockedToken	external	can modify state	-
mintLockedToken	external	can modify state	-
totalSupply	external	-	-
balanceOf	external	-	-
transfer	external	can modify state	-
allowance	external	-	-
approve	external	can modify state	-
transferFrom	external	can modify state	-
constructor	internal	can modify state	-
owner	public	-	-
renounceOwnership	public	can modify state	onlyOwner
transferOwnership	public	can modify state	onlyOwner
_msgSender	internal	-	-
_msgData	internal	-	-
constructor	public	can modify state	-
name	public	-	-
symbol	public	-	-

O3			
decimals	public	-	-
totalSupply	public	-	-
balanceOf	public	-	-
transfer	public	can modify state	-
allowance	public	-	-
approve	public	can modify state	-
transferFrom	public	can modify state	-
increaseAllowance	public	can modify state	-
decreaseAllowance	public	can modify state	-
_transfer	internal	can modify state	-
_mint	internal	can modify state	-
_burn	internal	can modify state	-
_approve	internal	can modify state	-
_setupDecimals	internal	can modify state	-
_beforeTokenTransfer	internal	can modify state	-
constructor	public	can modify state	-
getUnlockFactor	external	-	-
getUnlockBlockGap	external	-	-
totalUnlocked	external	-	-
unlockedOf	external	-	-

O3			
lockedOf	public	-	-
getStaked	external	-	-
getUnlockSpeed	external	-	-
claimableUnlocked	external	-	-
transfer	public	can modify state	-
transferFrom	public	can modify state	-
setUnlockFactor	external	can modify state	onlyOwner
setUnlockBlockGap	external	can modify state	onlyOwner
stake	external	can modify state	nonReentrant
unstake	external	can modify state	nonReentrant
claimUnlocked	external	can modify state	nonReentrant
_updateStakeRecord	internal	can modify state	-
mintUnlockedToken	external	can modify state	onlyAuthorizedMintCaller
mintLockedToken	external	can modify state	onlyAuthorizedMintCaller
setAuthorizedMintCaller	external	can modify state	onlyOwner
removeAuthorizedMintCaller	external	can modify state	onlyOwner
_settleUnlockAmount	internal	-	-
_mintUnlocked	internal	can modify state	-
_getUnlockSpeed	internal	-	-
_unlockTransfer	internal	can modify state	-

O3			
_pullToken	internal	can modify state	-
_pushToken	internal	can modify state	-

4.3 漏洞详情

[N1] [建议] 未检查 pair 是否存在

漏洞类型: 其它

详细内容

O3swapBSCPancakeBridge / O3swapETHUniswapBridge / O3swapHecoMdexBridge 合约的

_swapSupportingFeeOnTransferTokens 函数未检验 pair 是否存在，导致兑换失败

```
function _swapSupportingFeeOnTransferTokens(address[] memory path, address _to)
internal virtual {
        for (uint i; i < path.length - 1; i++) {
            (address input, address output) = (path[i], path[i + 1]);
            (address token0,) = PancakeLibrary.sortTokens(input, output);
            //SlowMist// 这里没有检查pair 是否存在，导致兑换失败
            IPancakePair pair = IPancakePair(PancakeLibrary.pairFor(pancakeFactory,
input, output));
            uint amountInput;
            uint amountOutput;
            { // scope to avoid stack too deep errors
            (uint reserve0, uint reserve1,) = pair.getReserves();
            (uint reserveInput, uint reserveOutput) = input == token0 ? (reserve0,
reserve1) : (reserve1, reserve0);
            amountInput = IBEP20(input).balanceOf(address(pair)).sub(reserveInput);
            amountOutput = PancakeLibrary.getAmountOut(amountInput, reserveInput,
reserveOutput);
            }
            (uint amount0Out, uint amount1Out) = input == token0 ? (uint(0),
amountOutput) : (amountOutput, uint(0));
            address to = i < path.length - 2 ? PancakeLibrary.pairFor(pancakeFactory,
output, path[i + 2]) : _to;
            pair.swap(amount0Out, amount1Out, to, new bytes(0));
        }
    }
```

解决方案

建议添加检查

漏洞状态

已修复

[N2] [中] 权限过大问题

漏洞类型: 权限控制攻击

详细内容

O3staking 合约的 collect 函数可以转出合约中的任何代币，包括用户的资产，存在权限过大问题，建议限制 token != stakingToken

```
    function collect(address token, address to) external nonReentrant onlyOwner
 _logs_ {
        //SlowMist// 权限过大问题，应该限制 token != stakingToken 本身
        uint balance = IERC20(token).balanceOf(address(this));
        _pushToken(token, to, balance);
    }
```

解决方案

限制转出 token 不能为 stakingToken

漏洞状态

已修复

5 审计结果

审计编号	审计团队	审计日期	审计结果

审计编号	审计团队	审计日期	审计结果
0X002105140001	SlowMist Security Team	2021.05.06 - 2021.05.14	通过

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 1 个中危漏洞， 1 个增强建议。其中 1个中危漏洞，1 个增强建议已确认；所有漏洞均已修复。

6 声明

厦门慢雾科技有限公司(下文简称 ”慢雾”) 仅就本报告出具前项目方已经发生或存在的事实出具本报告，并就此承担相应责任。对于出具以后项目方发生或存在的未知漏洞及安全事件，慢雾无法判断其安全状况，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，慢雾仅对该项目的安全情况进行约定内的安全审计并出具了本报告，慢雾不对该项目背景及其他情况进行负责。

慢雾科技
SLOWMIST

官方网址

www.slowmist.com

电子邮箱

team@slowmist.com

微信公众号