智能合约安全审计报告

慢雾安全团队于 2021-04-27 日，收到 Defibox 基金会对 Defibox swap 的智能合约安全审计申请。

如下为本次智能合约安全审计细节及结果：

合约哈希：

SHA256(dbswap.wasm)=

23b1d09ae1a434e69b6ffd3677b0165bb3dab9ea9ddb1b9c3e8f9b8fe85a489a

SHA256(lptoken.wasm)=

4647d42736b415317c237016b4ffedc52976b5486bfc0f72ec386ce696502f9a

复审合约哈希：

SHA256(lptoken-2021-05-26.wasm)=

a19c26b432f0ae2296d3fd7664624725f30db9e756756fd976bf6238bbf0148e

SHA256(lptoken-2021-06-28.wasm)=

50c92bde7272c01ac3f127f3d142fafe27b7b0c9997bcadd51e1d56e9814d406

编译器版本：

eosio-cdt-v1.7.0

本次审计项及结果：

（其他未知安全漏洞不包含在本次审计责任范围）

序号	审计大类	审计子类	审计结果
1	溢出审计	-	通过
2	权限控制审计	权限漏洞审计	通过
		权限过大审计	通过
3	安全设计审计	硬编码地址安全	通过
		显现编码安全	通过
		异常校验审计	通过
		类型安全审计	通过
4	性能优化审计	-	通过
5	设计逻辑审计	-	通过
6	拒绝服务审计	-	通过
7	回滚攻击审计	-	通过
8	重放攻击审计	-	通过

9	假通知审计	-	通过
10	假错误通知审计	-	通过
11	假币审计	-	通过
12	随机数安全审计	-	通过
13	粉尘攻击安全审计	-	通过
14	微分叉安全审计	-	通过
15	排挤攻击安全审计	-	通过

备注：审计意见及建议见代码注释 //SlowMist//……

审计结果：**通过**

审计编号：0X002104280003

审计日期：2021 年 04 月 28 日

复审时间：2021 年 06 月 28 日

审计团队：慢雾安全团队

（**声明：**慢雾仅就本报告出具前已经发生或存在的事实出具本报告，并就此承担相应责任。对于出具以后发生或存在的事实，慢雾无法判断其智能合约安全状况，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。）

总结：此为 Defibox Swap 合约，经反馈修正后，综合评估合约无已知风险。

慢雾科技
slow mist

官方网址

www.slowmist.com

电子邮箱

team@slowmist.com

微信公众号