# 数字货币钱包安全白皮书

360 信息安全部

2018 年 5 月

# 前言

区块链技术的迅速发展，使得数字货币渐渐走入的大众的视线，在 2017 年底，这股热潮达到顶峰，直接搅动着金融市场与科技市场，大量的数字货币交易流水催生了数字钱包开发行业， 根据钱包使用时的联网状态分为热钱包和冷钱包。

随着各种数字货币的诞生，为了方便用户记录地址和私钥，官方会同时发布全节点钱包，例如 Bitcoin Core，Parity 钱包 ，同时也有一些第三方公司为了进一步提高用户体验，他们相继开发了如比特派，imToken，AToken，币信，币包等钱包 APP，它们并不同步所有的区块数据，因此称其为轻钱包，这两种数字钱包都属于热钱包。冷钱包也称为硬件钱包，常见的冷钱包有库神钱包，Ledger Nano S，Trezor 等，由于私钥不接触网络，相对安全性也较高。不过由于业务场景的快速迭代以及推广需求，无论热钱包还是冷钱包都会有一些的安全隐患会被忽视。

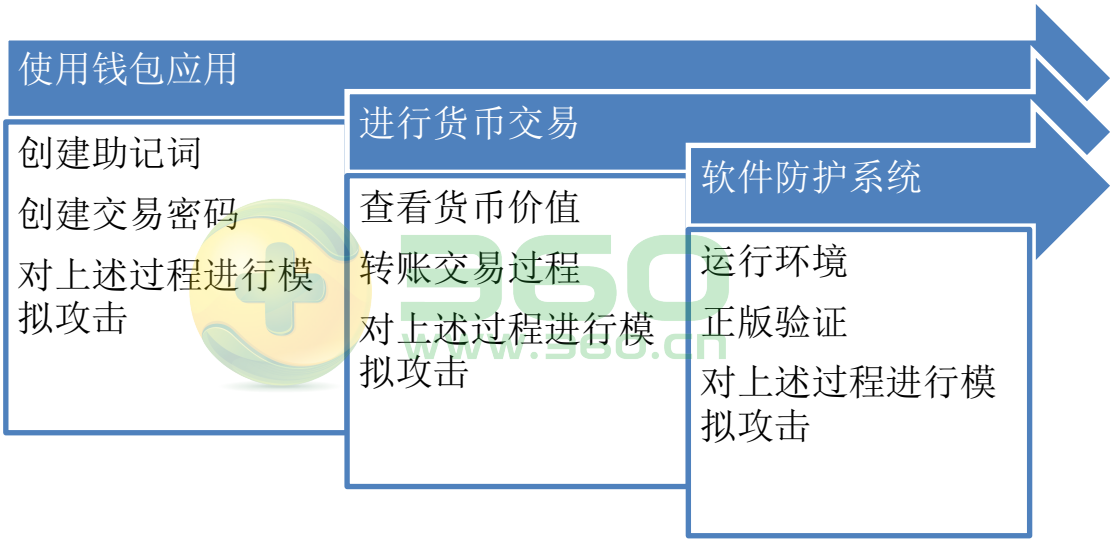
近期，我们对应用市场上流通的热钱包以及冷钱包进行了相关安全审核评估，发现了很多安全问题，360 信息安全部依靠通过对各类攻击威胁的深入分析及多年的安全大数据积累，旨在区块链时代为数字货币钱包厂商提供安全性建议，保障厂商与用户的安全，因此发布数字货币钱包安全白皮书为其作为参考。

# 一、钱包 APP 安全现状

近期 360 安全团队发现了国外某知名钱包 APP 的一个钱包不正确

加密存储漏洞，其钱包 APP 在第一次运行的时候，默认为用户创建一个新钱包并将钱包文件未加密存储在系统本地，攻击者可以读取存储的钱包文件，通过对钱包应用逆向分析等技术手段，还原该钱包的算法逻辑，并由此直接恢复出用户的助记词以及根密钥等敏感数据。

我们对目前热门的近二十款钱包 APP 进行了安全分析，从应用运行开始，创建助记词、备份数据、查看货币价值到进行交易，如下图我们的模拟攻击流程。




图：1-1 模拟黑客攻击流程

由于数字货币交易的一个安全重点就是运行环境，Android 是一个非常庞大而且复杂的系统，APP 的运行环境，针对数字钱包本身的功能设计，都将存在很大的安全隐患，如下图所示，我们将发现的安全风险较大的点进行归纳说明。

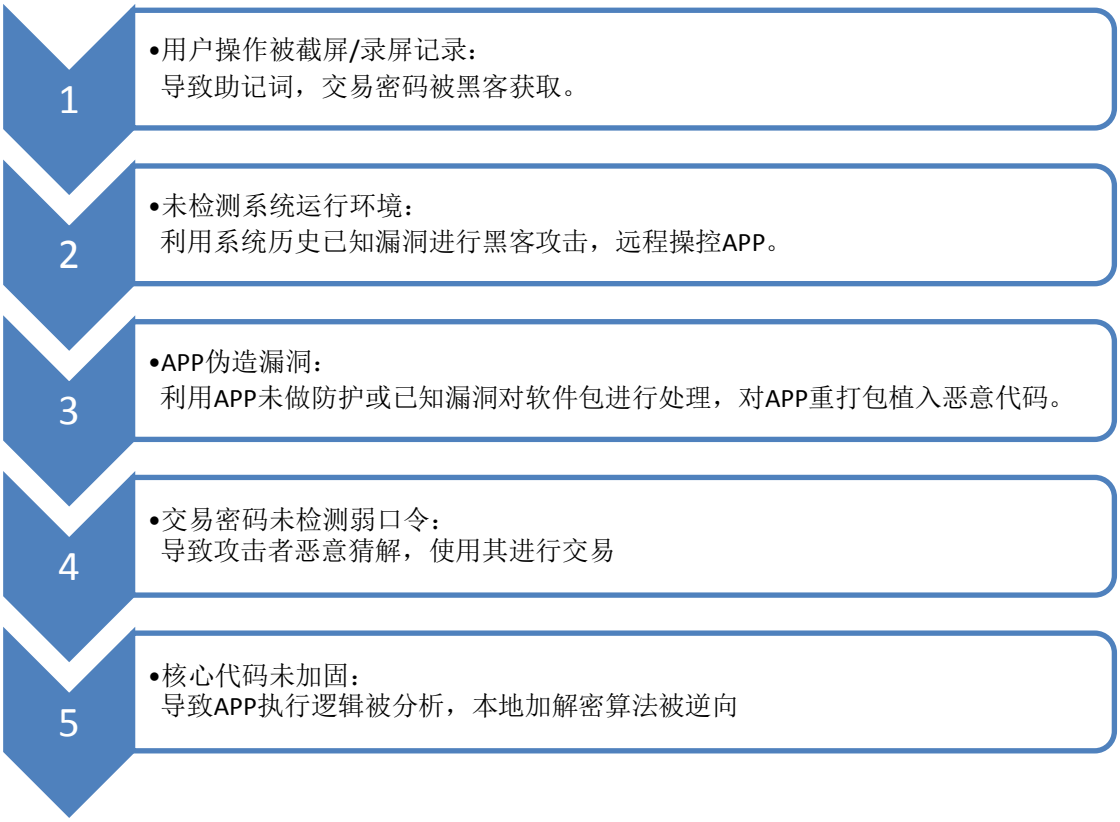



图:1-2 Top5 的安全隐患



我们可以看到，在无 root 下的截屏、录屏可以将我们输入的助记词，交易密码等信息进行得到；利用 Janus 签名问题对 APP 进行伪造，将软件植入恶意代码，可以修改转账人地址等操作，这些都会令用户的钱财受到损失。

## 二、审计热钱包安全隐患

区块链在造就无数财富神话的同时，伴随着而来的，是一系列已经发生的区块链攻击事件。2017 年 11 月，以太坊钱包 Parity 被爆漏洞，导致 93 万个以太坊被冻结，价值 2.8 亿美金。无独有偶，2018 年 1 月，日本最大比特币交易所 Coincheck 被黑，价值 5.3 亿美金的 NEM 被盗。可见，力图去中心化的区块链金融，并不符合大众脑海

中科技安全的第一印象。我们将钱包 APP 分为 APP 端与服务端，分别进行说明。

## 1.审计钱包 APP 端安全隐患

基于我们对当前数字钱包 APP 的安全现状分析，我们将发现的安全隐患进行归纳总结，如下文。


图：2-1 APP 端安全审核覆盖范围

### 1.1. 运行环境安全检测

#### 1.1.1. 手机系统漏洞扫描

钱包 APP 未对于手机当前系统版本进行检测并做出相关，将导致已知漏洞对手机系统的损害，使得钱包 APP 容易被黑客控制权限，我们将扫描相关严重漏洞，判断当前手机系统安全性。

#### 1.1.2. Root 环境检测

钱包 APP 未对于手机环境进行 root 检测，会导致 APP 运行在已 root 的手机上，使得 APP 相关核心执行过程被逆向调试分析，我们将会扫描 root 常见手段，来判定设备是否已被 root。

#### 1.1.3. APP 完整性检测

钱包 APP 未做完整性检测，会导致黑客可以对 APP 重新打包植入恶意代码，窃取用户助记词，私钥等敏感信息，我们将进行模拟攻击，对 APP 进行重打包，修改验证机制来判定是否可利用此漏洞。

#### 1.1.4. 网络代理检测

APP 在运行中，未检测是否使用相关代理，将会导致协议交互过程中网络数据被黑客监听，我们将进行模拟黑客攻击，确认是否安全。

#### 1.1.5. 网络安全检测

钱包 APP 未检测验证当前使用网络的 DNS 是否安全，将会会存在被劫持的可能，导致一些网络回传的数据被黑客恶意修改，我们将通过技术手段模拟黑客攻击，来确认是否安全。

### 1.2. 协议交互安全检测

#### 1.2.1. 新用户注册安全

在安装完 APP 后，新用户需要进行注册，才能使用钱包 APP，

在这个注册过程中，如将用户敏感信息上传至服务器，会存在很大安全风险，比如传输过程或服务器上被黑客攻击获取注册信息，我们将对网络传输数据进行逆向分析，查看是否存在隐患。

### 1.2.2. 创建交易安全

在用户创建交易时，交易双方的账号如果没有二次验证，则容易导致收款账户信息被恶意替换后无法知道，导致用户钱财损失问题，我们将会使用技术手段进行测试，验证钱包 APP 是否存在此风险。

### 1.2.3. 交易签名安全

在交易创建后，发送正式签名交易过程，如果相关协议设计不严格，会导致用户财产受到损失，我们会对交易过程逻辑代码进行逆向分析，查看是否存在相关安全隐患。

### 1.2.4. 交易完毕确认

交易完毕后，如果未对交易内容进行确认，会导致使用户清晰了解此次交易过程的记录，在 APP 上无法记录相关信息，无法查询个人交易记录，我们会对此过程进行分析，查看是否存在相关安全隐患。

### 1.2.5. 余额查询安全

钱包 APP 在进行余额查询时，无论是从货币官方服务器，还是钱包厂商服务器进行的查询，应严格对其返回给客户端的数据进行完整性验证，否则容意导致用户 APP 数据接

收虚假、异常信息，我们会对此流程进行确认，查看是否存在安全隐患。

## 1.3. 数据存储安全检测

### 1.3.1. 助记词创建安全

新用户使用钱包 APP 时，会生成助记词要求用户记录，此过程是否有检测截屏，录屏等操作，如未进行安全检测，将会导致钱包核心敏感信息泄露，用户钱财损失。

### 1.3.2. 助记词存储安全

助记词生成后，如果会在本地保存，在本地保存时是明文存储，将会导致黑客进行攻击获取用户助记词信息。如果是加密存储，加密算法安全性不高，将会导致黑客可以逆向分析算法，将加密数据进行恢复明文，导致用户助记词信息泄露。我们会模拟黑客攻击，检测相关流程是否存在安全隐患。

### 1.3.3. 私钥生成安全

钱包 APP 在新用户私钥生成过程，相关算法如果可被逆向分析，会导致黑客模拟生成的私钥，使用户的钱财受到损失，我们将会模拟黑客攻击，逆向分析相关算法，确认是否存在此安全隐患。

### 1.3.4. 私钥储存安全

私钥生成后，如果会在本地保存，在本地保存时是明文存

储，将会导致黑客进行攻击获取用户私钥信息。如果是加密存储，加密算法安全性不高，将会导致黑客可以逆向分析算法，将加密数据进行恢复明文，导致用户私钥信息泄露。我们会模拟黑客攻击，检测相关流程是否存在安全隐患。

#### 1.3.5. 本地存储数据敏感性检测

在本地存储数据时，是否会将敏感信息保存在本地，如果一些对用户敏感的信息保存在本地，容易被攻击者进行逆向分析，我们会对其进行逆向分析，查看本地是否存在敏感信息。

### 1.4. 功能设计安全检测



#### 1.4.1. 导入钱包功能安全

用户使用导入钱包的功能，是会将之前用户存储在系统中的私钥直接恢复，恢复过程如果被监控，相关功能设计不严格，会导致在此过程被黑客攻击，我们会模拟黑客攻击，进行相关验证。

#### 1.4.2. 交易密码安全

交易密码如果未检测弱口令，将会导致黑客对密码进行猜解，直接进行交易；交易密码日字旁本地存储，本地储存加密不严格，则会导致黑客对其进行逆向分析，获取到交易密码，我们将模拟黑客攻击，验证此安全隐患是否存在。

### 1.4.3. 用户输入安全

用户输入数据，如果功能设计不严格，将会被黑客监听窃取；如果采用第三方键盘进行，未对用户输入逻辑做校验，容易被黑客监听获取敏感信息，我们将会模拟黑客攻击，查看相关流程是否严格，验证此安全隐患是否存在。

### 1.4.4. 转账地址安全检测

钱包 APP 在输入转账地址或扫描二维码转账地址后，如果未检测地址被篡改，保证转账地址完整，会导致用户钱财受到损失，我们将会模拟黑客攻击，查看相关流程是否存在安全隐患。

### 1.4.5. 助记词，私钥网络储存安全

助记词和私钥应当禁止通过网络传输回 APP 厂商，防止服务器被攻击用户数据与钱财被盗取，如果有相关回传数据操作，容易导致用户数据与钱财被盗。我们将逆向分析相关网络协议，查看是否存在相关安全隐患。

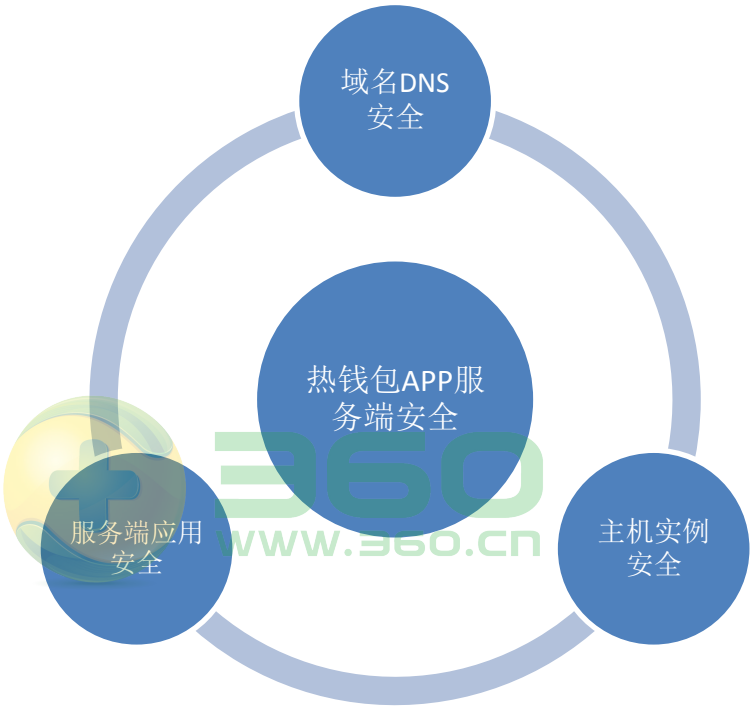
### 1.4.6. https 通信中的证书校验

在数据网络交互通信中，如果使用 https，未对证书做严格的校验，将会导致中间人劫持攻击，黑客将数据替换，导致用户在 APP 上收到虚假信息，我们将会模拟黑客攻击，对此过程进行验证，确认是否存在相关安全隐患。

## 2.审计钱包 APP 服务端安全隐患

服务端作为区块链数字钱包的中心化对象，显然已是黑客十分青睐的攻击目标，安全是其健壮运行的核心基石。

基于我们对当前数字钱包服务端的安全现状分析，我们将相关审计点进行归纳总结，并提供相关安全建议。




图：2-2 钱包 APP 服务端安全审核覆盖范围

### 2.1. 域名 DNS 安全检测

#### 2.1.1. 域名注册商安全检测评估

对数字钱包所用域名注册商，需进行评估，防止钱包域名被恶意社工篡改和攻击。建议使用国内外排名靠前的域名注册商。

#### 2.1.2. 域名记录安全检测

对数字钱包接口所用域名及其解析记录，增改进行审核，并定期复查，防止被 CNAME/NS/SOA 劫持，做好权限管理和日志收集。数字钱包使用云 CDN 时，合理配置相关参数，避免子域劫持，域名前置，Web 缓存欺骗等安全问题，同时选用业界安全性较好的 CDN 服务提供商。

2.1.3. DNS 服务安全检测

域名解析服务，钱包厂商自建的，做好上线前的审计和运行后的定期复查。使用第三方 DNS 解析服务的，建议一定要选用国内外大厂商，预防域名解析被恶意社工或利用漏洞篡改，或拒绝服务攻击。合理配置 DNS 配置参数，预防伪造邮件，证书校验,DNSSEC,高纬度攻击 BGP 等安全问题。

2.1.4. TLD/gTLD 安全检测

建议使用 org 等顶级域名，不要选用小众后缀域名，防止被恶意篡改和劫持上层记录。如 2017 年 6 月，Matthew 劫持 io 顶级域.

2.1.5. 全网多节点 DNS 解析监测

选用排名靠前的第三方服务，使用全球不同节点对 DNS 记录进行解析，监控解析结果是否正常，是否被污染篡改等。如遇大面积故障，协调多方及时应急响应。

2.1.6. 证书安全

数字钱包内置证书时，选用 20 年等时间较长的证书，避免 APP 升级迭代后的兼容问题。同时建议选择国内外知名证书

机构签发的证书，避免信任链牵连问题。

## 2.2. 主机实例安全检测

### 2.2.1. 口令安全

审计数字钱包所用服务口令强度，建议设置为强密码，SSH 类使用证书登陆，最好前置堡垒机。

### 2.2.2. 系统安全

数字钱包服务端系统，高危漏洞及时更新，系统和内核等加固配置，减轻未知的漏洞，预防被攻击后的提权和横向渗透等操作。

### 2.2.3. 访问控制

数字钱包服务端在云上时，云安全组 ACL 是其第一道防线，严格限制出入站端口和 ip 的开放，避免高危和敏感服务暴露。同时，控制敏感服务出站流量。VPC 是在云中预配置出一个逻辑隔离的环境，不要选用经典网络等各租户互通的网络环境，预防阿里云租户之前的经典网络内网攻击路线。数字钱包服务端系统，使用 Iptables 等保护系统相互隔离，控制资源仅可信域连接。

### 2.2.4. 日志审计

搜集和保存数字钱包服务端各种日志，便于服务状态监控，故障排查，被渗透后的溯源追踪等。日志保存时间至少 6 个月以上。

#### 2.2.5. 冗余安全

对数字钱包核心系统进行冗余配置，保证服务的高可用。定期进行系统快照，核心数据备份等。检测数字钱包账户下EBS(区块存储)，RDS(云数据库)，AMI(主机镜像)等所有快照和备份服务，严格保证其为私密权限，防止意外暴露。

#### 2.2.6. 云 IAM 授权检测

如使用云 IAM，因为 IAM 是云上对用户权限，资源权限控制的一种服务，检测数字钱包使用过程中的配置安全问题。妥善保管凭证，合理分配权限。

### 2.3. 服务端应用安全检测



#### 2.3.1. 代码安全

数字钱包 APP 代码和服务端代码,上线前进行进行安全审核，检查通过后，允许上线。每次改动代码后，也要进行安全复查，同时定期进行黑灰盒扫描测试。另外对代码进行严格控制，防止上传到 Github 等第三方代码托管平台。

#### 2.3.2. 服务应用安全

数字钱包服务端应用上线前，先进行安全加固，运行时保持低权限运行，同时定期监控，黑白盒扫描漏洞。

#### 2.3.3. 环境隔离

数字钱包不同功能的服务，建议模块化运行，保持相互独立

且隔离，防止越权访问和读取数据，减轻被攻击后的横向渗透。

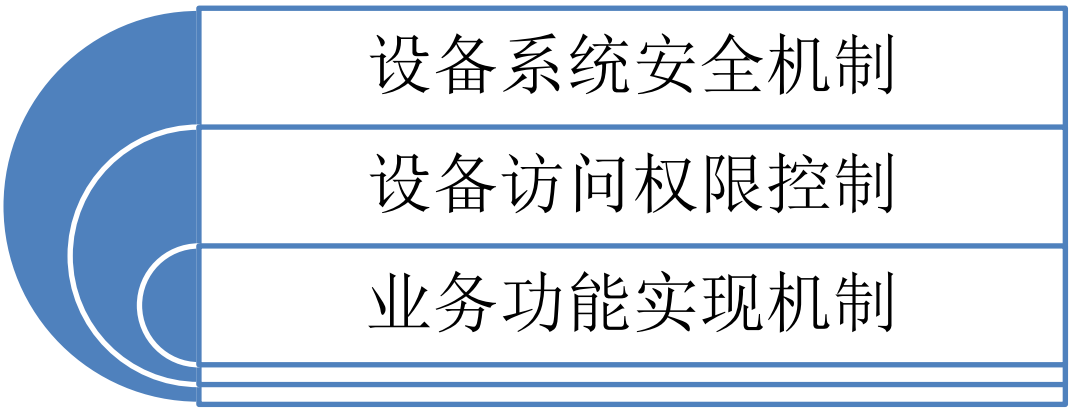
2.3.4. 云存储

数字钱包如使用类似 Amazon S3 的对象存储服务时，严格控制权限问题，防止未授权可读写造成一系列安全问题。

## 三、审计冷钱包安全隐患

2018 年，技术处于全球领先的硬件数字钱包制造商 Ledger 在完成 7500 万美元的 B 轮融资后被爆出钱包设计存在缺陷，黑客可通过恶意软件篡改钱包地址，并将数字货币转给黑客。

硬件钱包目前也是使用趋势，实际上是将密钥保存在了硬件芯片当中，不过依然会存在很多安全风险，我们将从以下几点说明。




图：3-1 冷钱包安全审核覆盖范围

### 1. 设备系统安全机制

1.1 硬件钱包是否存在联网控制

设备在使用过程中，是否有联网操作，是否全程隔绝物理

网络，如未做相关设计，黑客的攻击面则会变大，导致设备更加容易被攻击。

1.2 硬件钱包系统安全检测

设备是否保留蓝牙，wifi，nfc 相关近景协议模块，是否有安全防护措施，是否有漏洞扫描。

1.3 硬件钱包系统漏洞更新机制

如何设备存在漏洞，更新机制是如何进行的，在更新过程中，是设备与电脑进行连接刷机还是什么方式，如未校验系统完整性，则导致更新刷入的系统无法控制，刷入黑客修改的恶意系统，对所有流程进行控制。

1.4 设备丢失锁定方案

是否有健全的机制对设备丢失模式进行判定，将设备锁定，如未做相关设计，则容易导致用户钱财受到损失。



## 2. 设备访问权限控制

2.1 是否允许用户对设备进行连接调试

对设备是否加入了严格的权限控制，防止攻击者对设备进行连接调试，分析转账中功能实现部分，交易过程中本地数据读取等。

2.2 是否允许用户对设备存储区进行读写

对于设备存储区，是否有做严格加密，对存储区的权限控制是否严格，如不严格，则会被黑客进行拆机对存储区做

分析提取数据。

2.3 是否允许用户对设备内存进行转储分析

对设备被调试是否有做检测，防止内存数据泄露，如未做相关设计，则会导致黑客进行数据采集和逆向分析。

2.4 是否采用加密芯片

私钥存储是否采用加密芯片保存相关信息，运行系统和私钥存储是否分离，如未采用，则安全性相对会低。

## 3. 业务功能实现机制

3.1 设备使用密码设置

是否提醒用户设置解锁密码，解锁手势或指纹解锁，错误密码解锁时间周期，设备交易密码强度是否为较高，如未有完善的密码设置控制，则在设备丢失后无法被人直接进入查看个人隐私信息，进行交易。

3.2 创建钱包助记词安全

新用户使用钱包时创建助记词，私钥过程是否安全，是否本地保存，本地保存如何来做，如相关功能设计未考虑安全性，则会导致相关数据被逆向调试分析泄露，对用户钱财造成损失。

3.3 交易过程安全

对于收账地址是否完全显示，是否有验证地址被修改，如未校验，则容易使用户转账转错，钱财受到损失。。

### 3.4 数据存储安全

有哪些数据是保存在存储设备上，私钥储存方式如何，是否保存在设备存储卡上，被外部获取，如相关功能设计不完善，则容易被黑客攻击。

### 3.5 系统完整性安全

设备系统是否有严格的完整性校验，用于自检设备是否被人刷机，正品保障，否则容易在设备出厂经销地方被黑客或攻击者进行篡改。

## 四、总结

现阶段，市面上有大量良莠不齐的数字货币钱包存在，而不少开发团队在以业务优先的原则下，暂时对自身钱包产品的安全性并未做到足够的防护，一旦出现安全性问题会导致大量用户出现账户货币被盗，而由于数字货币实现的特殊性，被盗资产非常难以追回，因此钱包的安全性是至关重要的。我们团队会不断跟进钱包安全，为区块链生态安全贡献一份力量。

对于漏洞等级的相关说明，我们做了一下总结，如下表：

| 名称 | 等级 | 危害 |
| --- | --- | --- |
| 助记词创建过程不安全 | 高级 | 助记词的创建过程如果允许被录屏，截屏等操作，会导致助记词被窃取 |
| 助记词不安全存储 | 高级 | 助记词明文或者弱加密存储，黑客在拿到后可以暴力解密出来导致助记词被窃取 |
| 私钥不安全生成 | 高级 | 私钥生成过程存在问题，导致攻击者可模拟私钥生成，造成私钥被窃取 |
| 私钥不安全存储 | 高级 | 私钥使用不安全存储可能导致恶意应用获取到私钥，造成私钥被窃取 |
| 硬件钱包助记词不安全存储 | 高级 | 助记词的不安全存储可能导致助记词被窃 |

| | | |
|---|---|---|
| | | 取 |
| 转账地址可篡改 | 高级 | 如果恶意软件可以篡改转账地址将会导致用户将数字货币转到黑客账户 |
| 服务器弱口令 | 高级 | 服务器使用弱口令，黑客极易拿下服务器权限 |
| 硬件钱包系统漏洞攻击 | 高级 | 不进行定期扫描系统漏洞可能会存在漏洞，导致黑客攻击获取邮件钱包权限 |
| 本地敏感信息不安全存储 | 中级 | 本地敏感信息不安全存储可能导致敏感信息的泄露 |
| 钱包导入过程不安全 | 中级 | 钱包导入的时候如果允许录屏截屏会导致密钥泄露 |
| 交易密码弱口令 | 中级 | 如果交易密钥使用弱口令，黑客可以暴力破解并操作账户 |
| 用户输入不安全 | 中级 | 用户输入如果被黑客监听或者劫持，关键信息可能会被黑客猜测出来 |
| 助记词/私钥回传 | 中级 | 数字钱包开发商将私钥/助记词等数据回传可能导致私钥/助记词的泄露 |
| 查询越权 | 中级 | 如果用户数据在钱包服务器进行存储，越权漏洞会泄露用户信息 |
| 未进行系统漏洞扫描 | 中级 | 未进行系统漏洞扫描，系统可能存在能被黑客利用的漏洞，可能被黑客窃取到关键数据 |
| 域名解析被篡改 | 中级 | 域名解析被篡改会导致劫持 |
| 钱包域名 DNS 污染 | 中级 | DNS 被污染可能导致用户被劫持，可能被钓鱼窃取用户账户密码身份证等信息 |
| 服务器未定期进行漏洞扫描 | 中级 | 服务器未定期做漏洞扫描可能会存在高危漏洞，导致被黑客入侵拿下权限 |
| 云服务器未做访问控制 | 中级 | 服务器未做访问控制 |
| 服务器未进行日志审计 | 中级 | 服务器未定期审计日志可能会导致黑客长期控制服务器 |
| 核心代码泄露 | 中级 | 服务器和数字钱包核心代码泄露容易被黑客获取到审计出漏洞 |
| 服务器应用存在漏洞 | 中级 | 存在漏洞的服务器容易被黑客攻击，泄露用户敏感数据 |
| 服务器未实行环境隔离 | 中级 | 服务器未实现运行环境隔离可能会导致其它恶意应用窃取到用户敏感数据 |
| 云存储不安全配置 | 中级 | 使用第三方云存储上存储数字钱包数据时需做严格权限控制 |
| 硬件钱包无丢失应急机制 | 中级 | 当用户丢失硬件钱包，如无丢失应急机制，可能导致账户被盗 |
| 硬件钱包可调式 | 中级 | 硬件钱包可调式可导致程序运行时关键数据泄露 |
| 硬件钱包固件可读写 | 中级 | 攻击者可以通过芯片引脚进行固件的提取，导致固件被逆向分析 |

| | | |
|---|---|---|
| 硬件钱包芯片未加密 | 中级 | 未加密的芯片降低了被逆向分析的难度 |
| 硬件钱包未设置密码 | 中级 | 硬件钱包未设置密码可能在丢失后被直接用于转账，令用户处于极高的风险下 |
| 硬件钱包存储不安全 | 中级 | 如果存储设备可读写会导致敏感信息的泄露 |
| 硬件钱包固件完整性未校验 | 中级 | 未检测固件完整性，可能导致固件被篡改，植入恶意代码导致交易风险 |
| https 证书不严格校验 | 中级 | 证书不严格校验可导致中间人攻击 |

图：4-1 漏洞风险等级列表

## 五、关于我们

360 信息安全部致力于保护内部安全和业务安全，抵御外部恶意网络攻击，并逐步形成了一套自己的安全防御体系，积累了丰富的安全运营和对突发安全事件应急处理经验，建立起了完善的安全应急响应系统，对安全威胁做到早发现，早解决，为安全保驾护航。技术能力处于业内领先水平，培养出了较多明星安全团队及研究员，研究成果多次受国内外厂商官方致谢，如微软、谷歌、苹果等，多次受邀参加国内外安全大会议题演讲。目前主要研究方向有区块链安全、WEB 安全、移动安全（Android、iOS）、网络安全、云安全、IOT 安全、等多个方向，基本覆盖互联网安全主要领域。