hpt.finance 合约
智能合约安全审计复审报告

北京长亭科技有限公司

2021 年 02 月 10 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

经北京火币天下网络技术有限公司对本次合约安全审计项目授权，北京长亭科技有限公司区块链安全服务组在 2021 年 02 月 07 日 至 2021 年 02 月 09 日，对与北京火币天下网络技术有限公司合同与协议中限定的受审范围进行了安全审计。并于 2021 年 02 月 10 日对初审发现的安全漏洞进行复审。审计过程严格按照合同与协议中规定的审计范围进行。

目标版本合约安全审计发现的安全问题均已修复。

- **getCompAddress 函数实现错误，导致主要功能失效 [已修复]**
- **中心化预言机存在被操纵风险【已修复】**

3. 审计版本与范围

依照北京火币天下网络技术有限公司与北京长亭科技有限公司关于安全审计的合同与协议，本次合约安全审计目标版本为：

https://github.com/huobipool-community/hpt.finance
3b2ecd661c0008889c923635e65b9d75a9627e38

最终复审目标版本为:
https://github.com/huobipool-community/hpt.finance
9826fb61c34afb02485f9fa1d189c56a5dd35859

4. 项目概况

本次智能合约代码审计目标是基于 Compound Protocol 二次开发的去中心化金融项目 hpt.finance。项目的总代码量为 5488 行，指定的编译器版本为 ^0.5.16。

项目核心是 CToken 合约，主要实现了放贷与赎回、借钱与还钱、代还与清算等经济学功能。

此外，项目中还包含安全数学库、利息模型和项目管理等相关合约。

此合约项目的优秀特点:

1. 预言机有严格的身份验证，有效避免了价格被非法操纵的风险。
2. 预言机可批量喂价。
3. 利息模型更适合火币生态链，避免了利息计算错误导致的损失。

4. 变量、函数、事件及返回值命名规范，能够明确体现含义与功能。
5. 变量与函数的可见性定义明确合理。

5. 安全问题修复详情

5.1. getCompAddress 函数实现错误，导致主要功能失效

漏洞成因

Comptroller 合约定义了 getCompAddress 函数来硬编码治理代币的地址。
contracts/Comptroller.sol: L1374-L1380:

```
/**
* @notice Return the address of the COMP token
* @return The address of COMP
*/
function getCompAddress() public view returns (address) {
  return 0xc00e94Cb662C3520282E6f5717214004A7f26888;
}
```

可见该地址并非 Huobi ECO Chain 上的 hpt.finance 治理代币地址。

由于关键用户函数均会在底层调用 getCompAddress,该错误将导致主要功能无法正常运行。

漏洞危害

该漏洞将导致该借贷项目的大部分用户接口无法使用。

利用条件

该漏洞没有利用条件，一旦合约部署，相关接口就会失效。

修复建议

修改 Comptroller.sol 和 ComptrollerG3.sol 中的 getCompAddress 函数，将返回值改为 hpt.finance 的治理代币地址。

修复描述

getCompAddress 函数代码如下，
contracts/Comptroller.sol, L1378-L1380:

```
function getCompAddress() public view returns (address) {
    return 0xE499Ef4616993730CEd0f31FA2703B92B50bB536;
}
```

可见 COMP 治理代币的地址已经修改。

漏洞已修复。

5.2. 中心化预言机存在被操纵风险

漏洞成因

项目中的 SimplePriceOracle 合约实现了用于喂价的预言机。该预言机仅能被 admin 用户操作，属于中心化预言机。

该中心化预言机的安全性取决于两个方面:

1. admin 账户的安全
2. 数据源的可靠性

一般来说，SimplePriceOracle 的喂价数据来源是链上 top10 的 Exchanges。如果这些 Exchanges 的总深度较小，Oracle 中的 Token 价格将会被恶意操纵，hpt.finance 的安全也将受到威胁。

漏洞危害

攻击者可利用该漏洞操纵 hpt.finance 中的 token 价格，从而实现对市场的控制，最终实现套利。

利用条件

假设有受害者 borrowerA 抵押 ETH 借出 USDT。

攻击者在 Oracle 的数据源 Exchanges 中进行大宗的 ETH -> USDT Swap 交易，以此来压低 ETH 价格。

由于 ETH 价格下跌,borrowerA 的抵押总价值小于已贷出的 USDT 所需的保证金价值。因此，borrowerA 将被清算。

攻击者立刻以当前 ETH 价格清算 borrowerA 获得了大量 cETH,接着调平 Exchanges 中的 ETH 价格。

最终，攻击者出售从 borrowerA 处非法获取的大量 cETH 实现获利。

修复建议

建议实现一个去中心化的预言机系统，或者增加 Oracle 数据源的数量，以此提高攻击者操纵币价的成本。

修复描述

预言机合约添加了对多个数据源进行整合处理的代码。

contracts/SimplePriceOracle.sol, L41-L57:

```
{
    uint price = totalPrice / totalNum;
    uint price1 = prices1[address(CErc20(address(cToken)).underlying())];
    uint price2 = prices2[address(CErc20(address(cToken)).underlying())];
```

```
    uint price3 = prices3[address(CErc20(address(cToken)).underlying())];
    if (price1 < price) {
        return price2 < price3 ? price2 : price3;
    }
    else if (price2 < price) {
        return price1 < price3 ? price1 : price3;
    }
    else if (price3 < price) {
        return price1 < price2 ? price1 : price2;
    } else { //价格一样
        return price1;
    }
}
```

可见，预言机使用多三个数据源的中位数作为喂价数据。这提高了攻击者通过操纵市场进行攻击的成本。

漏洞已修复。

6. 代码优化建议

6.1.Market 缺少 borrow limit 限制

优化原因

hpt.finanace 当前使用的 Comptroller 版本为 G4，截止到报告编写时 Comptroller 合约的最新版本为 G7。

G4 版本中 Market 缺少 borrow limit 上限。

在少数极端情况下，supplier 提供的 liquidity 很少，而 borrower 的贷款需求又相对较大时，Market 将被借空。此时，supplier 必须等待 borrower 还清贷款才能赎回自己的资产。

borrow limit 限制了 Market.totalCash 中 totalBalance 的最大占比。当市场的总放款量超过了 borrow limit，Market 将暂时关闭 borrow 功能。

因此，borrow limit 的引入一定程度上保障了 supplier 的权益。

优化建议

将 Comptroller 代码更新为 G7 版本。

6.2.建议删除清算激励因子的最值限制

优化原因

G4 版本的 Comptroller 限制了 liquidationIncentive 的大小范围，这使得 admin 对市场的宏观调控能力受到约束。

在少数极端情况下，如果最大化的激励因子也无法有效刺激违约贷款的清算，那么 supplier 会因无法赎回资产而蒙受损失。

优化建议

将 Comptroller 代码更新为 G7 版本。

7. 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北京火币天下网络技术有限公司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