南明离火
移动应用检测平台

ANDROID 静态分析报告

咪咕阅读 • 7.9.7

分析日期: 2025-05-10 10:31:59

应用概览

文件名称:	咪咕阅读 v7.9.7.apk
文件大小:	22.77MB
应用名称:	咪咕阅读
软件包名:	com.andreader.prein
主活动:	com.cmread.bplusc.bookshelf.promptMainActivity
版本号:	7.9.7
最小SDK:	14
目标SDK:	23
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	23/100 (重大风险)
跟踪器检测:	2/432
杀软检测:	5 个杀毒软件报毒
MD5:	0b91ae51104935007665e48b154abe0c
SHA1:	74c0738f7aec8e[illegible]fcc2c5feb14a[illegible]
SHA256:	766ff7f413[illegible]1db125d57c55728[illegible]3b60917350fb4d92eb3c0bf0a7d9e

分析结果严重性分布

高危	中危	信息	安全	关注
54	45	1	1	23

四大组件导出状态统计

Activity组件：[illegible]个，其中export的有： 15个
Service组件：23个，其中export的有： 5个
Receiver组件：15个，其中export的有： 10个
Provider组件：5个，其中export的有： 1个

应用签名证书信息

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: C=ch, ST=liaoning, L=shenyang, O=cmread, OU=neusoft, CN=cm
签名算法: rsassa_pkcs1v15
有效期自: 2010-07-31 02:22:30+00:00
有效期至: 2037-12-16 02:22:30+00:00
发行人: C=ch, ST=liaoning, L=shenyang, O=cmread, OU=neusoft, CN=cm
序列号: 0x4c5388e6
哈希算法: sha1
证书MD5: d525163a0aaa9b96734d2c58fb661713
证书SHA1: 0cdc6d244dd64d7c2ef49c00526294c01420eda4
证书SHA256: df08b7f2bfded129f8a6b3f5c3a05da0858b219246aca7785f0bc9120940d578
证书SHA512:
b6e1b036e1c36df14f0c90b0ab0dd53ba68e48f46a4804238d42844284917b30bc3519bd748b6c4ae6c1c675faff7f6d8de1e828df2fb[illegible]8752542c9378058c

公钥算法: rsa
密钥长度: 1024
指纹: 935fb30144c6ce6aebff47cb155f7ee52741e2635042ec92133c25fc61be2be9
找到 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.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
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.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.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
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.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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
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.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.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.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
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.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
com.android.launcher.permission.UNINSTALL_SHORTCUT	签名	删除快捷方式	这个权限是允许应用程序删除桌面快捷方式。
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
android.permission.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。
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.EXPAND_STATUS_BAR	普通	展开/收拢状态栏	允许应用程序展开或折叠状态条。
android.permission.RESTART_PACKAGES	普通	重启进程	允许程序自己重启或重启其他程序
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.RECEIVE_USER_PRESENT	普通	允许程序唤醒机器	允许应用可以接收点亮屏幕或解锁广播。
cmread.permission.mineMineProviderWritePermission	未知	未知权限	来自 android 引用的未知权限。
android.permission.BROADCAST_PACKAGE_ADDED	签名	接收新增APP的通知	它允许一个应用程序接收到其他应用程序添加新包（即新安装的可执行文件）的广播消息。

android.permission.BROADCAST_PACKAGE_CHANGED	签名	接收APP变化的通知	它允许一个应用程序接收到其他应用程序变化（安装、卸载、修改）的广播消息。
android.permission.BROADCAST_PACKAGE_INSTALL	签名	接收APP安装的通知	它允许一个应用程序接收到其他应用程序安装新包（即新安装的可执行文件）的广播消息。
android.permission.BROADCAST_PACKAGE_REPLACED	签名	接收APP替换的通知	它允许一个应用程序接收到其他应用程序被覆盖安装的广播消息。
com.andreader.prein.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
com.meizu.flyme.push.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.meizu.c2dm.permission.RECEIVE	普通	魅族push服务权限	魅族push服务权限。
com.andreader.prein.push.permission.MESSAGE	未知	未知权限	来自 android 引用的未知权限。
com.andreader.prein.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
getui.permission.GetuiService.com.andreader.prein	未知	未知权限	来自 android 引用的未知权限。
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。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.cmread.bplusc.reader.LocalBookDistribution	Schemes: file://, Hosts: *, Mime Types: text/plain, application/epub+zip, */*, Path Patterns: *.txt, .*\\.epub, .*\\.umd,
com.cmread.bplusc.reader.ui.mainscreen.SMSWakeup	Schemes: http://, https://, about://, javascript://, cmread://, Hosts: wap.cmread.com, sign_for_alipay, cmread.com, Path Prefixes: /client, Path Patterns: .*\\viewbook.a, .*\\huodong.a, .*\\n.a, .*\\.a, /client.*,
com.tencent.tauth.AuthActivity	Schemes: tencent100875257://,
com.cmcc.migupaysdk.activity.UnionPayCashierActivity	Schemes: unionpay://, Hosts: com.andreader.prein,
com.cmcc.migupaysdk.activity.AssetsManageActivity	Schemes: assetmanage://, Hosts: com.andreader.prein,

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	应用程序使用代码签名证书进行签名

Manifest 配置安全分析

高危: **46** | 警告: **33** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Activity (com.cmread.bplusc.reader.comic.ComicReader) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
2	Activity (com.cmread.bplusc.reader.comic.WebpComic.ComicReaderWebp) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
3	Activity (com.cmread.bplusc.reader.mag.MagazineReader) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
4	Activity (com.cmread.bplusc.reader.listeningbook.ListeningBookActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
5	Activity (com.cmread.bplusc.bookshelf.AccountSecurityActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
6	Activity (com.cmread.bplusc.bookshelf.PersonalDataActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
7	Activity (com.cmread.bplusc.personal.PersonalInfoBaseActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
8	Activity (com.cmread.bplusc.personal.JobSelectActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。

9	Activity (com.cmread.bplusc.personal.LocationSelectActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
10	Activity (com.cmread.bplusc.settings.BookUpdateReminderActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
11	Activity (com.cmread.bplusc.reader.BookChapterList) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
12	Activity (com.cmread.bplusc.reader.listeningbook.download.ListeningDownloadManagerActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
13	Activity (com.cmread.bplusc.reader.listeningbook.ListeningContentsActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
14	Activity (com.cmread.bplusc.reader.listeningbook.lock.LockActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
15	Activity (com.cmread.bplusc.reader.book.ChapterListActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
16	Activity (com.cmread.reader.LocalBookReader) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
17	Activity (com.cmread.reader.LocalBookReader) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（23）升级至 29 及以上，从平台层面修复该漏洞。
18	Activity (com.cmread.reader.LocalBookReader) 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。
19	Activity (com.cmread.bplusc.reader.LocalBookDistribution) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
20	Activity (com.cmread.bplusc.reader.LocalBookDistribution) 未受保护。 存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。

21	Activity (com.cmread.reader.BookReader) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
22	Activity (com.cmread.reader.BookReader) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（23）升级至 29 及以上，从平台层面修复该漏洞。
23	Activity (com.cmread.reader.BookReader) 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	Activity (com.cmread.bplusc.reader.paper.pic.MnPaperPicture) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
25	Activity (com.cmread.bplusc.reader.ui.mainscreen.SMS_wakeup) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
26	Activity (com.cmread.bplusc.reader.ui.mainscreen.SMS_wakeup) 未受保护。 存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。
27	Activity (com.cmread.bplusc.recentlyread.RecentlyReadMoreActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
28	Activity (com.cmread.booknote.ui.BookNoteActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
29	Activity (com.cmread.bplusc.reader.recentlyread.MySpaceSetSecurityQuestionActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
30	Activity (com.cmread.bplusc.reader.recentlyread.WillModifyPassword) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
31	Activity (com.cmread.bplusc.plugin.FontManagement) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
32	Activity (com.cmread.bplusc.plugin.TTSManagement) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。

33	Activity (com.andreader.prein.wxapi.WXEntryActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
34	Activity (com.andreader.prein.wxapi.WXEntryActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（23）升级至 29 及以上，从平台层面修复该漏洞。
35	Activity (com.andreader.prein.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。
36	Activity (com.andreader.prein.wxapi.ShareWechatActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
37	Activity (com.andreader.prein.wxapi.ShareWechatActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（23）升级至 29 及以上，从平台层面修复该漏洞。
38	Activity (com.andreader.prein.wxapi.ShareWechatActivity) 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。
39	Activity (com.cmread.bplusc.websearch.MipcaActivityCapture) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
40	Activity (com.cmread.bplusc.websearch.WebScanNoResultActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
41	Activity (com.cmread.bplusc.gexin.GexinWakeup) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
42	Activity (com.cmread.bplusc.reader.playmedia.PEPlayerActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
43	Activity (com.cmread.bplusc.bookshelf.LocalSearchResultArticleActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。

44	Activity (com.andreader.prein.wxapi.WXPayEntryActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（23）升级至 29 及以上，从平台层面修复该漏洞。
45	Activity (com.andreader.prein.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。
46	Activity (com.tencent.tauth.AuthActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
47	Activity (com.tencent.tauth.AuthActivity) 未受保护。存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。
48	Broadcast Receiver (com.cmread.reader.tts.TTSMediaButtonReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
49	Broadcast Receiver (com.cmread.bplusc.reader.listeningbook.ListeningBookMediaButtonReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
50	Activity (com.cmcc.migupaysdk.activity.UnionPayCashierActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
51	Activity (com.cmcc.migupaysdk.activity.UnionPayCashierActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。
52	Activity (com.cmcc.migupaysdk.activity.AssetsManageActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。
53	Activity (com.cmcc.migupaysdk.activity.UnionPayWebActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（23）升级至 29 及以上，从平台层面修复该漏洞。
54	Activity (com.cmcc.migupaysdk.activity.UnionPayWebActivity) 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。

55	Activity (com.cmcc.wallet.openpay.MocamOpenPayEntry) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（23）升级至 29 及以上，从平台层面修复该漏洞。
56	Activity (com.cmcc.wallet.openpay.MocamOpenPayEntry) 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。
57	Service (com.andreader.prein.DemonService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
58	Service (com.andreader.prein.DemoPushService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
59	Broadcast Receiver (com.iBookStar.activityComm.AppInstallReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
60	Activity (com.cmread.settings.readingsettings.ReaderSettingMoreActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
61	Broadcast Receiver (com.igexin.sdk.HmsPushReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
62	Broadcast Receiver (com.huawei.hms.support.api.push.PushEventReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
63	Service (com.meizu.cloud.pushsdk.NotificationService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
64	Broadcast Receiver (com.meizu.cloud.pushsdk.SystemReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
65	Broadcast Receiver (com.igexin.sdk.FlymePushReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。

66	Service (com.xiaomi.mipush.sdk.PushMessageHandler) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
67	Broadcast Receiver (com.igexin.sdk.MiuiPushReceiver) 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。
68	Service (com.igexin.sdk.PushService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
69	Broadcast Receiver (com.igexin.sdk.PushReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
70	Activity 设置了 TaskAffinity 属性 (com.igexin.sdk.PushActivity)	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）。
71	Activity 设置了 TaskAffinity 属性 (com.igexin.sdk.GActivity)	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）。
72	Activity (com.igexin.sdk.GActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（23）升级至 29 及以上，从平台层面修复该漏洞。
73	Activity (com.igexin.sdk.GActivity) 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。
74	Broadcast Receiver (com.igexin.download.DownloadReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
75	Content Provider (com.igexin.download.DownloadProvider) 未受保护。 [android:exported=true]	警告	检测到 Content Provider 已导出，未受任何权限保护，任意应用均可访问。
76	Activity (com.sina.weibo.sdk.share.WbShareTransActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
77	Activity (com.sina.weibo.sdk.share.WbShareTransActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。

本报告由南明离火移动安全分析平台生成

78	Activity (com.sina.weibo.sdk.share.WbShareToStoryActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
79	Activity (com.sina.weibo.sdk.share.WbShareToStoryActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。

代码安全漏洞检测

高危: **8** | 警告: **10** | 信息: **1** | 安全: **1** | 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	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	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	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-2	升级会员：解锁高级权限
4	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
5	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

6	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
7	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
8	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
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	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了被破坏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	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。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
12	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

13	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
14	该文件是World Readable。任何应用程序都可以读取文件	高危	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
15	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
16	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
17	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
18	该文件是World Writable。任何应用程序都可以写入文件	高危	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
19	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

20	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MST G-RESILIENCE-1	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	armeabi/libaes-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。	False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 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	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用
2	armeabi/libaiui.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，以便它会被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 不会在易受攻击的 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	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离

3	armeabi/libkh.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，以便它会被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 不会在易受攻击的 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	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离
4	armeabi/libmg2dbase.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，以便它会被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 不会在易受攻击的 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	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离

5	armeabi/libmgunion.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，以便它会被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 不会在易受攻击的 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	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00009	将游标中的数据放入JSON对象	文件	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
00067	查询IMSI号码	信息收集	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	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
00092	发送广播	命令	升级会员：解锁高级权限
00056	修改语音音量	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
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限

00193	发送短信	短信	升级会员：解锁高级权限
00038	查询电话号码	信息收集	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00134	获取当前WiFi IP地址	WiFi 信息收集	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00121	创建目录	文件 命令	升级会员：解锁高级权限
00042	查询WiFi BSSID及扫描结果	信息收集 WiFi	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
00034	查询当前数据网络类型	信息收集 网络	升级会员：解锁高级权限
00016	获取设备的位置信息并将其放入 JSON 对象	位置 信息收集	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
00104	检查给定路径是否是目录	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
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	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
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	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
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
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
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
00039	启动网络服务器	控制 网络	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
00175	获取通知管理器并取消通知	通知	升级会员：解锁高级权限
00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限
00028	从assets目录中读取文件	文件	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
00025	监视要执行的一般操作	反射	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00126	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	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
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	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
00088	创建到给定主机地址的安全套接字连接	命令 网络	升级会员：解锁高级权限
00148	创建到给定主机地址的套接字连接	网络 命令	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
00146	获取网络运营商名称和 IMSI	电话服务 信息收集	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
00117	获取 IMSI 和网络运营商名称	电话服务 信息收集	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00032	加载外部类	反射	升级会员：解锁高级权限
00166	获取短信正文并从中检索字符串（可能是 PIN / mTAN）	短信 PIN码	升级会员：解锁高级权限
00119	将IMEI号写入文件	信息收集 文件 电话服务 命令	升级会员：解锁高级权限
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00171	将网络运算符与字符串进行比较	网络	升级会员：解锁高级权限
00066	查询ICCID号码	信息收集	升级会员：解锁高级权限
00076	获取当前WiFi信息并放入JSON中	信息收集 WiFi	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 控制	升级会员：解锁高级权限
00064	监控来电状态	控制	升级会员：解锁高级权限
00147	获取当前位置的时间	信息收集 位置	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	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	16/30	android.permission.VIBRATE android.permission.CAMERA android.permission.REQUEST_INSTALL_PACKAGES android.permission.GET_ACCOUNTS android.permission.RECORD_AUDIO android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE android.permission.WRITE_SETTINGS android.permission.READ_CONTACTS android.permission.GET_TASKS android.permission.SEND_SMS android.permission.RECEIVE_BOOT_COMPLETED android.permission.SYSTEM_ALERT_WINDOW android.permission.MODIFY_AUDIO_SETTINGS android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION
其它常用权限	9/46	android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.INTERNET android.permission.CHANGE_NETWORK_STATE android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT android.permission.READ_EXTERNAL_STORAGE android.permission.BLUETOOTH

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
ccc.sys.miui.com	安全	是	**IP地址:** 124.243.239.172 **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
speed.chap2c.com	安全	否	**IP地址:** 46.175.135.11 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图

logs.amap.com	安全	是	**IP地址:** 124.243.239.172 **国家:** 中国 **地区:** 江苏 **城市:** 南通 **纬度:** 32.030296 **经度:** 120.874779 **查看:** 高德地图
dls.migudm.cn	安全	是	**IP地址:** 124.243.239.172 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.061668 **经度:** 118.777092 **查看:** 高德地图
hdns.openspeech.cn	安全	是	**IP地址:** 124.243.239.172 **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
www.idpf.org	安全	否	**IP地址:** 192.67.174.10 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
a.fxltsbl.com	安全	是	**IP地址:** 124.243.239.172 **国家:** 中国 **地区:** 内蒙古自治区 **城市:** 呼和浩特 **纬度:** 40.810650 **经度:** 111.650665 **查看:** 高德地图
demo.m8book.cn	安全	否	No Geolocation information available.
paygate-yf.meituan.com	安全	是	**IP地址:** 36.138.4.148 **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
uem.migu.cn	安全	是	**IP地址:** 124.243.239.172 **国家:** 中国 **地区:** 福建 **城市:** 厦门 **纬度:** 24.479790 **经度:** 118.081871 **查看:** 高德地图
ad.ipadview.com	安全	否	No Geolocation information available.

epubmaker.cmread.com	安全	是	**IP地址:** 211.140.17.101 **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
aiui-ipv6.openspeech.cn	安全	是	**IP地址:** 124.243.239.172 **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
www.daisy.org	安全	否	**IP地址:** 65.52.139.180 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
www.cmread.com	安全	是	**IP地址:** 112.13.170.235 **国家:** 中国 **地区:** 浙江 **城市:** 温州 **纬度:** 27.999420 **经度:** 120.666817 **查看:** 高德地图
alog.umengcloud.com	安全	是	**IP地址:** 124.243.239.172 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.061668 **经度:** 118.777992 **查看:** 高德地图
wap.cmread.com	安全	是	**IP地址:** 101.236.69.63 **国家:** 中国 **地区:** 浙江 **城市:** 温州 **纬度:** 27.999420 **经度:** 120.666817 **查看:** 高德地图
adxserver.ad.cmvideo.cn	安全	是	**IP地址:** 36.138.4.148 **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

tsm.cmpay.com	安全	是	**IP**地址: 58.222.42.53 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
scs.openspeech.cn	安全	是	**IP**地址: 36.138.4.148 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
www.ibookstar.com	安全	是	**IP**地址: 121.40.56.194 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
api.weibo.com	安全	是	**IP**地址: 36.138.4.148 国家: 中国 地区: 云南 城市: 昆明 纬度: 25.038891 经度: 102.718330 查看: 高德地图
cmread.lingxicloud.com	安全	否	No Geolocation information available.
api.ibookstar.com	安全	是	**IP**地址: 36.138.4.148 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
a.10086.cn	安全	是	**IP**地址: 36.138.4.148 国家: 中国 地区: 甘肃 城市: 兰州 纬度: 36.056690 经度: 103.792221 查看: 高德地图
ad.ibookstar.com	安全	否	No Geolocation information available.
record.cmread.com	安全	是	**IP**地址: 112.25.122.118 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

biss.cmread.com	安全	是	**IP地址:** 112.13.170.229 **国家:** 中国 **地区:** 浙江 **城市:** 温州 **纬度:** 27.999420 **经度:** 120.666817 **查看:** 高德地图
m.139site.com	安全	否	**IP地址:** 69.16.230.166 **国家:** 美国 **地区:** 密歇根 **城市:** 兰辛 **纬度:** 42.733280 **经度:** -84.637104 **查看:** Google 地图
mgx.cmread.com	安全	是	**IP地址:** 211.140.17.91 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161685 **查看:** 高德地图
metok.sys.miui.com	安全	是	**IP地址:** 240.181.52.36 **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 链接安全分析

URL信息	源码文件
• http://profandesign.se/swfupload/ • http://cdn.cmread.com/coverFile/470987621/5527c1c8af2ee56056a5f409856b705b48573f3201a/cover180240.jpg • http://cdn.cmread.com/coverFile/473296772/5527c1c8ad93e08405538b49c9844705b84f49b12daf/cover180240.jpg • https://www.dropbox.com/developers • https://developers.google.com • https://open.weibo.com • https://dev.twitter.com • http://cdn.cmread.com/coverFile/471976871/5527c1c8a2e2ee56056a5f4068d4a605b63d315b5163/cover180240.jpg • https://developer.linkedin.com • http://cdn.cmread.com/coverFile/466721554/5527c1c8aee2ee56056a5f40890cc805ae98d6c5dbba/cover180240.jpg • http://getpocket.com/developer/apps/new • http://www.flickr.com/services • http://www.swfupload.org • http://cdn.cmread.com/coverFile/469482592/5527c1c8a393e08405538b4999229a05b5b16285db45/cover180240.jpg • http://cdn.cmread.com/coverFile/449792925/5527c1c8ad93e58805538b46ac4e09058639b86e3a13/cover180240.jpg • http://developers.pinterest.com	

- http://cdn.cmread.com/coverFile/440342966/5527c1c8ade2dfbe056a5f40f53b3b05bbc05d26da01/cover180240.jpg
- http://open.weibo.com
- http://cdn.cmread.com/coverFile/475272449/5527c1c8a293e08405538b498846fa05bc01c36728cb/cover180240.jpg
- https://get.adobe.com/cn/flashplayer
- http://cdn.cmread.com/coverFile/458889822/5527c1c8a193c38405538b4c9915f505992149ea3dba/cover.jpg
- http://open.t.163.com
- http://media.line.me/zh-hant
- http://wap.cmread.com/rbc/p/yssm.jsp?vt=3
- http://cdn.cmread.com/coverFile/472866049/5527c1c8aa93e58805538b46a456a505b7d2db42a110/cover180240.jpg
- https://api.weibo.com/oauth2/default.html
- http://cdn.cmread.com/coverFile/620556864/5527c1c8a593e08405538b49a96dc505ad99a25c8c77/180x240.jpg
- http://www.wapforum.org/DTD/xhtml-mobile10.dtd
- http://cdn.cmread.com/coverFile/441896165/5527c1c8ab93e08405538b49d29f940598fbfb5ed3b7/cover180240.jpg
- http://cdn.cmread.com/coverFile/470203756/5527c1c8ad93c38405538b4cb31c0c05b2cc6d73b2d[illegible]e/cover180240.png

自研引擎-A

- http://cdn.cmread.com/coverFile/455771828/5527c1c8a2e2ee56056a5f4068d77705ae048c67ba52/cover180240.jpg
- http://connect.qq.com/intro/login
- http://wap.cmread.com/cbc/cover_file/6953/409186953/20170310163841/180x240.jpg
- http://note.youdao.com/open/developguide.html
- http://wap.cmread.com/rbc/p/yhfwxy.jsp?vt=3
- http://dev.t.qq.com
- http://dev.renren.com
- http://open.mingdao.com
- http://cdn.cmread.com/coverFile/468019125/5527c1c8a4e2dfbe056a5f40e5101c05ae3cdba4a7f0/cover180240.jpg
- http://cdn.cmread.com/coverFile/620506743/5527c1c8a5e2ee56056a5f4070afbb05b2104836e53a/180x240.jpg
- http://cdn.cmread.com/coverFile/456558180/5527c1c8aa93c38405538b4cb91dcf059104c48bb931/cover180240.jpg
- https://developer.foursquare.com
- http://cdn.cmread.com/coverFile/464903639/5527c1c8aa93e58805538b46a4511305ad035b994792/cover180240.png
- http://vk.com/dev
- http://open.t.sohu.com
- http://www.tumblr.com/developers
- http://www.mob.com
- http://cdn.cmread.com/coverFile/450334714/5527c1c8a7e2eb92056a5f408df02305acad2f4c4a3b/cover180240.jpg
- http://open.kaixin001.com
- http://cdn.cmread.com/coverFile/463023440/5527c1c8a1e2eb92056a5f40862c3705a9cc76b3266c/cover.jpg
- http://www.vinterwebb.se
- http://instagram.com/developer
- http://www.alistapart.com/articles/flashsatay
- http://swfupload.google.com
- http://cdn.cmread.com/coverFile/453711026/5527c1c8af93e08405538b49c1cefd058fefe710f8d6/cover180240.jpg
- http://developers.douban.com
- http://cdn.cmread.com/coverFile/449222851/5527c1c8a3e2ee56056a5f4090c1a305863ea536e18e/cover180240.jpg
- http://sizzlejs.com
- http://open.yixin.im
- http://cdn.cmread.com/coverFile/461734960/5527c1c8a993e08405538b49a0f008059c1cf3d18a53/cover180240.jpg

• javascript:document.body.innerhtml= • http://wap.cmread.com	com/cmread/web/fragment/WebFragment.java
• http://wap.cmread.com/sso/ • http://wap.cmread.com/hbc/ • http://wap.cmread.com/bbc/ • http://wap.cmread.com/mbc/ • http://wap.cmread.com/rbc/ • http://wap.cmread.com/cbc/	com/cmread/config/a.java
• http://cmread.lingxicloud.com/msp.do	com/cmread/bplusc/plugin/TTSManagement.java
• http://wap.cmread.com	com/cmread/network/presenter/g.java
• http://epubmaker.cmread.com:9876/epubmaker/mrmp/clientdownmeb?whiteid=	com/cmread/bplusc/hiddenfeature/a.java
• http://ad.ibookstar.com/api/ad/baitong/return/ • http://ad.ibookstar.com/api/ad/active/return/	com/iBookStar/e/a.java
• http://wap.cmread.com/r/p/messhareback.jsp?vt=3&cm= • http://wap.cmread.com/r/p/messhareback.jsp?vt=3	com/cmread/bplusc/reader/book/picshare/g.java
• https://tsm.cmpay.com/html/commons/?m=getmocam&os=android	com/cmcc/wallet/openpay/MocamOpenPayConfig.java
• http://m.139site.com	com/cmread/bplusc/web/fragment/SimpleWebFragment.java
• www.ibookstar.com	com/iBookStar/activityComm/DownloadService.java
• http://ad.ipadview.com/api/ad/ad/getsc/senad	com/iBookStar/a/f.java
• http://ad.ipadview.com	com/iBookStar/a/e.java
• http://ad.ipadview.com/api/ad	com/iBookStar/a/d.java
• http://ad.ipadview.com/api/ad/ad/senddeviceinfo	com/iBookStar/a/c.java
• http://ad.ipadview.com/api/ad	com/iBookStar/a/b.java
• http://speed.chap2c.com/extra/information/getinformation?positionid=%d&acc=%s • http://speed.chap2c.com/extra/information/list?acc=%s	com/iBookStar/a/a.java
• https://uem.migu.cn:18088/uds/uploadcrash.html	com/migu/uem/crash/d.java
• 10.0.0.200 • 10.0.0.172	com/baidu/b/a/j.java
• https://meta.sys.miui.com	com/xiaomi/b/b.java
• http://api.ibookstar.com/pay/alipay_client.html	com/iBookStar/views/CommonWebView$b.java

• http://ad.ipadview.com/api/ad/banner/getrerouteadparams?bookname=%s&bookauthor=%s&bannertype=100	com/iBookStar/views/BannerAdView.java
• http://a.10086.cn/pams2/l/s.do?c=1427&j=l&p=72&src=5210069799	com/cmread/bplusc/web/hybrideimp/CallTypeJSHandler.java
• https://api.weibo.com/oauth2/default.html	com/cmread/bplusc/reader/ui/share/BindWeiBo.java
• javascript:clearsessionstorage	com/cmread/uilib/view/AdvancedWebView.java
• https://record.cmread.com:7443/alllog.datacollector.web/execute.action?token= • https://record.cmread.com:18443/alllog.statisticanalyser.web/logupload/fileupload?token=	com/neusoft/track/d/b.java
• https://record.cmread.com:7443/alllog.datacollector.web/getxmlconfig.action?token=	com/neusoft/track/c/b.java
• http://cmread.lingxicloud.com/msp.do	com/cmread/bplusc/reader/voicesearch/b.java
• https://api.weibo.com/2/users/counts.json • https://api.weibo.com/2/users/domain_show.json • https://api.weibo.com/2/users/show.json	com/cmread/bplusc/e/b.java
• http://wap.cmread.com	com/cmread/bplusc/bookshelf/gf.java
• http://www.cmread.com/advertise/index.php/pull/ad?place_id=mdawmday mdawmmqsg6kf fhuyeprnmauc2agpuqohe56nnn6kpgn-nt2byhulnxmjoct-qayd	com/cmread/bplusc/bookshelf/fu.java
• http://wap.cmread.com/rbc/p/txt_fxmdh.jsp?discode=	com/cmread/bplusc/h/n.java
• http://logs.amap.com/ws/log/upload?product=%s&type=%s&platform=%s&channel=%s&sign=%s	com/a/ak.java
• https://api.weixin.qq.com/sns/oauth2/access_token?appid=wx48ce50d026c16e5c&secret=e4adcaed3eee2482f01cc6a6c80c17e2&code= • https://api.weixin.qq.com/sns/userinfo?access_token= • https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=wx48ce50d026c16e5c&grant_type=refresh_token&refresh_token=	com/andreader/prein/wxapi/a.java
• javascript:clearsessionstorage	com/cmread/bplusc/reader/paper/MnPaperRichReader.java
• http://m.139site.com	com/cmread/bplusc/web/fragment/SearchResultPageFragment.java
• https://api.weibo.com/oauth2/default.html	com/cmread/bplusc/reader/ui/ShareWeiboActivity.java
• http://221.181.100.64:8088/	com/cmread/reader/m/d.java
• https://a.fxltsbl.com/	cn/richinfo/dm/b/a.java
• 10.0.0.172	com/d/a/a/ac.java

• 211.140.17.101 • 211.140.7.177 • 211.140.7.165 • http://211.140.17.91:80/miguxing_api/fcode/getfcode • http://mgx.cmread.com:80/miguxing_api/fcode/getfcode • 211.140.7.188	com/cmread/bplusc/h/a.java
• javascript:clearsessionstorage	com/cmread/bplusc/shakelottery/ResultDialog.java
• http://biss.cmread.com:8080	com/cmread/bi/e/c.java
• http://wap.cmread.com/r/p/messhareback.jsp?vt=3	com/cmread/bplusc/reader/book/picshare/h.java
• http://wap.cmread.com/sso/p/thirdloginforclient.jsp?e_l=3&client_flag=1&type=1 • http://wap.cmread.com/sso/p/thirdloginforclient.jsp?e_l=3&client_flag=1&type=2	com/cmread/bplusc/layout/ThirdLoginActivity.java
• http://m.139site.com	com/cmread/bplusc/web/fragment/MonthlyWebFragment.java
• http://m.139site.com	com/cmread/bplusc/web/fragment/RechargeWebFragment.java
• http://m.139site.com	com/cmread/bplusc/reader/paper/i.java
• http://m.139site.com	com/cmread/bplusc/web/fragment/MainWebPageFragment.java
• http://m.139site.com	com/cmread/bplusc/web/fragment/CommonWebFragment.java
• http://demo.m8book.cn:8050/10see/index.do	com/index/comicliveplayer/d.java
• https://api.weibo.com/oauth2/default.html	com/cmread/bplusc/login/dh.java
• http://adxserver.ad.cmvideo.cn/request/api10	com/cmread/reader/k/a/c.java
• 211.140.17.101 • 211.140.7.177 • 211.140.7.165 • http://211.140.17.91:80/miguxing_api/fcode/getfcode • 211.140.7.183 • http://mgx.cmread.com:80/miguxing_api/fcode/getfcode	com/cmread/utils/a.java
• https://api.weibo.com/oauth2/revokeoauth2	com/cmread/bplusc/reader/ui/share/w.java
• http://adxserver.ad.cmvideo.cn/request/api10	com/cmread/bookshelf/d/a.java
• http://www.cmread.com/advertise/index.php/pull/ad	com/cmread/reader/k/a/e.java
• http://221.181.100.53:8088	com/cmread/bplusc/reader/mag/az.java
• http://cmread.lingxicloud.com/xtts.do • http://cmread.lingxicloud.com/msp.do	com/cmread/reader/tts/au.java

• http://www.baidu.com/	com/cmread/bi/a.java
• javascript:f_getnewscontent • javascript:top.tlbs={};top.tlbsembed=true	com/cmread/web/view/JSWebView.java
• 10.0.0.172	com/cmread/network/d/d/h.java
• http://wap.cmread.com/r/p/clientdlwap.jsp?vt=3	com/cmread/settings/help/HelpAbout.java
• https://paygate-yf.meituan.com/paygate/notify/alipay/paynotify/simple	com/alipay/test/a.java
• http://www.idpf.org/2007/opf	a/a/a/b/i.java
• http://www.daisy.org/z3986/2005/ncx/	a/a/a/b/f.java
• http://www.idpf.org/2007/opf	a/a/a/b/h.java
• http://ccc.sys.miui.com	com/xiaomi/b/a/f.java
• http://dls.migudm.cn/client/comic/sub_opftp_001/20160902/9000000278/090000003399/20160902111331dvcdhx14_webpq75/00003.webp?st=xuk9ojwusnqwfrmcxeqz2g&e=1499330206 • http://dls.migudm.cn/client/comic/sub_opftp_001/20160902/9000000278/090000003399/20160902111331dvcdhx14_webpq75/00002.webp?st=mluroe0itr7axzul0h8pvg&e=1499330206 • http://dls.migudm.cn/client/comic/sub_opftp_001/20160902/9000000278/090000003399/20160902111331dvcdhx14_webpq75/00005.webp?st=h0-_uxkpmbefibiehndiwg&e=1499330206 • http://dls.migudm.cn/client/comic/sub_opftp_001/20160902/9000000278/090000003399/20160902111331dvcdhx14_webpq75/00006.webp?st=xptngc4qxwzgfwgqsgnvjg&e=1499330206 • http://dls.migudm.cn/client/comic/sub_opftp_001/20160902/9000000278/090000003399/20160902111331dvcdhx14_webpq75/00004.webp?st=nkmphynfpk8o4gl[illegible]o4xg&e=1499330206 • http://dls.migudm.cn/client/comic/sub_opftp_001/20160902/9000000278/090000003399/20160902111331dvcdhx14_webpq75/00001.webp?st=0sab2big8[illegible]k2yoosamha&e=1499330206	com/cmread/bplusc/reader/comic/WebpComic/b/b.java
• http://alog.umengcloud.com/app_logs	com/d/a/c.java
• www.baidu.com	com/neusoft/track/c.java
• http://hdns.openspeech.cn:80/sipt/dsolver • https://aiui-ipv6.openspeech.cn:443/athena/opsync • http://aiui-ipv6.openspeech.cn:80/sync/v1/upload.do • https://aiui-ipv6.openspeech.cn:443/v1.1/servsp/register • 36.7.172.9 • 42.62.116.27 • https://aiui-ipv6.openspeech.cn:443/athena/instant • 103.8.32.157 • http://[illegible].openspeech.cn:80/scs • http://117.121.4.242:3200 • ws://aiui-ipv6.openspeech.cn:80/aiui/v2.1/upload.do • 42.62.116.26 • 117.121.48.213 • 117.121.56.5 • http://aiui-ipv6.openspeech.cn:80/aiui/v1/pushnode.do • http://aiui-ipv6.openspeech.cn:80/sync/v1/syncthird.do • 127.0.0.1	lib/armeabi/libaiui.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
AIUI	iFlyTek	AIUI 为开发者提供了多种集成方式，帮助开发者开发出多样化的语音交互应用。
AndFix	Alibaba	AndFix 是一种在线修复错误而无需重新分发 Android App 的解决方案。
个推	个推	SDK 快速集成，免费注册使用。智能推送+场景推送，有效提升用户活跃度与粘性。
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。
讯飞 SDK	科大讯飞	讯飞开放平台作为全球首个开放的智能交互技术服务平台，致力于为开发者打造一站式智能人机交互解决方案。
微博 SDK	Weibo	微博 Android 平台 SDK 为第三方应用提供了简单易用的微博 API 调用服务，使第三方客户端无需了解复杂的验证机制即可进行授权登陆，并提供微博分享功能，可直接通过微博官方客户端分享微博。
ShareSDK	MobClub	ShareSDK 是全球最流行的应用和手机游戏社交 SDK，到目前为止，我们已经支持了几十万名客户。 ShareSDK 可以轻松支持世界上40多个社交平台的第三方登录、分享和关好友列表操作。短短几个小时，这个小程序包将使您的应用程序完全社会化！想在中国社交平台上发布你的应用吗？这可能是你最好的选择！
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。
HMS Core	Huawei	HMS Core 是华为终端云服务提供的端、云开放能力的合集，助您高效构建精品应用。
Huawei Push	Huawei	华为推送服务（HUAWEI Push Kit）是华为为开发者提供的消息推送平台，建立了从云端到终端的消息推送通道。开发者通过集成 HUAWEI Push Kit 可以实时推送消息到用户终端应用，构筑良好的用户关系，提升用户的感知度和活跃度。
HMS Update	Huawei	用于 HMS SDK 引导升级 Huawei Mobile Services(APK)，提供给系统安装器读取升级文件。
腾讯开放平台	Tencent	腾讯核心内部服务，十年技术沉淀，助你成就更高梦想。
MiPush	Xiaomi	小米消息推送服务在 MIUI 上为系统级通道，并且全平台通用，可以为开发者提供稳定、可靠、高效的推送服务。
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。
Meizu Push	Meizu	魅族推送服务是由魅族公司为开发者提供的消息推送服务，开发者可以向集成了魅族 push SDK 的客户端实时地推送通知或者消息，与用户保持互动，提高活跃率。

第三方追踪器检测

名称	类别	网址
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333

敏感凭证泄露检测

可能的密钥
UniPush推送的=> "MIPUSH_APPKEY" : "XM_5821713812625"
UniPush推送的=> "MIPUSH_APPID" : "XM_2882303761517138625"
凭证信息=> "MANA_APPKEY" : "CN-App-000040-259"
个推-推送服务的=> "PUSH_APPID" : "wR6RDRBkJ071EC4ltvpK86"
华为HMS Core 支付ID的=> "com.huawei.hms.client.cpid" : "cpid=900086000020109266"
UniPush推送的=> "MEIZUPUSH_APPKEY" : "MZ_ee6e833474274c10b1afaac6b85257bd"
UniPush推送的=> "MEIZUPUSH_APPID" : "MZ_111493"
百度地图的=> "com.baidu.lbsapi.API_KEY" : "x8RwT5rBsrT97FYhKxMhkmn18jryktVm"
华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "appid=10084466"
个推-推送服务的=> "PUSH_APPKEY" : "MZsLCJ6zRu85vmn8YNJ2k7"
微信分享的=> "wx_app_id" : "wx48ce50d026c16e5c"
友盟统计的=> "UMENG_APPKEY" : "54f7fae4fd98c59236000b74"
个推-推送服务的=> "PUSH_APPSECRET" : "ee9bVRMoin95h4qxyJfO91"
凭证信息=> "MIGU_APPKEY_AD" : "573a80c1"
71AEC47B7B6BBF4678CF436843209B58
2FDgvkGVlKtvyo6NX8HbSycCiDHWR2gaqJRI3JrAcFbGxZAxTnmUE8MNnhRWfoMZJHX2
e4adcaed3eee2482f01cc6a6c80c17e2
54f7fae4fd98c59236000b74
39280363481451541647
st=xuk9OJWUSNQwFRxcXFQZzg
nIv73IaNK+RyzSwcm0b2Viqn0v6wq3+S5imcdP8zbeX60IAGzRU9Jhtb45S41d95M8vdAgMBAAEC
MIICeAIBADANBgkqhkiG9w0BAQEFAASCAmIwggJeAgEAAoGBAINIb+bvijuh7CRmtYd8cFdM8FsO
MDAwMDAwMDAwMMqsg6KkfHaYeprNmauc2aGPuqOhe56nnn6KpGN
eb94d3ee70624bb5ac1bec1a9a394cb4
BCDAD939567A55E63871424A3C3703D
f6040d0e807aaec325ecf44823765544e92905158169f694b282bf17388632cf95a83bae7d2d235c1f039b0df1dcca5fda619b6f7f459f2ff8d70ddb7b601592fe29fcae5dc028f319b3b12495e67aa5390942a997
50125c27acb4f10f93e07272ced00a30

2f40b4cef39a112b191356c8f0fd0e020
df51b21746a0cb68b7cd6f8f54a99fd7
-39280363481451541647
513C7837EA6F92F24B901BFE899A81A37CF0530F
d525163a0aaa9b96734d2c58fb661713
npik2NKF7ZKLKzUKMS1stjlEmKZV/L2lJ+ab33IyTqxFEXbJ6oY9Lm5AEDTipTQJBAJr4jvM32Fwv
24907259431961377209480304447420314675278854956424737688244507998454379688588314890162679979323703303509407962455321114740230473925801787094352815766245422946132075234850344929148285651531727730533518911880903982108113841855011171179916037741763864091274766288565660656130097561316515972662625404679809749468766758424686005523121587712484197006033276206772443157554459677269191029650152631352883817402115937512620782857384365971336644015984200566902747607268548771819782202264482119368208604967088609640185930251728450410958541809530401165592416371337308398370369103059327974517867858550510249576441592847849402163337
nbuwPkMenQLebVPVuJbndYgAUlXgb3lnKaX+/tEIjFg1N9CjFEjHwDLU5hELavJnKweX2nY2fBytU
2FsPONw4QOqEQkzYvoiuVATWxbyQmsCJ
aad0b4f69f2a8751a8c0f2cc57b04437
a8cb572c8030b2df5c2b622608bea02b0c3e5d4dff3f72c9e3204049a45c0760cd3304a78d5710e0c693cc
id=MDAwMDAwMDAwMMqsg6KKfHuYeprNmauc2aGPuqOhe56nnn6KpGlJ
niUj9efYlhh3nu3Z4M3EgV9WMmSBoqbE23gUCQQCowHkOHMCZdaU5Uu6uHAmpgDcCJRCJ/IF7wHqB

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。