

PlatON钱包安全审计过程文档

前言：

慢雾安全团队于2021-03-22收到 PlatON 团队对 ATON钱包 项目进行安全审计的申请。

项目介绍：

此次安全审计项目核心目标是 ATON钱包 项目进行快速全面的安全审计，审计周期为 5 个工作日。检测潜在的威胁点，帮助 ATON钱包 从 App端等提升一个安全维度。

协力PlatON团队一起为客户的资金安全做出最有效的推进，更好的保护广大PlatON用户的安全。

审计时间：

【审计周期】：5 个工作日

【审计团队】：慢雾安全团队

【审计时间】：2021年03月23日 - 2021年04月07日

审计范围

对目标项目如下部分进行审计：

1、Android 端

2、iOS 端

审计结果:

审计完成

Android 安全审计

Name: aton_android_v1.0.0.0_202103271729_1000_x_unjiagu_PlatONNetwork_7ebc09c8.apk

MD5: 82a2fc20eb42d54bc979ec2bb527022b

SHA256: 83a329622a3f203e2bc789fb640b768e20049527d3bcf9eb42256f78eee6acbc

1、运行环境安全

过程描述

没有越狱环境检测

审计结论

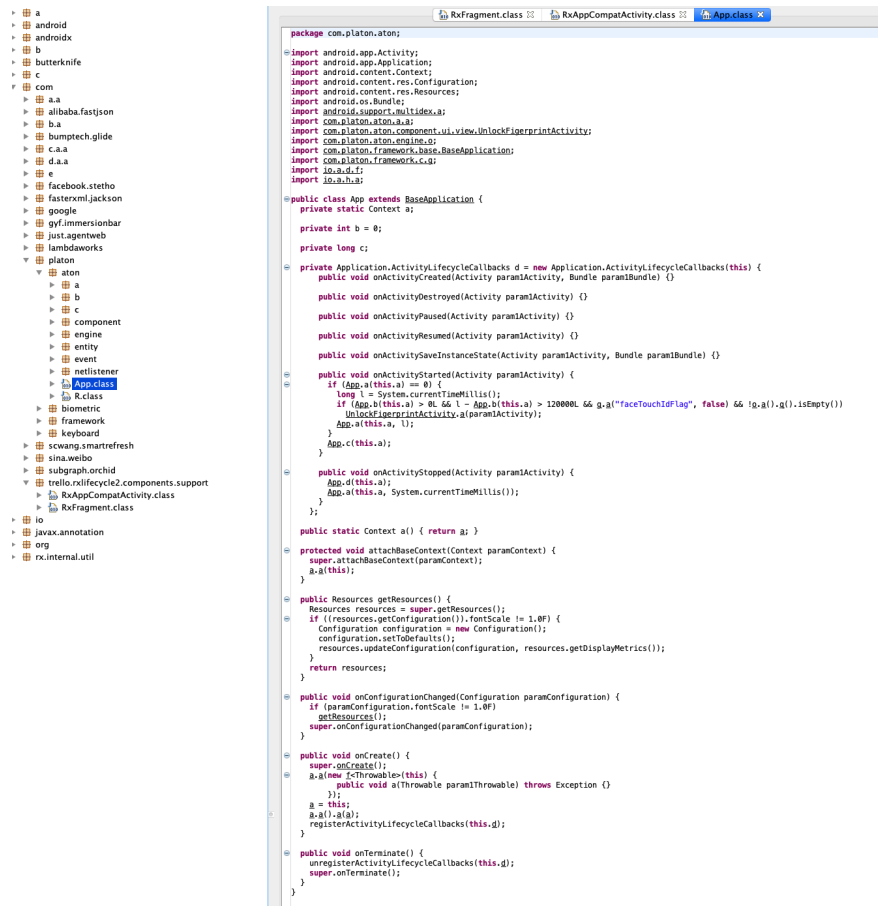
没有越狱环境检测，可以直接在越狱机上使用钱包

解决方案

增加环境检测，遇到越狱环境自动退出

2、文件反编译

过程描述



未加壳, 可以反编译出源码

审计结论

App安装包未加壳、混淆处理

解决方案

对App进行加壳混淆处理, 可以参考如下链接进行处理

加壳: <https://jiagu.360.cn/#/global/index>

混淆: <https://github.com/danleechina/mixplaintext>

3、访问控制策略

过程描述

读取配置文件, 查看App权限获取情况

android.permission.WRITE_EXTERNAL_STORAGE 允许向外部存储写入数据

android.permission.READ_EXTERNAL_STORAGE 允许读取设备外部存储空间

android.permission.READ_PHONE_STATE 允许读取手机状态

android.permission.CAMERA 允许使用相机拍摄照片和视频

审计结论

限申请没有问题

解决方案

无

4、通信加密与传输安全检测

过程描述

使用HTTPS进行传输

```
POST /app/v0760/token/tokenlist HTTP/1.1
Host: aton.alaya.network
Content-Type: application/json
Connection: close
Accept: */*
Aton-Version: 1.0.0
Accept-Language: zh-Hans
Content-Length: 59
Accept-Encoding: gzip, deflate
User-Agent: platonWallet/78 CFNetwork/1125.2 Darwin/19.4.0
```

```
{
  "walletAddr": "atpla2lrgzjrte4w4tmx4lpehtpvfm7n08t737qfw"
}
```

```
1 HTTP/1.1 200
2 Server: nginx/1.16.1
3 Date: Wed, 07 Apr 2021 02:45:12 GMT
4 Content-Type: application/json; charset=UTF-8
5 Connection: close
6 Content-Length: 715
7
8 {"errMsg": "成功", "code": 0, "data": [{"tokenAddress": null,
  "isToken": false, "name": null, "symbol": null, "decimal": 18, "free":
  "30000000000000000000", "lock": "0", "icon": null, "canTransfer":
  true}, {"tokenAddress":
  "atp16lellpkrv894hmg8am7ns3p2qny2vqj85ud8s6", "isToken": true,
  "name": "Ethereum", "symbol": "aETH", "decimal": 18, "free": "0",
  "lock": "0", "icon": null, "canTransfer": true}, {"tokenAddress":
  "atplw4vvn96l19w0rmyeh77ku2tlvyz545mam8rldk", "isToken": true,
  "name": "aLAT", "symbol": "aLAT", "decimal": 18, "free": "0", "lock":
  "0", "icon": null, "canTransfer": false}, {"tokenAddress":
  "atplh3y5wt82z09amcd4mrhpz4jt543t5r9td9v49s", "isToken": true,
  "name": "Tether USD", "symbol": "aUSDT", "decimal": 6, "free": "0",
  "lock": "0", "icon": null, "canTransfer": true}]}
```

审计结论

安全

解决方案

无

5、接口安全检测

过程描述

对所有API进行测试：

```
POST /app/v0760/transaction/estimateGas HTTP/1.1
x-aton-cid: 201018
Accept-Language: zh-cn
Aton-Version: 1.0.0
Content-Type: application/json; charset=utf-8
Host: aton.alaya.network
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.11.0
Content-Length: 212

{
  "from": "atpla2lrgzjrte4w4tmx4lpehtpvfm7n08t737qfw",
  "nodeId": "0xfad2c7f917eb3057d85031eae8bbda52541b527ddld24a25e7e9b",
  "txType": 1004
}
```

```
1 HTTP/1.1 200
2 Server: nginx/1.16.1
3 Date: Wed, 07 Apr 2021 10:12:11 GMT
4 Content-Type: application/json; charset=UTF-8
5 Connection: close
6 Content-Length: 58
7
8 {
  "errMsg": "交易异常，请重试",
  "code": 4,
  "data": null
}
```

无

无

7、业务安全检测

过程描述

(1) 地址簿

添加联系人有地址检查：



< 添加新地址

地址名称：

我

钱包地址：

lax1evsd6tg3ejnug6f2tvpq0hjsmt95l0hqml345

地址格式不正确

地址存在本地，删除 APP 前请先备份

(2) 密码安全

涉及密码的业务功能，如：转账、备份私钥等，没有错误尝试次数且没有密码强度要求，可以无限制进行输入尝试

(3) 节点委托

[illegible]

```
1 HTTP/1.1 200
2 Server: nginx/1.16.1
3 Date: Wed, 07 Apr 2021 10:57:37 GMT
4 Content-Type: application/json;charset=UTF-8
5 Connection: close
6 Content-Length: 104
7
8 {"errMsg": "成功", "code": 0, "data":
9  "0x9d42fe0f682d9573687b20c9412569f3572405e8de1b3c2458a5847ddbc64f2
10 b"}
```

审计结论

未发现安全问题

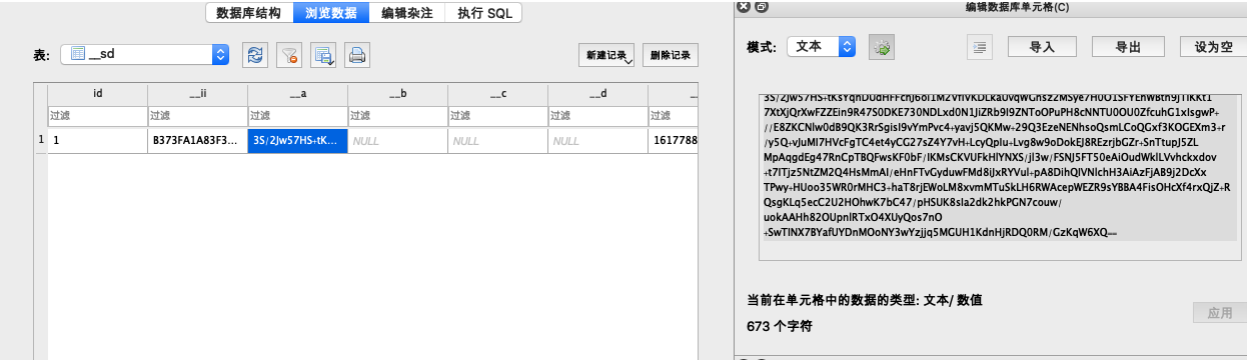
解决方案

无

10、SQLite数据库安全检测

过程描述

对数据库进行检查，未发现敏感信息：



审计结论

未发现敏感信息

解决方案

无

11、文件存储安全检测

过程描述

钱包JSON文件明文方式存储在files/portal文件内

portal																			
18000000	41414141	06000000	41414141	65000001	A80E0100	03009802		AAAAE	.	x	AAAA	AAAA	AAAAE	.	.				
10000000	41414141	08000000	41414141	00000000	41414141	00000000	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA				
50000002	900E000F	00000000	41414141	02000016	0688AA82	5A0A0000	AAAAE	.	.	AAAAE	.	AAAA	AAAA	...Z	.				
50000003	300F0010	400F800E	41414141	45000017	08092809	08121012	AAAA	.	.	AAAAE	0	@	.	AAAAE	(
81300000	41414141	01000004	08000000	00000000	41414141	01000004	@	P	X	h	h	x	.	.	.				
17470000	41414141	00000001	61766174	61725F38	00000000	00000007		AAAA	AAAA	atp	atp	atp	atp	AAAA	avatar_8				
10000008	70617468	496E6465	78000000	00000006	736F7274	496E6465	AAAA	uuid	.	isHD	.	pathIndex	.	sortInde	.				
10000007	64657074	68000000	00000000	0000000A	6865794A	736F6E00	x	selectedIndex	.	parentId	.	depth	.	keyJson	.				
10000008	6061696E	4E657441	64647265	73730001	74657374	4E657441	.	name	.	address	.	mainNetAddress	.	testNetA	.				
10000005	75706461	74655469	60650000	00000005	61766174	61720000	ddress	keystorePath	.	createTime	.	updateTime	.	avatar	.				
10000008	62616368	65645570	00000000	00000007	69735368	6F770000	.	mnemonic	.	chainId	.	backedUp	.	isShow	.				
1000000C	41414141	11000025	63336232	30366532	2D366664	392D3439	.	chainType	.	hrp	.	AAAA	%c3b206e2-6fd9-49	.	.				
10000000	41414141	45000003	90136811	98110000	41414141	06000001	2c-8ed0-c1027f640421	AAAA	.	AAAAE	.	h	.	AAAA	.				
10000000	41414141	01000001	01000000	00000000	41414141	45000003	2b3c	AAAAe	.	AAAA	+	AAAA	.	AAAAE	.				
14000000	41414141	08000000	41414141	1100002B	30786561	62653334	.	.	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA	+0xeabe34				
10000000	41414141	45000003	78093012	88090000	41414141	08000001	0a435e6aeaaf66afc39fdd616277e9bceb	AAAAE	.	x	0	.	AAAA	.	.				
18010000	41414141	07000001	87ADBEAB	78010000	41414141	00000001	AAAA	AAAAe	.	0	.	AAAAx	AAAAx				
1C000001	32303130	31380001	41414141	01000001	01000000	00000000	avatar_3	AAAAe	.	0	0	.	AAAA	201018	AAAA				
10000000	41414141	01000000	41414141	08000000	41414141	08000004	AAAA	AAAA	alaya	AAAA	atp	AAAA	AAAA	AAAA	AAAA				
10000000	41414141	08000004	41414141	08000004	41414141	45000002	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA	AAAA	AAAAE	.				
11000004	08000000	00000000	41414141	1100002B	61747031	61326C72	p	.	AAAA	AAAA	%	AAAA	.	AAAA	+atp1a2lr				
10000000	41414141	0A000001	71000000	00000000	41414141	45000005	gzjrte4w4tmx4lpelhtpvfm7n08t737qfw	AAAA	.	q	.	AAAAE	.	AAAAE	.				
1C000004	616C6179	61000002	616C6179	61000002	616C6179	61000002	.	.	.	AAAAE	.	AAAA	alaya	alaya	alaya				
50000001	C8379803	10147813	41414141	45000002	7005281C	7F000000	alaya	AAAA	AAAA	AAAA	AAAA	AAAAe	.7.	x	AAAAE				
i77A6A72	74653477	34746078	346C7065	6C687470	76666037	6E303874	AAAA	AAAA	.	{	"address":	"atp1a2lrgzjrte4w4tmx4lpelhtpvfm7n08t	.	.	.				
i02D3564	65366536	62363966	3733222C	22766572	73696F6E	223A332C	737qfw",	"id":	"9432f735-31d0-4305-b470-5de6e6b69f73",	"version":	3,				
iA7B226E	223A3136	3338342C	2270223A	312C2273	616C7422	3A223233	"crypto":	{	"kdf":	"scrypt",	"kdfparams":	{	"n":	16384,	"p":	1,"salt":	"23		
i4316137	37346634	34663866	66613463	37303333	33653163	3231222C	6d0d27b6aa2758ed7c7adcc85e452c09249741a774f44f8ffa4c70333e1c21",		
i1353935	64666136	66353432	35343163	36393335	30646231	31386666	"r":	8,"klen":	32},"mac":	"f2bca709b1c1595dfa6f542541c69350db118ff		
i2616573	20313238	20637472	222C2263	69706865	72706172	61607322	a4c931ef3830cd84634b165eb",	"cipher":	"aes-128-ctr",	"cipherparams":		
i0343264	22702C22	63697068	65727465	7874223A	22343633	33616334	:{	"iv":	"08fc9959cfd51a4c2bf8f0859f71042d",	"ciphertext":	"4633ac4		
i2336337	64323737	64663865	36656130	37373739	3622707D	00000000	0634b8fae83ad62382b45fd106c98b58427823c7d277df8e6ea077796"}}		
i02D3266	62663037	66336330	36336337	34633463	36396162	64346264	AAAA	.	UTC--2021-04-07T17-51-43.543--2fbf07f3c063c74c4c69abd4bd		
i0343936	34393964	31663262	30363535	37323462	66383535	37336266	3f0194319e9939cfda2416a63021fadd90290496499d1f2b0655724bf85573bf		
i1342E6A	736F6E00	00000000	41414141	11000097	39303163	30653033	d95c084abfd7acede618521cb126f3401d07a4.json	AAAA	.	901c0e03		
i3353238	61386331	62333039	63633861	33643639	36663734	32376537	9530a0d8ffa45c6726e0c4612635b760a243c528a8c1b309cc8a3d696f7427e7		
i5326132	65643364	32333166	64663139	66316366	65663236	63633264	489183411207d57fc9c552aafbc3fd7a7754e2a2ed3d231fdf19f1cfef26cc2d		
i500000A	38039803	10140017	F81B300C	380DC00D	200F181C	7F000000	305f63b8d8ac9a	AAAAE	.	p	8	AAAAE	.	8	.	.	0	8	.
i5000001	00189803	10146014	41414141	65000001	50219803	10147014	AAAA	.	AAAAE	.	.	AAAAE	.	AAAAE	P!	.	.	p	.
i5000001	40189803	10140017	41414141	00000004	00000000	00000000	AAAA	.	.	AAAAE	.	@	.	.	AAAA

审计结论

钱包JSON文明存储

解决方案

建议对JSON进行加密后存储

12、SSL Pinning安全检测

过程描述

没有进行双向校验

审计结论

没有进行双向校验

解决方案

建议对SSL证书进行双向校验

13、Deeplinks 安全检测

过程描述

查看配置文件未发现配置Deeplinks

审计结论

未配置Deeplinks

解决方案

无

14、录屏截图安全策略

过程描述

允许截图，但有安全提示：



录屏没有限制、也无提示。

审计结论

没有限制截图，但有安全提示，录屏没有任何提示跟限制

解决方案

建议不允许截图私钥、助记词等敏感信息，增加录屏的安全提醒

15、键盘缓存安全检测

过程描述

使用默认键盘，可能存在被键盘记录器记录的风险

审计结论

使用默认键盘，可能存在密码被记录的风险

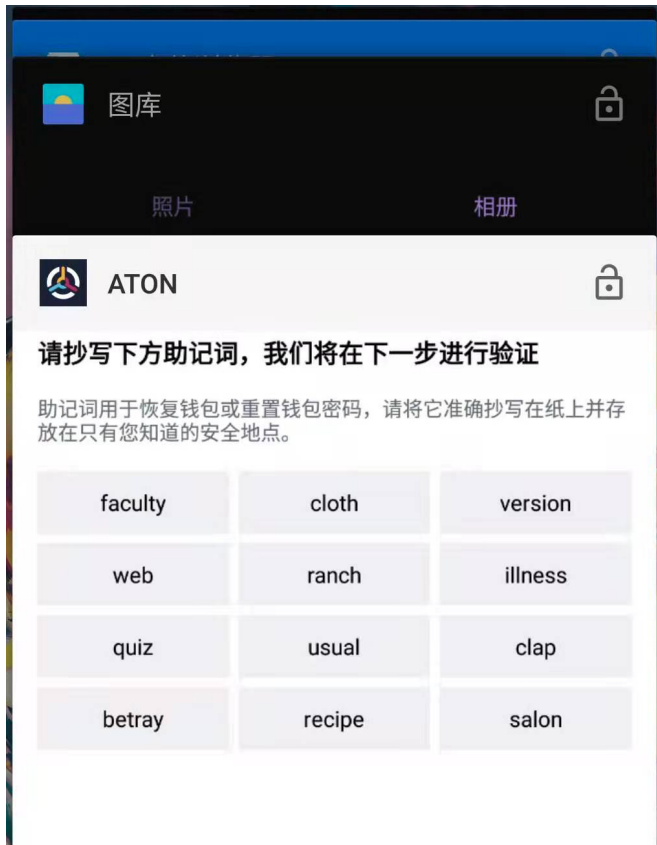
解决方案

使用自定义键盘或是商业加密键盘，数字键盘随机排列

16、模糊处理及挂起安全检测

过程描述

没有进行模糊处理及重新唤醒的安全检查



审计结论

没有模糊处理，App重新唤醒没有安全检查

解决方案

对App切换及挂起时，进行模糊处理；当App从挂起状态重新唤醒时增加安全检查

17、转账安全审计

过程描述

转账需要验证密码，未发现安全问题

审计结论

无

解决方案

无

18、基于客户端的身份验证安全检测

过程描述

钱包默认配置：打开不需要任何认证，可能存在潜在的安全问题：用户个人资产信息暴露。

审计结论

钱包默认情况下无需身份验证可以直接打开App，用户资产可能暴露

解决方案

建议钱包创建后，强制开启身份验证功能

iOS 安全审计

Name:platonWallet_1.0.0_20210324_144809.ipa

MD5:9b076a9d8402db2339b341751cc0d149

SHA256:b485f1638ee25845e45de9020b7c28297708de447cbf15210cadbc00dd826cc7

1、运行环境安全

过程描述

有越狱环境检测

审计结论

有越狱环境检测，但没有自动退出

解决方案

检测到越狱环境自动退出

2、文件反编译

过程描述

```

#import <objc/NSObject.h>

#import "NSCoding-Protocol.h"
#import "NSCopying-Protocol.h"
#import "TWTRJSONConvertible-Protocol.h"

@class NSDictionary, NSString, NSURL;

@interface TWTRUser : NSObject <NSCoding, NSCopying, TWTRJSONConvertible>
{
    _Bool _isVerified;
    _Bool _isProtected;
    NSString *_userID;
    NSString *_name;
    NSString *_screenName;
    NSString *_profileImageURL;
    NSDictionary *_validatedDictionary;
}

+ (id)validateJSONDictionary:(id)arg1;
+ (id)JSONValidator;
@property(copy, nonatomic) NSDictionary *validatedDictionary; // @synthesize validatedDictionary=_validatedDictionary;
@property(readonly, copy, nonatomic) NSString *profileImageURL; // @synthesize profileImageURL=_profileImageURL;
@property(readonly, nonatomic) _Bool isProtected; // @synthesize isProtected=_isProtected;
@property(readonly, nonatomic) _Bool isVerified; // @synthesize isVerified=_isVerified;
@property(readonly, copy, nonatomic) NSString *screenName; // @synthesize screenName=_screenName;
@property(readonly, copy, nonatomic) NSString *name; // @synthesize name=_name;
@property(readonly, copy, nonatomic) NSString *userID; // @synthesize userID=_userID;
- (void).cxx_destruct;
@property(readonly, copy) NSString *debugDescription;
@property(readonly, copy) NSString *description;
@property(readonly, copy, nonatomic) NSURL *profileURL;
@property(readonly, copy, nonatomic) NSString *profileImageLargeURL;
@property(readonly, copy, nonatomic) NSString *profileImageMiniURL;
@property(readonly, copy, nonatomic) NSString *formattedScreenName;
- (_Bool)isEqual:(id)arg1;
@property(readonly) unsigned long long hash;
- (id)copyWithZone:(struct _NSZone *)arg1;
- (void)encodeWithCoder:(id)arg1;
- (id)initWithCoder:(id)arg1;
- (void)setPropertiesFromValidatedDictionary:(id)arg1;
- (id)initWithValidatedDictionary:(id)arg1;
- (id)initWithJSONDictionary:(id)arg1;

// Remaining properties
@property(readonly) Class superclass;

@end

```

审计结论

进行反编译和 class-dump 的过程中未发现加壳或混淆处理，由于 iOS 的封闭性，无法直接通过反编译得到源码，但是可以通过反编译可以得到 .h 的描述文件，里面描述了类，方法名，参数和属性等信息

解决方案

对App进行加壳混淆处理，可以参考如下链接进行处理

加壳：<https://jiagu.360.cn/#/global/index>

混淆：<https://github.com/danleechina/mixplaintext>

3、访问控制策略

过程描述

读取plist配置文件，查看App权限获取情况

```

<string>iphones14.2</string>
<key>NSPhotoLibraryUsageDescription</key>
<string>请授权访问相册</string>
<key>UIViewControllerBasedStatusBarAppearance</key>
<true/>
<key>CFBundleIcons</key>
<dict>
  <key>CFBundlePrimaryIcon</key>
  <dict>
    <key>CFBundleIconFiles</key>
    <array>
      <string>AppIcon20x20</string>
      <string>AppIcon29x29</string>
      <string>AppIcon40x40</string>
      <string>AppIcon60x60</string>
    </array>
    <key>CFBundleIconName</key>
    <string>AppIcon</string>
  </dict>
</dict>
<key>UIStatusBarStyle</key>
<string>UIStatusBarStyleDefault</string>
<key>CFBundleDisplayName</key>
<string>ATON</string>
<key>LSRequiresIPhoneOS</key>
<true/>
<key>LSApplicationQueriesSchemes</key>
<array>
  <string>weixin</string>
  <string>qq</string>
  <string>sinaweibo</string>
  <string>fb</string>
  <string>twitter</string>
  <string>sinaweibohd</string>
  <string>weibosdk</string>
  <string>fbapi</string>
  <string>fb-messenger-api</string>
  <string>fbauth2</string>
  <string>fbshareextension</string>
</array>
<key>NSLocationWhenInUseUsageDescription</key>
<string>请授权访问位置</string>
<key>DTSDKBuild</key>
<string>18B79</string>
<key>NSCameraUsageDescription</key>
<string>request use camera</string>
<key>CFBundleShortVersionString</key>
<string>1.0.0</string>
<key>CFBundleSupportedPlatforms</key>
<array>
  <string>iPhoneOS</string>
</array>
<key>UISupportedInterfaceOrientations</key>
<array>

```

审计结论

申请了定位和相册权限

解决方案

无

4、通信加密与传输安全检测

过程描述

使用HTTPS进行传输

```
POST /app/v0760/token/tokenlist HTTP/1.1
Host: aton.alaya.network
Content-Type: application/json
Connection: close
Accept: */*
Aton-Version: 1.0.0
Accept-Language: zh-Hans
Content-Length: 59
Accept-Encoding: gzip, deflate
User-Agent: platonWallet/78 CFNetwork/1125.2 Darwin/19.4.0

{
  "walletAddr": "atpla2lrgzjrte4w4tmx4lpehtpvfm7n08t737qfw"
}
```

```
1 HTTP/1.1 200
2 Server: nginx/1.16.1
3 Date: Wed, 07 Apr 2021 02:45:12 GMT
4 Content-Type: application/json; charset=UTF-8
5 Connection: close
6 Content-Length: 715
7
8 {
  "errMsg": "成功",
  "code": 0,
  "data": [
    {
      "tokenAddress": null,
      "isToken": false,
      "name": null,
      "symbol": null,
      "decimal": 18,
      "free": "3000000000000000000",
      "lock": "0",
      "icon": null,
      "canTransfer": true
    },
    {
      "tokenAddress": "atp16lellpkrv894hmg8am7ns3p2qny2vqj85ud8s6",
      "isToken": true,
      "name": "Ethereum",
      "symbol": "aETH",
      "decimal": 18,
      "free": "0",
      "lock": "0",
      "icon": null,
      "canTransfer": true
    },
    {
      "tokenAddress": "atp1w4vvn961l9w0rmyeh77ku2tlvyz545mam8rldk",
      "isToken": true,
      "name": "aLAT",
      "symbol": "aLAT",
      "decimal": 18,
      "free": "0",
      "lock": "0",
      "icon": null,
      "canTransfer": false
    },
    {
      "tokenAddress": "atplh3y5wt82z09amed4mrhpz4jt543t5r9td9v49s",
      "isToken": true,
      "name": "Tether USD",
      "symbol": "aUSD",
      "decimal": 6,
      "free": "0",
      "lock": "0",
      "icon": null,
      "canTransfer": true
    }
  ]
}
```

审计结论

安全

解决方案

无

5、接口安全检测

过程描述

对所有API进行测试:

```
POST /app/v0760/transaction/list HTTP/1.1
Host: aton.alaya.network
Content-Type: application/json
Connection: close
Accept: */*
Aton-Version: 1.0.0
Accept-Language: zh-Hans
Content-Length: 121
Accept-Encoding: gzip, deflate
User-Agent: platonWallet/78 CFNetwork/1125.2 Darwin/19.4.0

{
  "beginSequence": ,
  "walletAddrs": [
    "atpla2lrgzjrte4w4tmx4lpehtpvfm7n08t737qfw"
  ],
  "direction": "new",
  "listSize": 20 'or' '='
}
```

```
1 HTTP/1.1 200
2 Server: nginx/1.16.1
3 Date: Wed, 07 Apr 2021 08:11:55 GMT
4 Content-Type: application/json; charset=UTF-8
5 Connection: close
6 Content-Length: 58
7
8 {
  "errMsg": "交易异常, 请重试",
  "code": 4,
  "data": null
}
```

审计结论

安全

解决方案

无

6、App缓存安全检测

过程描述

对App目录内的缓存文件进行检查, 未发现敏感信息, 仅保存了HTTP通信相关的内容:


添加联系人有地址检查:

< 添加新地址

地址名称：

我

钱包地址：

lax1evsd6tg3ejnug6f2tvpq0hjsmt95l0hqml345 

地址格式不正确

地址存在本地，删除 APP 前请先备份

(2) 密码安全

涉及密码的业务功能，如：转账、备份私钥等，没有错误尝试次数且没有密码强度要求，可以无限制进行输入尝试

(3) 节点委托

```
POST /app/v0760/transaction/submitSignedTransaction HTTP/1.1
Host: aton.alaya.network
Content-Type: application/json
Connection: close
Accept: */*
Aton-Version: 1.0.0
Accept-Language: zh-Hans
Content-Length: 576
Accept-Encoding: gzip, deflate
User-Agent: platonWallet/78 CFNetwork/1125.2 Darwin/19.4.0

{"data":{"remark":"","signedData":"0xf8be058502540be4
"sign":"0x1c643b6555f79cd02bfb73376a20a6fc5a05e54e0cb6a58e28
}}
```

```
1 HTTP/1.1 200
2 Server: nginx/1.16.1
3 Date: Wed, 07 Apr 2021 09:38:45 GMT
4 Content-Type: application/json; charset=UTF-8
5 Connection: close
6 Content-Length: 104
7
8 {"errMsg":"成功","code":0,"data":
  "0x439bd288afa2ccb410cb94e2bfcebc33c29cd500e989abc14371736353
  ca84cd"}
```

[illegible]

审计结论

解决方案

8、WebKit安全检测

审计结论

解决方案

9、Webview DOM安全检测

审计结论

解决方案

10、SQLite数据库安全检测

对数据库进行检查，未发现敏感信息：

表: cfurl_cache_receiver_data				新建记录	删除记录	模式: JSON	导入	导出	设为空
	entry_ID	isDataOnFS	receiver_data						
	过滤	过滤	过滤						
1	1	0	{'aid': '01A4NNth1R_SScpumTTecU2ZHfQPqGk3tw9XtjkkMwQTm-Vc-'}						
2	2	0	{'msg': 'OK', 'st': 200, 'data': {'uid': '3bc0f1a73ed0b055b74b511715261e17', ...}}						
3	3	0	{'errMsg': '成功', 'code': 0, 'data': {'isNeed': false, 'isForce': false, 'newVersion': ...}}						
4	4	0	{'errMsg': '成功', 'code': 0, 'data': {'actualTxCost': '4872000000000000', 'from': ...}}						
5	5	0	{'jsonrpc': '2.0', 'id': 1, 'result': '0x2540be400'}						
6	6	0	{'errMsg': '', 'code': 0, 'data': {'addr': '1ax1evsd6tg3ejnug6f2vtpq0hjsmt95I0h...						
7	7	0	{'aid': '01AyOfCJwcWZkUkJocOFF5utPupyx9JA-TxyYJA8L-hbVu8-'}						
8	8	0	{'aid': '01Azrlng1yolPx8yEYz7-WNZgw6WFyupkgGAzV89saDR8C7q8-'}						
9	9	0	{'errMsg': '成功', 'code': 0, 'data': {}}						
10	10	1	0DC45D33-18D0-4830-A44D-714C945F3887						
11	11	0	{'errMsg': '成功', 'code': 0, 'data': {'nodelid': '0xc2bae3e813d6ab96562304f43...						
12	12	0	{'errMsg': '成功', 'code': 0, 'data': {'free': '2000000000000000000000', 'loc...						
13	13	0	{'errMsg': '成功', 'code': 0, 'data': {'0xb6cf58adcf432b88598a2ad97ef946c9e...						
14	14	0	{'errMsg': '成功', 'code': 0, 'data': {'hash': '0xb6cf58adcf432b88598a2ad97...						

1

{'msg': 'OK', 'st': 200, 'data': {'uid': '3bc0f1a73ed0b055b74b511715261e17', ...}}

111 个字符

应用

远程(R)

身份

名称

提交

上次修改

大小

审计结论
仅保存了转账记录等正常信息，未发现敏感信息

解决方案
无

11、文件存储安全检测

过程描述

钱包JSON文件明文方式存储在Documents/keystore目录下



审计结论

钱包JSON文明存储，iOS备份机制自动备份Documents文件夹下内容，配置文件存储位置有风险点

解决方案

建议对JSON进行加密后存储并将文件迁移至library目录下，新建目录保存，并将其加入备份排除名单中。

12、SSL Pinning安全检测

过程描述

没有进行双向校验

审计结论

没有进行双向校验

解决方案

建议对SSL证书进行双向校验

13、Deeplinks安全检测

过程描述

查看配置文件：

URL NAME	SCHEMES
fb Editor	fb2374479646134721
weibo Editor	wb3563537424

Showing 1 to 2 of 2 entries

Previous1Next

对其进行常见安全测试

审计结论

未发现安全问题

解决方案

建议如无必要，可以去掉Deeplinks的支持

14、录屏截图安全策略

过程描述

允许截图，但有安全提示：

< 备份助记词

请抄写下方助记词，我们将在下一步进行验证

助记词用于恢复钱包或扫描二维码，请将它准确抄写在纸上并存放在只有您能访问的地方。



请勿截图

如果有人获取了您的助记词，将可以直接获取您的资产！请抄写下助记词并存放在安全的地方。

我知道了

录屏没有限制、也无提示：

正在录制

< 验证助记词

请按顺序点击助记词，以确认您已经正确备份。

1	2	3
4	5	6
7	8	9
10	11	12

usual	ranch	salon	quiz	web
recipe	version	cloth	illness	clap
faculty	betray			

完成备份

清空

审计结论

没有限制截图，但有安全提示，录屏没有任何提示跟限制

解决方案

建议不允许截图私钥、助记词等敏感信息，增加录屏的安全提醒

15、键盘缓存安全检测

过程描述

使用自定义键盘，按键随机排列

审计结论

安全

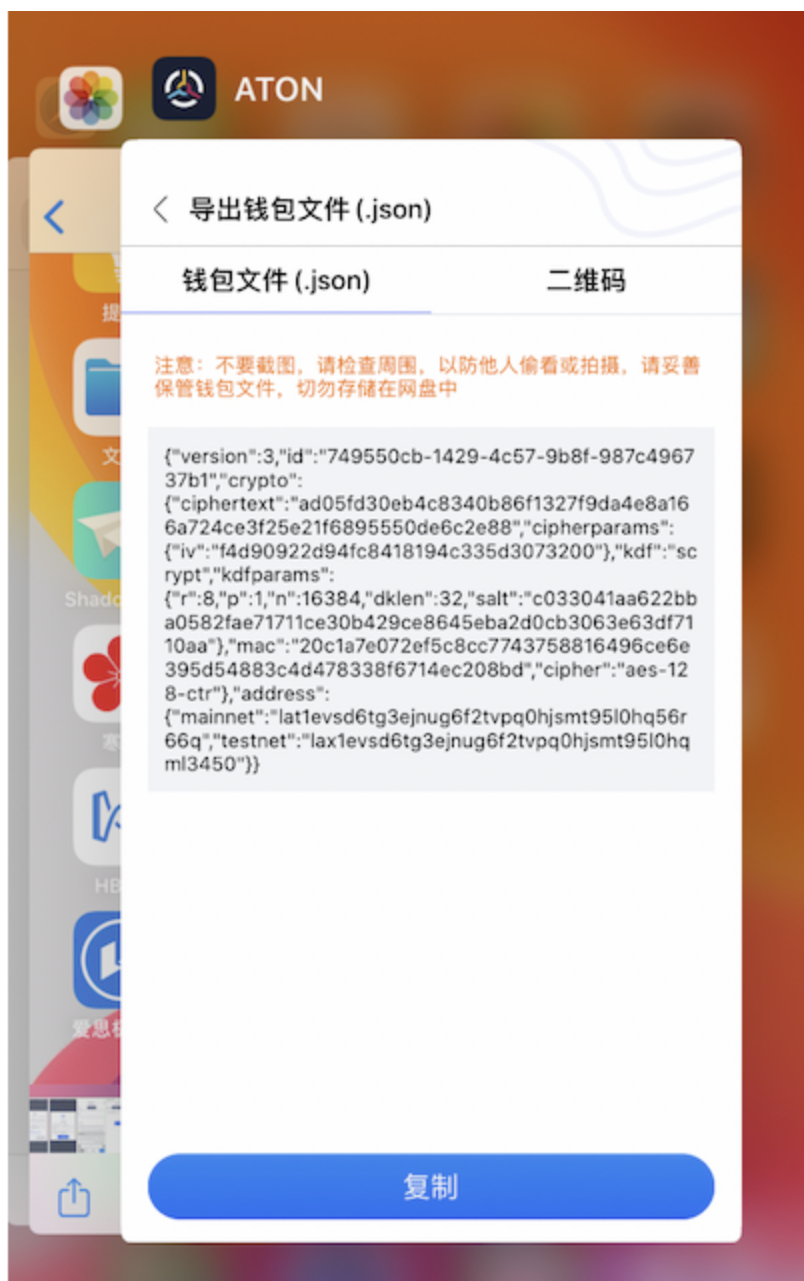
解决方案

无

16、模糊处理及挂起安全检查

过程描述

没有进行模糊处理及重新唤醒的安全检查



审计结论

没有模糊处理，App重新唤醒没有安全检查

解决方案

对App切换及挂起时，进行模糊处理；当App从挂起状态重新唤醒时增加安全检查

17、转账安全审计

过程描述

转账需要验证密码，未发现安全问题

审计结论

无

解决方案

无

18、基于客户端的身份验证安全检测

过程描述

钱包默认配置：打开不需要任何认证，可能存在潜在的安全问题：用户个人资产信息暴露。

审计结论

钱包默认情况下无需身份验证可以直接打开App，用户资产可能暴露

解决方案

建议钱包创建后，强制开启身份验证功能。

免责声明

1、厦门慢雾科技有限公司(下文简称“慢雾”) 仅就本报告出具前项目方已经发生或存在的事实出具本报告, 并就此承担相应责任。对于出具以后项目方发生或存在的未知漏洞及安全事件, 慢雾无法判断其安全状况, 亦不对此承担责任。

2、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。