南明离火
移动应用检测平台

ANDROID 静态分析报告

时光计划录 • v20210415

分析日期: 2025-03-11 17:44:22

i应用概览

文件名称:	com.ynkj.jdb4c.android.apk
文件大小:	7.15MB
应用名称:	时光计划录
软件包名:	com.ynkj.jdb4c.android
主活动:	com.zhangke.shizhong.activity.SplashActivity
版本号:	20210415
最小SDK:	21
目标SDK:	30
加固信息:	360加固
开发框架:	Java/Kotlin
应用程序安全分数:	49/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：安全
MD5:	fc200b052f534d4e4657c66f2631d954
SHA1:	6dbf7ebfaa283f73ccb3ff7511e15fc546926c25
SHA256:	519e96f004fe7250da96c121f29924b7eca5d67e72bc59159674e93491dc1e0

分析结果严重性

高危	中危	信息	安全	关注
3	12	2	2	6

四大组件信息

Activity组件：26个，其中export的有： 0个
Service组件：1个，其中export的有： 0个
Receiver组件：1个，其中export的有： 1个
Provider组件：3个，其中export的有： 0个

证书信息

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: L=c, O=c, OU=c, CN=c
签名算法: rsassa_pkcs1v15
有效期自: 2019-08-01 07:08:24+00:00
有效期至: 2069-07-19 07:08:24+00:00
发行人: L=c, O=c, OU=c, CN=c
序列号: 0x78b769ea
哈希算法: sha256
证书MD5: 1ffadc5081102f0266b63dc1835c5da9
证书SHA1: d4d8d58c0334e4c6d6e9eaaec379c968eff61ea3
证书SHA256: 98d710665ff1200cc1445a2310aaedb534441ae214b6324ab3095f549a8b8b1e
证书SHA512:
9a99d08129381371cf4736674217a47586f2a8ce1c0e829fdd5448ab50fc2fea343f69a0050fcd759053d5cd0af324076ad7642bf9f3824cfb06fea2a4e77cdd

公钥算法: rsa
密钥长度: 2048
指纹: 3870cf1f216a4390a825d478057a87b2a4f1cbe14920bef2166b8eafd3396013
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
android.permission.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。

网络通信安全

序号	范围	严重级别	描述

证书安全分析

高危: 0 | 警告: 1 | 信息: 1

标题	严重程度	描述信息

本报告由南明离火移动安全分析平台生成

已签名应用	信息	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **0** | 警告: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
2	Broadcast Receiver (com.simplepeng.updaterlibrary.DownloadReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。

安全漏洞检测

高危: **3** | 警告: **8** | 信息: **2** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
2	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
3	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
4	已启用。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息。	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

5	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
6	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
7	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
8	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
9	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
10	此应用程序使用SQL Cipher。SQLCipher为sqlite数据库文件提供256位AES加密	信息	OWASP MASVS: MSTG-CRYPTO-1	升级会员：解锁高级权限
11	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
12	应用程序可以读取/写入外部存储器。任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
13	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

14	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
15	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

行为分析

编号	行为	标签	文件
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限

00035	查询已安装的包列表	反射	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	3/30	android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	5/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

域名检测

域名	状态	中国境内	位置信息
note.youdao.com	安全	是	**IP地址:** 106.75.100.17 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
pv.sohu.com	安全	是	**IP地址:** 106.75.100.17 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
upload.qiniu.com	安全	是	**IP地址:** 106.75.100.17 **国家:** 中国 **地区:** 江苏 **城市:** 扬州 **纬度:** 32.397221 **经度:** 119.435600 **查看:** 高德地图
www.douban.com	安全	是	**IP地址:** 140.143.177.206 **国家:** 中国 **地区:** 北京市 **城市:** 北京 **纬度:** 39.911 **经度:** 116.395 **查看:** 高德地图
api.imjad.cn	安全	否	No Geolocation information available.

recommend.wetolink.com	安全	是	**IP地址:** 117.21.200.176 **国家:** 中国 **地区:** 江西 **城市:** 九江 **纬度:** 29.733330 **经度:** 115.983330 **查看:** 高德地图
app-router.leancloud.cn	安全	是	**IP地址:** 106.75.100.17 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
s.s.s	安全	否	No Geolocation information available.
movie.douban.com	安全	是	**IP地址:** 106.75.100.17 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图

URL链接分析

URL信息	源码文件
• 127.0.0.1	cn/leancloud/network/SimpleNetworkingDetector.java
• http://upload.qiniu.com	cn/leancloud/upload/QiniuAccessor.java
• 119.29.29.29	cn/leancloud/network/DNSDetoxicant.java
• https://recommend.wetolink.com/eb/v2/app_recommend/pull?limit=10&package_name=	me/drakeet/support/about/extension/RecommendedLoader.java
• https://%s.%s.%s • https://app-router.leancloud.cn	cn/leancloud/core/AppRouter.java
• http://pv.sohu.com/cityjson?ie=utf-8	com/zhangke/shizhong/utils/ToolsCore.java
• https://note.youdao.com/ynoteshare1/index.html?id=3d521476d84e37970b576a7cdf6f5c89&type=note	com/zhangke/shizhong/dialog/TermsActivity.java
• http://106.14.135.179/immersionbar/phone/ • http://106.14.135.179/immersionbar/	com/zhangke/shizhong/utils/Utils.java
• https://note.youdao.com/ynoteshare1/index.html?id=3cfd60628c0974633c306629dfbc58e1&type=note	com/zhangke/shizhong/dialog/PrivacyPolicyActivity.java
• https://movie.douban.com/ • https://www.douban.com/ • https://api.imjad.cn/	com/zhangke/shizhong/common/AppClient.java

• https://github.com/0xzhangke • https://github.com/0xzhangke/shizhong	com/zhangke/shizhong/page/other/AboutActivity.java

第三方SDK

SDK名称	开发者	描述信息
360 加固	360	360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁。
AgentWeb	Justson	AgentWeb 是一个基于的 Android WebView ， 极度容易使用以及功能强大的库，提供了 Android WebView 一系列的问题解决方案 ， 并且轻量和极度灵活。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。

追踪器

名称	类别	网址
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

密钥凭证

可能的密钥
友盟统计的=> "UMENG_APPKEY" : "5b62bdeba40fa31bc1000254"
友盟统计的=> "UMENG_CHANNEL" : "UMENG"
6077e8310b38b842665d349c
3d521476d84e37970b576a7cdf6f5c89
3cfd60628c0974633c306629dfbc58e1
QxciDjdHjuAIf8VCsqhmGK3O2V7pBQTZ

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。