南明离火
移动应用检测平台

ANDROID 静态分析报告

小星记账 • v3.5.6

分析日期: 2025-05-16 07:35:36

应用概览

文件名称:	小星记账 v3.5.6.apk
文件大小:	14.75MB
应用名称:	小星记账
软件包名:	com.cxincx.xxjz
主活动:	com.cxincx.xxjz.startup.StartupActivity
版本号:	3.5.6
最小SDK:	23
目标SDK:	34
加固信息:	360加固
开发框架:	Java/Kotlin
应用程序安全分数:	50/100 (中风险)
跟踪器检测:	2/432
杀软检测:	2 个杀毒软件报毒
MD5:	fc874cbe3e7799525bd545413369d8e7
SHA1:	a197adc9db4dfdd88e356b54219f8db798e16efb
SHA256:	b66a69559c7a30f43a237e703350b4c3fcd90c023f3cbc153ca829af22c914c

分析结果严重性分布

高危	中危	信息	安全	关注
2	43	3	2	8

四大组件导出状态统计

Activity组件：119个，其中export的有： 14个
Service组件：10个，其中export的有： 5个
Receiver组件：13个，其中export的有： 8个
Provider组件：2个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: L=xm
签名算法: rsassa_pkcs1v15
有效期自: 2021-07-05 08:45:56+00:00
有效期至: 3019-11-06 08:45:56+00:00
发行人: L=xm
序列号: 0x607d5316
哈希算法: sha256
证书MD5: d825f2c6eae2411bf63f76e285d47b04
证书SHA1: 7efb9951d6cdbd33c655a84b359876809c9ddf19
证书SHA256: 654dba666abba24cf57da9ee762ea55f7ef01f33785a5ff9538587759243803c
证书SHA512:
d55a25fa57eeb0ccab1e4676f3f2212fe5df57f81edbdb45dc3dc257e1c455f04d10283a23defe738a233341f2f32141d2d05d0a64e3bce383143b06778edcf2

公钥算法: rsa
密钥长度: 2048
指纹: d459a598c62371b93519bdb441a8f90d0979d99f67c9d29ee2717ad376605516
共检测到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
android.permission.FOREGROUND_SERVICE_DATA_SYNC	普通	允许前台服务进行数据同步	允许常规应用程序使用类型为“dataSync”的 Service.startForeground。
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.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.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.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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
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.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
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.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。

android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动，这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
com.cxincx.xxjz.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.cxincx.xxjz.startup.StartupActivity	Schemes: win.60abca19c9aacd3bc4e5463f://,
com.cxincx.xxjz.ypauth.YPAuthActivity	Schemes: ypauthcdf91ae9353f476f1nbc12689e21bc788://,
com.cxincx.xxjz.detail.scheme.SchemeActivity	Schemes: xxjz://, Hosts: api, Paths: /create, /dialog,

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **0** | 警告: **34** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息

1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	Broadcast Receiver (com.cxincx.xxjz.setting.auto.service.AutoServiceReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
3	Broadcast Receiver (com.cxincx.xxjz.widget.appwidget.AppWidget) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
4	Broadcast Receiver (com.cxincx.xxjz.widget.appwidget.AppWidget2) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
5	Broadcast Receiver (com.cxincx.xxjz.widget.appwidget.MiuiWidget) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
6	Broadcast Receiver (com.cxincx.xxjz.widget.appwidget.MiuiWidget2) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
7	Activity (com.cxincx.xxjz.setting.push.OpenAppActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
8	Activity 设置了 TaskAffinity 属性 (com.cxincx.xxjz.wxapi.WXEntryActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
9	Activity (com.cxincx.xxjz.wxapi.WXEntryActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
10	Activity 设置了 TaskAffinity 属性 (com.cxincx.xxjz.wxapi.WXPayEntryActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
11	Activity (com.cxincx.xxjz.wxapi.WXPayEntryActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
12	Activity (com.cxincx.xxjz.detail.DetailCreateActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

13	Activity (com.cxincx.xxjz.detail.search.RefundSearchActivity) 未受保护。[android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
14	Activity (com.cxincx.xxjz.setting.export.ExportImportHomeActivity) 未受保护。[android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
15	Activity (com.cxincx.xxjz.setting.bx.BxActivity) 未受保护。[android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
16	Activity 设置了 TaskAffinity 属性 (com.cxincx.xxjz.setting.MiuiWidgetDataSettingActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
17	Activity (com.cxincx.xxjz.setting.MiuiWidgetDataSettingActivity) 未受保护。[android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
18	Activity 设置了 TaskAffinity 属性 (com.cxincx.xxjz.setting.MiuiWidgetDataSettingActivity2)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
19	Activity (com.cxincx.xxjz.setting.MiuiWidgetDataSettingActivity2) 未受保护。[android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
20	Activity (com.cxincx.xxjz.detail.PreActivity) 未受保护。[android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
21	Activity (com.cxincx.xxjz.ypauth.YPAuthActivity) 未受保护。[android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
22	Activity 设置了 TaskAffinity 属性 (com.cxincx.xxjz.detail.scheme.SchemeActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
23	Activity (com.cxincx.xxjz.detail.scheme.SchemeActivity) 未受保护。[android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

24	Service (com.cxincx.xxjz.setting.auto.service.AutoService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
25	Broadcast Receiver (com.cxincx.xxjz.setting.auto.service.SmsBroadcastReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BROADCAST_SMS [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
26	Service (com.cxincx.xxjz.setting.push.tile.DetailCreateTile) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
27	Service (com.cxincx.xxjz.setting.push.tile.DetailTemplateTile) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
28	Service (com.cxincx.xxjz.setting.push.tile.SearchTile) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
29	Activity (com.alipay.sdk.app.PayResultActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
30	Activity (com.alipay.sdk.app.AlipayResultActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
31	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

本报告由南明离火移动安全分析平台生成

32	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
33	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
34	高优先级 Intent（1000） - {1} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

高危: **2** | 警告: **7** | 信息: **3** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	应用程序记录日志信息,不得记录敏感信息	警告	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	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
4	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
5	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

6	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
7	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
8	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
9	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
10	使用弱加密算法	高危	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
11	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
12	可能存在路径遍历：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
13	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
14	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY (栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)
1	arm64-v8a/libobjectbox-jni.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会在溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会容易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk', '__memcpy_chk', '__read_chk', '__vsnprintf_chk', '__memmove_chk', '__vsprintf_chk']	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
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
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限

00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	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
00013	读取文件并将其放入流中	文件	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
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
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	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
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
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
00092	发送广播	命令	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	8/30	android.permission.READ_PHONE_STATE android.permission.RECORD_AUDIO android.permission.SYSTEM_ALERT_WINDOW android.permission.CAMERA android.permission.RECEIVE_SMS android.permission.READ_SMS android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	7/46	android.permission.FOREGROUND_SERVICE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE com.google.android.gms.permission.AD_ID

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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
h5.m.taobao.com	安全	是	**IP地址:** 117.85.69.185 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图
cxincx.com	安全	否	**IP地址:** 185.199.109.153 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065613 **经度:** -79.891724 **查看:** Google地图
beian.miit.gov.cn	安全	是	**IP地址:** 124.238.251.188 **国家:** 中国 **地区:** 河北 **城市:** 廊坊 **纬度:** 39.509720 **经度:** 116.694717 **查看:** 高德地图
www.coolapk.com	安全	是	**IP地址:** 124.238.251.188 **国家:** 中国 **地区:** 安徽 **城市:** 苏州 **纬度:** 33.636440 **经度:** 116.978851 **查看:** 高德地图
weibo.com	安全	是	**IP地址:** 124.238.251.188 **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
asr.cloud.tencent.com	安全	是	**IP地址:** 124.238.251.188 **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

objectbox.io	安全	否	**IP地址:** 85.13.163.69 **国家:** 德国 **地区:** 图林根 **城市:** 弗里德斯多夫 **纬度:** 50.604919 **经度:** 11.035770 **查看:** Google 地图
mobilegw.dl.alipaydev.com	安全	是	**IP地址:** 124.238.251.188 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
mobilegw.alipaydev.com	安全	是	**IP地址:** 10.75.132.131 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
dav.jianguoyun.com	安全	是	**IP地址:** 124.238.251.188 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图
www.andykhan.com	安全	否	**IP地址:** 213.171.195.105 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 格洛斯特 **纬度:** 51.865681 **经度:** -2.243100 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件

• https://registry.npmmirror.com/css-select/-/css-select-5.1.0.tgz • https://registry.npmmirror.com/domutils/-/domutils-3.2.1.tgz • https://www.gitbook.com • https://registry.npmmirror.com/parse5/-/parse5-7.2.1.tgz • https://www.coolapk.com/apk/com.cxincx.xxjz • https://github.com/julmot/mark.js • https://registry.npmmirror.com/github-slugid/-/github-slugid-1.0.1.tgz • https://www.alipan.com/cpx/member?userCode=MzAwMTg5 • https://registry.npmmirror.com/domelementtype/-/domelementtype-2.3.0.tgz • https://registry.npmmirror.com/cheerio/-/cheerio-1.0.0.tgz • https://registry.npmmirror.com/iconv-lite/-/iconv-lite-0.6.3.tgz • https://registry.npmmirror.com/safer-buffer/-/safer-buffer-2.1.2.tgz • https://mt2.cn • https://registry.npmmirror.com/gitbook-plugin-anchor-navigation-ex/-/gitbook-plugin-anchor-navigation-ex-1.0.14.tgz • http://jmblog.github.io/color-themes-for-highlightjs • http://jmblog.github.com/color-themes-for-google-code-highlightjs • https://registry.npmmirror.com/gitbook-plugin-chapter-fold/-/gitbook-plugin-chapter-fold-0.0.4.tgz • https://registry.npmmirror.com/htmlparser2/-/htmlparser2-9.1.0.tgz • https://registry.npmmirror.com/dom-serializer/-/dom-serializer-2.0.0.tgz • https://registry.npmmirror.com/whatwg-mimetype/-/whatwg-mimetype-4.0.0.tgz • https://registry.npmmirror.com/cheerio-select/-/cheerio-select-2.1.0.tgz • https://registry.npmmirror.com/html-entities/-/html-entities-1.2.0.tgz • https://registry.npmmirror.com/gitbook-plugin-hide-element/-/gitbook-plugin-hide-element-0.0.4.tgz • https://v.douyin.com/iYLwor48 • https://registry.npmmirror.com/colors/-/colors-1.4.0.tgz • https://github.com/chriskempson/tomorrow-theme • https://cxincx.com/change-log • https://registry.npmmirror.com/gitbook-plugin-search-pro/-/gitbook-plugin-search-pro-2.0.2.tgz • https://registry.npmmirror.com/parse5-parser-stream/-/parse5-parser-stream-7.1.2.tgz • https://registry.npmmirror.com/boolbase/-/boolbase-1.0.0.tgz • https://v.douyin.com/iYLwkCF9 • https://v.douyin.com/iYLwfPd4 • https://v.douyin.com/iYLKRwXK • https://registry.npmmirror.com/domhandler/-/domhandler-5.0.3.tgz • https://registry.npmmirror.com/encoding-sniffer/-/encoding-sniffer-0.2.0.tgz • https://registry.npmmirror.com/css-what/-/css-what-6.1.0.tgz • https://registry.npmmirror.com/entities/-/entities-4.5.0.tgz • https://registry.npmmirror.com/whatwg-encoding/-/whatwg-encoding-3.1.1.tgz • https://v.douyin.com/iYLK8RSR • https://www.wandoujia.com/apps/5981757/history • https://registry.npmmirror.com/undici/-/undici-6.21.0.tgz • https://v.douyin.com/iYLwV2PV • https://git.io/vwTVl • https://txc.gtimg.com/data/652486/2024/0705/d9b6bf267c16d55ef1061f2a2c954d5.webp • https://registry.npmmirror.com/emojify.js/-/emojify.js-1.1.0.tgz • https://registry.npmmirror.com/gitbook-plugin-favicon/-/gitbook-plugin-favicon-0.0.2.tgz • https://registry.npmmirror.com/nth-check/-/nth-check-2.1.1.tgz • https://registry.npmmirror.com/parse5-htmlparser2-tree-adapter/-/parse5-htmlparser2-tree-adapter-7.1.0.tgz • https://registry.npmmirror.com/gitbook-plugin-splitter/-/gitbook-plugin-splitter-0.0.8.tgz	自研引擎-A
• https://cxincx.com/agreement/index.html • https://beian.miit.gov.cn/ • https://cxincx.com/privacy/index.html • https://cxincx.com/user/index.html • https://cxincx.com/change-log/	com/cxincx/xxjz/setting/a.java
• https://cxincx.com	h4/c.java
• https://dav.jianguoyun.com/dav/	h3/d.java

• https://api.mch.weixin.qq.com/pay/refundquery • https://api.mch.weixin.qq.com/pay/orderquery	g3/b.java
• https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s • https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code	h4/a.java
• https://cxincx.com	b1/g.java
• http://www.andykhan.com/jexcelapi/index.html	jxl/read/biff/e0.java
• https://h5.m.taobao.com/mlapp/olist.html	m0/c.java
• https://mobilegw.dl.alipaydev.com/mgw.htm • https://mobilegw.alipaydev.com/mgw.htm • https://mobilegw.alipay.com/mgw.htm	m0/d.java
• https://openapi.alipay.com/gateway.do?	com/cxincx/xxjz/setting/auto/v.java
• https://weibo.com/u/	com/cxincx/xxjz/accountbx.java
• https://www.coolapk.com/	com/cxincx/xxjz/setting/auto/z.java
• https://cxincx.com/agreement/index.html	com/cxincx/xxjz/y_vip/ui/b.java
• https://cxincx.com/agreement/index.html	com/cxincx/xxjz/y_vip/ui/VipActivity.java
• https://mcgw.alipay.com/sdklog.do • https://loggw-exsdk.alipay.com/loggw/logupload.do • https://mobilegw.dl.alipaydev.com/mgw.htm • https://mobilegw.alipaydev.com/mgw.htm • https://mobilegw.alipay.com/mgw.htm	t0/a.java
• https://cxincx.com/config/v2	i0/c.java
• https://asr.cloud.tencent.com/server_time	q3/a.java
• https://openapi.alipay.com/gateway.do?	m4/a.java
• https://cxincx.com/config/rate	com/cxincx/xxjz/setting/auto/q.java
• https://dav.jianguoyun.com/dav/	com/cxincx/xxjz/y_vip/pay/OrderModel.java
• https://cxincx.com/support/	com/cxincx/xxjz/setting/HelpActivity.java
• https://cxincx.com/user/index.html • https://cxincx.com/privacy/index.html	d4/a.java
• http://m.alipay.com/?action=h5quit	a2/f.java
• https://objectbox.io/sync/	lib/arm64-v8a/libobjectbox-jni.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息

Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
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。
LAME	The LAME Project	LAME is a high quality MPEG Audio Layer III (MP3) encoder licensed under the LGPL.
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
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。
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 缓取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

第三方追踪器检测

名称	类别	网址
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
友盟统计的=> "UMENG_APPKEY" : "60bca379c9aacd3bd4e5463f"
友盟统计的=> "UMENG_CHANNEL" : "common"
AKIDvjIdqrdCi6NaiiV1RHIajvLXXVLyNaZM
0d9f25be9724d[illegible]685fe8b9c4c76
b6cbad6c[illegible]d0d209afc69ad3b7a617efaae9b3c47eabe0be42d924936fa78c8001b1fd74b079e5ff9690061dacfa4768e981a526b9ca77156ca36251cf2f906d105481374998a7e6e6e18f75ca98b8ed2eaf86ff402c874cca0a263053f22237858206867d210020daa38c48b20cc9dfd82b44a51aeb5db459b22794e2d649

NQyVeHCndrpk0/2z81859jUzwIDAQAB
zxcvbnmlkjhgfdsaqwertyuiopQWERTYUIOPASDFGHJKLZXCVBNM1234567890
e6b1bdcb890370f2f2419fe06d0fdf7628ad0083d52da1ecfe991164711bbf9297e75353de96f1740695d07610567b1240549af9cbd87d06919ac31c859ad37ab6907c311b4756e1e208775989a4f691bff4bbbc58174d2a96b1d0d970a05114d7ee57dfc33b1bafaf6e0d820e838427018b6435f903df04ba7fd34d73f843df9434b164e0220baabb10c8978c3f4c6b7da79d8220a968356d15090dea07df9606f665cbec14d218dd3d691cce2866a58840971b6a57b76af88b1a65fdffd2c080281a6ab20be5879e0330eb7ff70871ce684e7174ada5dc3159c461375a0796b17ce7beca83cf34f65976d237aee993db48d34a4e344f4d8b7e99119168bdd7
QrMgt8GGYI6T52ZY5AnhtxkLzb8egpFn3j5JELl8H6wtACbUnZ5cc3aYTsTRbmkAkRJeYbtx92LPBWm7nBO9Ull7y5i5MQNmUZNf5QENUcR5tGyo7yJ2G0MBjWvy6iAtlAbacKP0SwOUeUWx5dsBdyhxa7Id1APtybSdDgicBDuNjI0mlZFUzZSS9dmN8lBD0WTVOMz0pRZbR3cysomRXOO1ghqJdTcyDbzpNAEszN8RMGjrzyU7Hjbmwi6YNK
308202bb308201a3a0030201020204607d5316300d06092a864886f70d01010b0500300d310b3009060355040713027866d302d170d3231303730353038343535365a180f333031393131303630383435353 65a300d310b3009060355040713027866d30820122300d06092a864886f70d010101050003820 10f003082010a0282010100b8fa9a390665754ba15957a07dcab016c1d2efef4d25790127226bbedea1be9cc8cca1604f670631e4944ade4a9fd998f862b8b8e3943dc4af6b3f0f04cb982c0c7c68f069d8cf63110232d9bf681665a3a88c32e49fe93adb8d45bee17b0 6daee68ffb0c17055e2856d3b1d62a88606c9a1708ae811cc0c6879df5472b16cba7f57f17fb97739aa395fd75fa01e2274021979adcec3ae17652677bb3 bc43445c82f6a6920ad1425c33af80c1dc2b94afe2d6b1a5e3d35e0441508856f71fdcad6d99b5f4b72e296468ac0a4bfe922309c8963fcc2e7 018d608acb77e75cb329ec 1235f2031691eb8e1045a84b0cb437a1483535647f1ef779f6002a90203010001a321301f301d0603551d0e041604 58231ef6d9c343ce4af5 85cfb837bbb300d06092a864886f70d01010b0500038201010022b7bfad34d967658d67d2ec0cb97a673fb5 a2c4 127cf2064494b29b 52952d503fec9005d40cf6a15ddb3f339498e988821a7f9dbdc3094af8d51da0224a788c5f39015d1fd5d38a415f1 5a fb03e3a4e0552063bc6 75 366f1d59a9de7f3949513c3f16990dc23e1520bc39aa85cf078632f14112f53e3311b2f56144daf005f69c69d0cadbe997eed4f7856b9ff2689ca4217430 b1e2429dbdb64eba68fdcc5b9f6cc885431984b3976b598768bad5e693238d67254536d513cc78351e1208b7 8c2a5d88b7a4b7d25aad f b956be4835ef75b3d2c6f8902fc40aaf8cb571f8ce316e8e07031a8bcb93cce3b6d08d9ba6cb7433fdb67a84
od230r1hB8DiJd4sO72Y3gE9dX1spC0a

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患。