智能合约安全审计报告

HydroSwap

SECBIT

Aug 14, 2018

1. 综述

HydroSwap 合约是基于 0x 协议的 Token（及ETH）之间的兑换合约，其目的是实现各ERC20 Token 及 ETH 之间的币币交换。安比（SECBIT）实验室于 2018 年 8 月 12 日至 2018 年 8 月 14 日对合约进行审计。审计过程从**代码漏洞**，**逻辑漏洞**和**发行风险评估**三个维度对合约进行分析。审计结果表明，HydroSwap 合约并未包含致命的安全漏洞，代码质量较高。安比（SECBIT）实验室给出了如下发行风险提示项（详见第4章节）。

风险类型	描述	风险级别
发行风险	HydroSwap 合约在交易中需承担额外的手续费	低

2. 合约信息

该部分描述了合约的基本信息和代码组成。

2.1 基本信息

名称	HydroSwap
行数	77
文件来源	项目方
文件哈希	62561c7c55c4864e00288ac5e3ab2f671ce436e0
合约阶段	尚未部署
依赖合约	WETH，Exchange(0x)，TokenTransferProxy(0x)

2.2 合约函数列表

以下展示了 HydroSwap 合约包含的函数:

函数	行数	描述
constructor	6	构造函数，设置WETH，Exchange(0x)，TokenTransferProxy(0x)合约地址
swap	6	Token 或 ETH 交换

3. 合约分析

该部分描述了合约代码的详细分析内容，从 HydroSwap 合约功能，外部依赖合约相关功能两部分来进行说明。

3.1 HydroSwap 合约功能

HydroSwap 合约包含两个函数构造函数和 swap() 函数

1. 构造函数

   设置exchangeAddress，tokenProxyAddress，wethAddress，一旦设置后就不可变。

   exchangeAddress：交易合约地址

   tokenProxyAddress：Token 转账代理合约地址

   wethAddress：WETH Token 合约地址

2. swap() 函数

   这一部分是合约的核心部分，是基于 0x 协议的币币转账协议。

   在 0x 协议中有两个角色：taker和maker。maker 创建订单并签名，taker 填写订单。 本合约作为中间角色，替代了 0x 协议中的 taker 的角色，简化了maker签名订单的流程，并且实现了 ETH 和 token 间的转账。

1. taker 账户（即函数的调用者）将 ETH 或 Token 转入 HydroSwap 合约中。
    - 若为 ETH 则转入 WETH 合约中， HydroSwap 合约地址的账户增加相应额度的 WETH
    - 若为 token 则在调用该函数前应给与当前合约足够额度的授权）
2. 当前合约授权代理合约对于额度的 token转账权限。
3. 当前合约到 Exchange 合约中填写订单，完成转账。若交易失败，则抛出异常。
4. 当前合约将 maker 账户中要转出的 ETH 或 Token 转入 taker 地址。

3.2 外部依赖合约

1. ETH 的 Token 化合约 (WETH)

   将 ETH 转入该合约兑换相应数量的 WETH，也可将账户中的 WETH 兑换出相应的 ETH 转出，以 Token 的形式来执行 ETH 转账
2. 0x 协议代币交换合约(Exchange)

   Token 交易合约，与本合约相关的仅填写订单 `fillOrder()` 接口
3. 0x 协议代理合约(TokenTransferProxy)

   Exchange 合约中进行授权转账的代理合约

4. 审计详情

该部分描述合约审计流程和详细结果。

4.1 审计过程

本次审计工作，严格按照安比（SECBIT）实验室审计流程规范执行，从代码漏洞，逻辑问题以及合约发行风险三个维度进行全面分析。审计流程大致分为四个步骤:

- 各审计小组对合约代码进行逐行分析，根据合约审计内容要求进行审计
- 各审计小组对合约漏洞和风险进行评估
- 审计小组之间交换审计结果，并对审计结果进行逐一审查和确认
- 审计小组配合审计负责人生成审计报告

4.2 审计结果

本次审计首先经过安比（SECBIT）实验室推出的分析工具 SECBIT Solidity Static Analysis Extension（内部版本） 和 sf-checker（内部版本）检查，再利用开源安全分析工具 Mythril（0.8.19版本）检查，检查结果由审计小组成员详细确认。审计小组成员对合约源码进行逐行检查、评估，汇总审计结果。

编号	分类	结果
1	合约各功能能够正常执行	√
2	合约代码不存在明显的漏洞（如整数溢出）	√
3	能够通过编译器的编译并且编译器没有任何警告输出	√
4	合约代码能够通过常见检测工具检测，并无明显漏洞	√
5	不存在明显的 Gas 损耗	√
6	底层调用（call，delegatecall，callcode）或内联汇编的操作不存在安全隐患	√
7	代码中不包含已过期或被废弃的用法	√
8	代码实现清晰明确，函数可见性定义明确，变量数据类型定义明确，合约版本号明确	√
9	不存在冗余代码	√
10	不存在受时间和外部网络环境影响的隐患	√
11	业务逻辑实现清晰明确	√
12	代码实现逻辑与注释等资料保持一致	√
13	代码不存在设计意图中未提及的逻辑	√
14	业务逻辑实现不存在疑义	√

4.3 风险提示

安比（SECBIT）实验室在对 HydroSwap 合约风险进行评估以后，指出合约存在如下风险项：

- HydroSwap 合约在交易中需承担额外的手续费
  - 风险级别：**低**
  - 风险描述：在 0x 协议的代币交易过程中，交易双方需承担一定的手续费，taker 部分费用由 HydroSwap 合约承担，但在实际的 taker（即 HydroSwap 合约调用者）与 HydroSwap 合约交换代币的过程中，并没有支付费用。因而这部分费用只能由 HydroSwap 合约自行承担。
    - 若 HydroSwap 合约中没有足够的 ZRX Token 来支付手续费，会导致交易失败。
    - 若手续费金额较高时，存在通过一定手段构造订单数据，套取手续费的风险。

5. 结论

安比（SECBIT）实验室在对 HydroSwap 合约进行分析后，并未发现严重的代码缺陷和漏洞，代码质量较高。HydroSwap 合约本质上是基于 0x 协议的 Token 交换合约，巧妙的将 ETH 转换为 Token 实现与 Token 之间的兑换。另外，合约发行中存在 1 项风险点，上文已给出具体的分析说明。

免责声明

SECBIT 智能合约安全审计从合约代码质量、合约逻辑设计和合约发行风险等方面对合约的正确性、安全性、可执行性进行审计，但不做任何和代码的适用性、商业模式和管理制度的适用性及其他与合约适用性相关的承诺。本报告为技术信息文件，不作为投资指导，也不为代币交易背书。

附录

漏洞风险级别介绍

风险级别	风险描述
高	可以严重损害合约完整性的缺陷，能够允许攻击者盗取以太币及Token，或者把以太币锁死在合约里等缺陷。
中	在一定限制条件下能够损害合约安全的缺陷，造成某些参与方利益损失的缺陷。
低	并未对合约安全造成实质损害的缺陷。
信息	不会带来直接的风险，但与合约安全实践或合约合理性建议有关的信息。

安比（SECBIT）实验室致力于参与共建共识、可信、有序的区块链经济体。

https://www.secbit.io

audit@secbit.io

@secbit_io