链安全审计报告

DeepBrainChain 公链安全审计报告

审计团队：零时科技安全团队

时间：2021-05-19

DeepBrainChain安全 审计报告

1. 概述

零时科技安全团队于2021年5月10日至5月14日对**DeepBrainChain**项目进行了安全审计，这次审计主要关注于代码本身，对代码内容及引用库、依赖库的安全性进行了分析。在本次审计中，代码本身并未出现严重的安全问题，也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。

本次 **DeepBrainChain** 项目安全审计结果：**通过审计。**

审计报告MD5：9CBF12C2D32B862D8D73597341E58F2E

2. 项目背景

2.1 项目简介

> 项目名称：DeepBrainChain
>
> 项目官网：https://www.deepbrainchain.org/
>
> 代码仓库：https://github.com/DeepBrainChain/DeepBrainChain-MainChain/tree/v0.2
>
> 审计版本：commit e97c29ab9f2c5a10a51247d34497cb1851091250
>
> 主要编码语言：Rust

2.2 审计范围

> 代码仓库：https://github.com/DeepBrainChain/DeepBrainChain-MainChain

2.3 安全审计项

零时科技安全团队对约定内的安全审计项目进行安全审计，本次安全审计的范围，不包含未来可能出现的新型攻击方式、升级活篡改后的代码、项目前端代码安全与项目平台服务器安全。

本次安全审计项目包括如下：

1. 代码合规审计

   代码相似度审计

   代码补丁审计

   路线图审计

   充值方案审计

2. P2P 安全

   节点连接数审计

   节点性能审计

消息格式校验

消策略审计

通信加密审计

“异形攻击”审计

3. RPC 安全

远程调用权限审计

畸形数据请求审计

通信加密审计

同源策略审计

4. 加密签名安全

随机数生成算法审计

密钥存储审计

密码学组件调用审计

哈希强度审计

交易延展性审计

加解密模糊测试

5. 账户与交易模型安全

事务校验审计

事务重放审计

“假充值”审计

6. 静态代码检查

内置函数安全

标准库安全审计

第三方库安全审计

注入审计

序列化算法审计

内存泄露审计

算术运算审计

资源消耗审计

异常处理审计

日志安全审计

7. Python脚本安全审计

8. Android端APP安全测试

3. 架构分析

3.1 目录结构

```
    ├─bench
    |  └─src
    ├─browser-testing
    |  └─src
    ├─cli
    |  ├─bin
    |  ├─browser-demo
    |  ├─doc
    |  ├─res
    |  ├─src
    |  └─tests
    ├─docs
    |  ├─freq_ask_questions
    |  |  └─freq_ask_questions.assets
    |  ├─How_to_rent_supernode.assets
    |  ├─join_dbc_network_vm.assets
    |  ├─join_dbc_testnet.assets
    |  ├─join_dbc_testnet_EN.assets
    |  ├─prepare_vm_EN.assets
    |  └─staking_dbc_and_voting.assets
    ├─executor
    |  ├─benches
    |  ├─src
    |  └─tests
    ├─inspect
    |  └─src
    ├─pallets
    |  ├─dbc-staking
    |  |  ├─fuzzer
    |  |  |  └─src
    |  |  ├─reward-curve
    |  |  |  ├─src
    |  |  |  └─tests
    |  |  └─src
    |  └─dbc-testing
    |      └─src
    ├─primitives
    |  └─src
    ├─rpc
    |  └─src
    ├─rpc-client
    |  └─src
    ├─runtime
    |  └─src
    ├─scripts
    ├─testing
    |  └─src
    └─traits
        └─phase-reward
            └─src
```

4. 审计详情

4.1 公链代码审计

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。

5. 安全审计工具

工具名称	功能
零时内部工具包	零时(鹰眼系统)自研发工具包
codeql	为全球安全研究人员提供支持的库和查询

6. 漏洞风险评估标准

高等危害

高等危害是指漏洞发生在核心系统业务逻辑（区块、交易、资金、共识验证处理等涉及核心资产与数据的逻辑），对整个区块链体系造成大量经济损失、大面积混乱、或获取节点宿主机权限等严重且多数不可逆的危害。

包括但不限于：

- 任意节点远程命令执行
- 区块链网络分叉
- 篡改历史区块数据
- 伪造、重放任意交易或区块并大量获益
- 获取任意节点托管的私钥
- 任意铸币、盗币
- 给任意账户造成资金损失
- 篡改鉴权、收费、转账等核心系统逻辑
- 破坏链上保密设计

中等危害

中等危害是指漏洞对部分节点或账户造成较严重危害，可以使部分区块链系统停滞，造成较大混乱或经济损失的问题。

包括但不限于：

- 任意节点程序崩溃或无响应
- 任意节点宿主机崩溃或无响应
- 使任意节点无法验收合法交易
- 使任意节点无法与其他节点维持任何有效连接
- 断开任意节点与其他节点的连接
- 伪造、重放任意交易或区块但无法大量获益
- 伪造签名、获得使用他人私钥给任意数据签名的能力
- 获取某些账户的私钥
- 获得少量非预期资金收益
- 给某些账户造成资金损失
- 越权修改账户地址或权限设置

低等危害

低等危害是指漏洞对部分节点或账户造成一定程度的混乱或经济损失的问题，不会对区块链系统、节点或账户造成实质性损害，但依然需要改进，具有潜在风险的问题。

包括但不限于：

- 重放特定交易或区块
- 使任意节点启动失败
- 使任意节点无法与其他节点建立有效连接
- 显著降低其他攻击的利用难度
- 使服务端RPC接口失效
- 不会直接造成经济损失的敏感信息泄漏
- 一定程度降低其他攻击的利用难度

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项目安全状态，因此不对此承担责任。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。

市场有风险，投资需谨慎，此报告仅对项目代码进行安全审计和结果公示，不作投资建议和依据。

零时科技
NONEAGE

咨询电话：86-17391945345 18511993344
邮　　箱：support@noneage.com
官　　网：www.noneage.com
微　　博：weibo.com/noneage