

智能合约安全审计报告



Ocean 智能合约安全审计报告

审计团队：零时科技安全团队

时间：2021-03-07

Ocean智能合约安全审计报告

1.概述

零时科技安全团队于2021年03月06日，接到 **Ocean项目**的安全审计需求，团队与2021年03月06日至2021年03月07日对 **Ocean智能合约** 进行了安全审计，审计过程中零时科技安全审计专家与Ocean项目相关接口人进行沟通，保持信息对称，在操作风险可控的情况下进行安全审计工作，尽量规避在测试过程中对项目产生和运营造成风险。

经过与Ocean项目方沟通反馈确认审计过程中发现的漏洞及风险均已修复或在可承受范围内，本次Ocean智能合约安全审计结果：通过安全审计。

合约报告MD5：E004C2EF8FDC06A255803F4BB7D6E327

2.项目背景

2.1 项目简介

项目名称：Ocean

项目官网：<https://oceandao.finance/>

合约类型：代币合约

代码语言：Solidity

官方GitHub仓库地址：<https://github.com/oceanswap/ocean-core/tree/audit>

合约文件：Ocean.sol，OceanPool.sol，LPTokenWrapper.sol

2.2 审计范围

Ocean官方提供合约及MD5：

Ocean.sol 24a950aaf94011d6b58a39026c68ab3d

OceanPool.sol d41e96bab1230fbebe17b7f61ab5d0c2

LPTokenWrapper.sol 500f255429d1d3e686e1383ac97f61b4

2.3 安全审计项

零时科技安全专家对约定内的安全审计项目进行安全审计，本次智能合约安全审计的范围，不包含未来可能出现的新型攻击方式，不包含合约升级活篡改后的代码，不包括在后续跨链部署时的操作过程，不包含项目前端代码安全与项目平台服务器安全。

本次智能合约安全审计项目包括如下：

- 整数溢出
- 重入攻击
- 浮点数和数值精度
- 默认可见性
- Tx.origin身份验证
- 错误的构造函数
- 未验证返回值
- 不安全的随机数
- 时间戳依赖
- 交易顺序依赖
- Delegatecall调用
- Call调用
- 拒绝服务
- 逻辑设计缺陷
- 假充值漏洞
- 短地址攻击
- 未初始化的存储指针
- 代币增发
- 冻结账户绕过
- 权限控制
- Gas使用

3.合约架构分析

3.1 目录结构

```

└─contracts
  │ Ocean.sol
  └─distribution
    │ OceanPool.sol
    └─token
      └─LPTokenWrapper.sol

```

3.2 OceanPool合约

Contract

OceanPool

- shutdown()
- lastTimeRewardApplicable()
- rewardPerToken()
- earned(address account)
- stake(uint256 amount)
- withdraw(uint256 amount)
- exit()
- getReward()
- transferBack(address back, uint256 amount)
- notifyRewardAmount(uint256 reward)
- earnedShutdown(address account)
- rewardPerTokenShutdown()

3.3 LPTokenWrapper合约

Contract

LPTokenWrapper

- totalSupply()
- balanceOf(address account)
- stake(uint256 amount)
- withdraw(uint256 amount)

3.4 Ocean合约

Contract

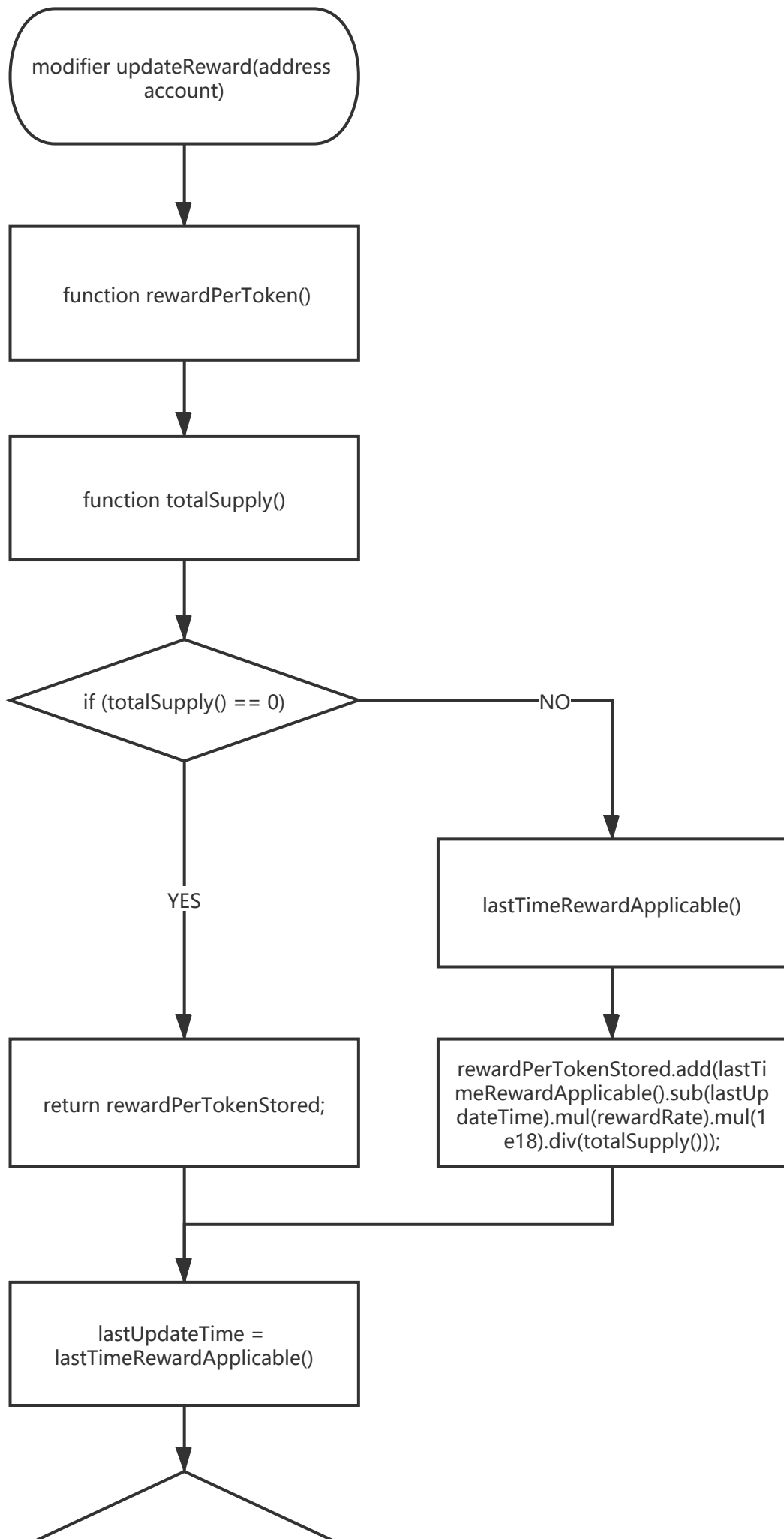
Ocean

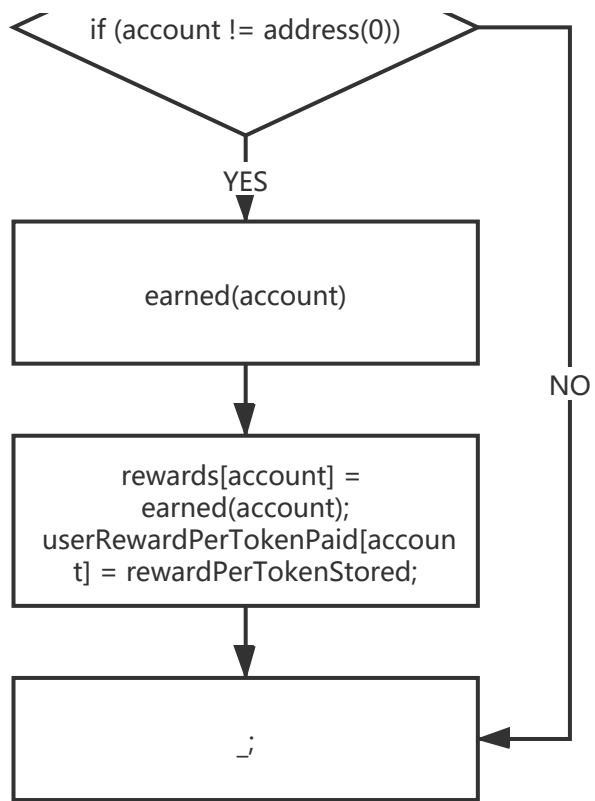
- mint(address recipient, *uint256 amount*)
- burn(uint256 amount)
- burnFrom(address account, uint256 amount)
- _beforeTokenTransfer(address from, address to, uint256 amount)

3.5 合约部分逻辑流程图

通过对Ocean合约的安全审计，安全审计人员列出了审计过程中部分合约逻辑的代码流程图，如下：

OceanPool合约部分逻辑：updateReward()





4.审计详情

4.1 漏洞分布

本次安全审计漏洞风险按危险等级分布：

漏洞风险等级分布			
高危	中危	低危	通过
0	0	0	21



本次智能合约安全审计高危漏洞0个，中危0个，低危0个，通过21个，安全等级高。

4.2 漏洞详情

对约定内的智能合约进行安全审计，未发现可以直接利用并产生安全问题的安全漏洞，通过安全审计。

4.3 其他风险

其他风险是指合约安全审计人员认为有风险的代码，在特定情况下可能会影响项目稳定性，但不能构成直接危害的安全问题。

4.3.1 管理员权限过大问题

- 发生原因

如果智能合约中的管理员权限较大，当管理者账户私钥不慎丢失或者被恶意人员所操控，可能会影响项目稳定性。

- 问题点

通过审计合约发现，合约中部分的设置，更新，逻辑操作功能由管理者来操作，存在安全隐患。如果管理者账户私钥不慎丢失或者被恶意人员所操控，将会影响项目稳定性。

- 安全建议

需安全有效存储部署者地址私钥，避免丢失或者被恶意人员获取，将风险降到最低。

5.安全审计工具

工具名称	功能
Oyente	可以用来检测智能合约中常见bug
securify	可以验证以太坊智能合约的常见类型
MAIAN	可以查找多个智能合约漏洞并进行分类
零时内部工具包	零时科技内部审计工具包+ https://audit.noneage.com

6.漏洞风险评估标准

漏洞等级	漏洞风险描述
高危	能直接导致代币合约或者用户数字资产损失的漏洞，比如：整数溢出漏洞、假充值漏洞、重入漏洞、代币违规增发等。能直接造成代币合约所有权变更或者验证绕过的漏洞，比如：权限验证绕过、call代码注入、变量覆盖、未验证返回值等。能直接导致代币正常工作的漏洞，比如：拒绝服务漏洞、不安全的随机数等。
中危	需要一定条件才能触发的漏洞，比如代币所有者高权限触发的漏洞，交易顺序依赖漏洞等。不能直接造成资产损失的漏洞，比如函数默认可见性错误漏洞，逻辑设计缺陷漏洞等。
低危	难以触发的漏洞，或者不能导致资产损失的漏洞，比如需要高于攻击收益的代价才能触发的漏洞 无法导致安全漏洞的错误编码问题。

免责声明：

零时科技仅就本报告出具之前发生或存在的事实出具报告并承担相应责任，对于出具报告之后发生的事实由于无法判断智能合约安全状态，因此不对此承担责任。零时科技对该项目约定内的安全审计项进行安全审计，不对该项目背景及其他情况进行负责，项目方后续的链上部署以及运营方式不在本次审计范围。本报告只基于信息提供者截止出具报告时向零时科技提供的信息进行安全审计，对于此项目的信息有隐瞒，或反映的情况与实际情况不符的，零时科技对由此而导致的损失和不利影响不承担任何责任。



咨询电话：86-17391945345 18511993344

邮箱：support@noneage.com

官网：www.noneage.com

微博：weibo.com/noneage

