数字货币钱包安全审计报告

Loopr 钱包 (iOS)

SECBIT

2018 年 12 月 15 日

1. 综述

Loopr 钱包是一款数字货币钱包应用。安比（SECBIT）实验室于 2018 年 8 月到 2018 年 9 月对 Loopr 钱包（iOS）进行审计。审计过程从**数字钱包资产安全**，**iOS 应用常规风险**和**服务端应用安全风险**三个维度对钱包进行分析。审计结果表明，Loopr 钱包并未发现致命的安全漏洞，安比（SECBIT）实验室给出了如下几点功能实现安全隐患，发行风险提示以及优化建议项（详见第 4 章节）。

风险类型	描述	风险级别
钱包资产安全	未实施防截屏措施	中 (v0.9.10 已修复)
钱包资产安全	退出助记词页面再进入后没有重新生成助记词	中 (v0.9.10 已修复)
风险提示	钱包生成完毕后会在控制台print私钥	低 (已修复)

2. 钱包信息

应用名称	Loopr 钱包
应用类型	iOS
是否上架	否
文件来源	GitHub
文件类型	源码
代码路径	https://github.com/Loopring/loopr-ios
commit id	909c0e94d4b864119663cd2cabe4e544dc87336c
支持币种	ETH, ERC20 Token

3. 钱包审计分析

该部分针对钱包审计范围的主要功能和主要特性进行了详细分析，从实现的相关功能和安全两部分来进行说明。

3.1 相关功能分析

Loopr 钱包作为一款加密数字货币钱包，针对数字货币部分的主要功能分为四个部分：创建钱包，导入钱包，密钥管理和转账收款等。

- 创建钱包
  - 用户根据使用向导创建一个或多个钱包
  - 钱包创建完毕后可以校验助记词或跳过校验步骤
- 导入钱包
  - 用户可以通过输入助记词、Keystore、私钥来导入钱包
- 密钥管理
  - 修改钱包名称
  - 备份助记词
  - 导出 Keysotre 文件
- 转账收款
  - 支持对 ETH、ERC20 Token 进行转账和收款

3.2 安全分析

Loopr 钱包在安全部分主要分为以下几部分：

- 随机数的生成

  随机数核心功能由 TrustWallet 的 Keystore 库提供，该库调用了 Trezor 钱包的密语生成库，总体相对安全，目前未曝出过相关安全问题。

- 助记词的生成

  App 中使用了 Trezor 的 TrezorCrypto 库，该库使用 srand()、rand()，这两个函数在 Swift 语言中已经标记为 unavailable，推荐使用 `arc4random` 产生的随机数来产生助记词，代码实现遵循 BIP39 规范，暂未发现安全问题。

- 密钥派生

  密钥派生使用 TrustWallet 库中提供的 BIP32 相关函数，按照 BIP44 标准派生密钥，实现过程正确，coin type 正确，并使用 BIP39 密码保护方式保护助记词，暂未发现兼容性问题。

- 密钥存储

  使用了 BIP39 规范中的带密码保护的助记词，将助记词与用户输入的密码拼接后进行密钥派生，由于密钥派生为人为设计的缓慢算法，可以抵御助记词泄漏后对用户密码的暴力破解攻击。

- 密钥管理

  提供了多种格式的密钥导出的功能。

- 防截屏措施

  未发现防截屏措施（已在 v0.9.10 中修复）

- 是否使用不安全的第三方键盘
  - 未使用第三方键盘
- 是否在网络中传输敏感信息
  - 未发现与钱包私钥相关信息在网络上传输。
- 是否包含获取敏感权限
  - 无明显不必要的权限请求，例如通讯录、地理位置等。

4. 审计结果详情

该部分描述钱包审计流程和详细结果，并对发现的问题（数字钱包资产安全，iOS 应用常规风险和服务端应用安全风险），数字资产钱包发行的风险点和附加提示项进行详细的说明。

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，逻辑问题以及数字资产钱包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：

- 各审计小组根据审计内容对钱包应用展开进行审计
- 各审计小组对钱包应用的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）实验室内部工具和外部开源工具的检查，检查结果由审计小组成员详细确认。随后审计小组成员对钱包应用源码进行检查，汇总审计结果。审计内容总结为如下。

编号	分类	结果
1	助记词的创建和存储过程风险检测	通过
2	本地敏感信息的保存风险检测	通过
3	钱包导入过程风险检测	通过
4	密码算法，随机数算法风险检测	通过
5	业务逻辑流程风险检测	通过
6	用户权限划分风险检测	通过
7	数字货币钱包 App 运行环境风险检测	通过
8	数字货币钱包 App 开发合规性风险检测	通过
9	数字货币钱包 App 组件风险检测	通过
10	服务器端用户敏感信息保存的风险检测	通过
11	服务器端应用存在风险检测	通过
12	钱包应用与服务器端通信风险检测	通过

4.3 问题列表

问题是明显存在的安全风险点，安比（SECBIT）实验室在对 Loopr 钱包应用风险进行评估以后，指出钱包存在如下问题点，并根据问题提出一些规避方案，具体描述如下：

1. 未实施防截屏措施
    - 风险级别：**中**
    - 问题类型：钱包资产安全
    - 风险检测类别：
        - 私钥的创建和存储过程风险检测

        - 助记词的创建和存储过程风险检测
    - 问题描述：

      助记词显示界面用户可以截屏，将助记词存于相册

    - 影响结果：

      屏幕截图泄漏、手机遭受攻击都有可能导致助记词泄漏

    - 规避方案：

      对于 iOS，可以参考一些比特币钱包的做法，具体描述如下：

        - 生成密钥阶段用户截屏一次便生成一次新的助记词
        - 导入密钥阶段可以考虑隐藏输入完毕的单词

- 修改结果：
    - 加入了防截屏措施，用户每次截屏后都会重新产生一组助记词。

4.4 风险提示

风险点是在用户使用过程中，也可能是产品设计过程中可能存在的安全隐患，安比（SECBIT）实验室在对 Loopr 钱包应用风险进行评估以后，指出钱包存在如下风险项：

1. 助记词未重新生成
    - 风险级别：**低**
    - 风险描述：

      在用户输入钱包密码页面以及助记词显示页面，点击左上角的返回按钮，将页面退回到钱包名称输入页面后，重新输入钱包名称或密码后点击下一步，助记词没有发生变化。

    - 修改结果：

      每次进入助记词显示界面均会产生新的助记词。

2. 未明显提醒用户不能遗忘钱包密码
    - 风险级别：**中**
    - 风险描述：

      在新版 Loopr(UP) 钱包中，使用了 BIP39 密码来保护助记词，通过这种方式保护的助记词与一般常见的钱包保护方式很不一样，助记词与密码拼接后才是真正的密钥生成种子，所以用户必须同时记住助记词和和密码才能恢复出私钥，遗失任意一部分都将导致资产无法解锁。

5. 结论

Loopr 钱包根据标准协议规范 BIP32、BIP39、BIP44 实现了数字货币钱包的基本功能（创建账户、密钥管理、转账收款等），并根据应用本身特定需求实现了一些功能。安比（SECBIT）实验室在对 Loopr 钱包应用（iOS）进行分析后，发现一些问题和风险点，并给出一些附加提示项，上文均已给出具体的分析说明。

免责声明

SECBIT 数字货币钱包安全审计从账户安全、资产安全和钱包发行风险等方面对钱包应用的正确性、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数字资产钱包适用性相关的承诺。本报告为技术信息文件，不作为投资指导。

附录

漏洞风险级别介绍

等级	描述
高	可以严重损害用户数字资产安全的缺陷，能够允许攻击者盗取用户数字资产，或者无法使用数字资产等缺陷。
中	在一定限制条件下能够损害数字资产安全的缺陷，造成某些参与方利益损失的缺陷。
低	并未对数字资产安全造成实质损害的缺陷。
提示	不会带来直接的风险，但与数字资产安全实践或数字货币钱包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://secbit.io
audit@secbit.io
@secbit_io