南明离火
移动应用检测平台

ANDROID 静态分析报告

Foya • v4.7.9

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2025-04-10 10:37:02

应用概览

文件名称:	Foya v4.7.9.apk
文件大小:	29.29MB
应用名称:	Foya
软件包名:	net.faifdsvc234ep.rwdsmgcvosdpaf77c
主活动:	com.wind.im.MainActivity
版本号:	4.7.9
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	44/100 (中风险)
跟踪器检测:	1/432
杀软检测:	4 个杀毒软件报毒
MD5:	9bd562133392a0fe1b88a2238dec0618
SHA1:	4ad9cbbfdd54b9db439da0e00976d0d04ee675e4
SHA256:	35268c662bca6c7c6f4da8cc9[illegible]307c5d2911466a6[illegible]143d145c4b6c8d5f

分析结果严重性分布

高危	中危	信息	安全	关注
7	27	2	2	13

四大组件导出状态统计

Activity组件：108个，其中export的有：0个
Service组件：16个，其中export的有：0个
Receiver组件：17个，其中export的有：15个
Provider组件：1个，其中export的有：0个

应用签名证书信息

二进制文件已签名
v1 签名: False

本报告由南明离火移动安全分析平台生成

v2 签名: True
v3 签名: False
v4 签名: None
主题: C=CN, ST=0fMr, L=CdSJ, O=OvSN, OU=lgU8, CN=pumm
签名算法: rsassa_pkcs1v15
有效期自: 2024-09-30 18:16:54+00:00
有效期至: 2052-02-16 18:16:54+00:00
发行人: C=CN, ST=0fMr, L=CdSJ, O=OvSN, OU=lgU8, CN=pumm
序列号: 0x35227e63
哈希算法: sha256
证书MD5: 9e22052572be822b9163d0628c153555
证书SHA1: e7f420dc63185b9bd64d0a88c28f0902469c005d
证书SHA256: a58923ad4534e0d002244f1f2231c471fa18ba681cecdde063e6ebfc62f7639b
证书SHA512:
7bc67031bc75ea10114b0253e4613cabbc8af2db41b410bbf69ba06097e9b7ffff422b77cfafb21df27a73c4cf3f65311a249e3a6[illegible]3c6557fdc86ae941f65de

公钥算法: rsa
密钥长度: 2048
指纹: 5012793d9c82ccafcff8f716c353baf42d857e86614589abacdcbec26cc966c1
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.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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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_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.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.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.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.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。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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。
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.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。
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.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.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）
net.faifdsvc234ep.rwdsmgcvosdpaf77c_com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
net.faifdsvc234ep.rwdsmgcvosdpaf77c_com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
net.faifdsvc234ep.rwdsmgcvosdpaf77c_com.huawei.android.launcher.permission.CHANGE_BADGE	未知	未知权限	来自 android 引用的未知权限。
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.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
net.faifdsvc234ep.rwdsmgcvosdpaf77c.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
net.faifdsvc234ep.rwdsmgcvosdpaf77c_com.meizu.flyme.push.permission.RECEIVE	未知	未知权限	来自 android 引用的未知权限。
net.faifdsvc234ep.rwdsmgcvosdpaf77c.pushpermission.MESSAGE	未知	未知权限	来自 android 引用的未知权限。
net.faifdsvc234ep.rwdsmgcvosdpaf77c_com.meizu.c2dm.permission.RECEIVE	未知	未知权限	来自 android 引用的未知权限。
net.faifdsvc234ep.rwdsmgcvosdpaf77c.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。

本报告由南明离火移动安全分析平台生成

net.faifdsvc234ep.rwdsmgcvosdpaf77c.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
net.faifdsvc234ep.rwdsmgcvosdpaf77c.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
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。
net.faifdsvc234ep.rwdsmgcvosdpaf77c_com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	未知权限	来自 android 引用的未知权限。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯
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。
net.faifdsvc234ep.rwdsmgcvosdpaf77c_com.meizu.flyme.permission.PUSH	未知	未知权限	来自 android 引用的未知权限。
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。
net.faifdsvc234ep.rwdsmgcvosdpaf77c_com.asus.msa.SupplementaryDID.ACCESS	未知	未知权限	来自 android 引用的未知权限。
net.faifdsvc234ep.rwdsmgcvosdpaf77c_freemme.permission.msa	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
	Schemes: tencent1[illegible]://,

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: **0** | 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: **0** | 警告: **17** | 信息: **0** | 屏蔽: **0**

本报告由南明离火移动安全分析平台生成

序号	问题	严重程度	描述信息
1	应用程序具有网络安全配置[android:networkSecurityConfig=@7F160003]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
2	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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。
3	Activity设置了TaskAffinity属性 ()	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名。
4	Broadcast Receiver (com.wind.im.push.receiver.VivoPushMessageReceiverImpl) 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。
5	Broadcast Receiver (com.xiaomi.push.service.receivers.NetworkStatusReceiver) 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。
6	Broadcast Receiver (com.xiaomi.push.service.receivers.PingReceiver) 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。
7	Broadcast Receiver (com.wind.im.push.receiver.XiaomiPushMessageReceiver) 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。
8	Broadcast Receiver (com.wind.im.push.receiver.MeizuPushServerMsgReceiver) 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。
9	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 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。
10	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 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。
11	Broadcast Receiver (com.meizu.cloud.pushsdk.MzPushSystemReceiver) 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。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

12	Broadcast Receiver (androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryChargingProxy) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
13	Broadcast Receiver (androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryNotLowProxy) 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。
14	Broadcast Receiver (androidx.work.impl.background.systemalarm.ConstraintProxy$StorageNotLowProxy) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
15	Broadcast Receiver (androidx.work.impl.background.systemalarm.ConstraintProxy$NetworkStateProxy) 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。
16	Broadcast Receiver (androidx.work.impl.background.systemalarm.RescheduleReceiver) 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。
17	Broadcast Receiver (androidx.work.impl.background.systemalarm.ConstraintProxyUpdateReceiver) 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。
18	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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。

代码安全漏洞检测

高危: **7** | 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	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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

2	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
3	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
4	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
5	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
6	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
7	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
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	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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

10	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
11	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
12	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
13	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
14	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
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
16	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
17	可能存在跨域漏洞。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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

18	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
19	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

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)

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

1	arm64-v8a/librtmp-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
00036	从 res/raw 目录获取资源文件	反射	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
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
00013	读取文件并将其放入流中	文件	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
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
00015	将缓冲流（数据）放入 JSON 对象	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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

00024	Base64解码后写入文件	反射 文件	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
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
00026	方法反射	反射	升级会员：解锁高级权限
00031	检查当前正在运行的应用程序列表	反射 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
00191	获取短信收件箱中的消息	短信	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
00153	通过 HTTP 发送二进制数据	http	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
00025	监视要执行的一般操作	反射	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
00121	创建目录	文件 命令	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
00079	隐藏当前应用程序的图标	规避	升级会员：解锁高级权限
00065	获取SIM卡提供商的国家代码	信息收集	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
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
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
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
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
00130	获取当前WIFI信息	WiFi 信息收集	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
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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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
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
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 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
00189	获取短信内容	短信	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
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
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
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
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
00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

恶意软件常用权限	12/30	android.permission.VIBRATE android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.READ_PHONE_STATE android.permission.GET_TASKS android.permission.MODIFY_AUDIO_SETTINGS android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_CONTACTS android.permission.REQUEST_INSTALL_PACKAGES android.permission.WRITE_SETTINGS
其它常用权限	11/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FOREGROUND_SERVICE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.READ_EXTERNAL_STORAGE android.permission.FLASHLIGHT

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
photo.home.163.com	安全	是	**IP地址:** 111.124.202.251 **国家:** 中国 **地区:** 贵州 **城市:** 遵义 **纬度:** 27.686441 **经度:** 106.907135 **查看:** 高德地图
doh.pub	安全	是	**IP地址:** 1.12.12.21 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
www.hao123.com	安全	是	**IP地址:** 180.101.49.115 **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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

doh.360.cn	安全	是	**IP地址:** 106.63.24.74 **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
norma-external-collect.meizu.com	安全	是	**IP地址:** 183.60.176.112 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
ac.dun.163.com	安全	是	**IP地址:** 180.97.214.232 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
gw.m.163.com	安全	是	**IP地址:** 180.97.214.232 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
resolver.msg.xiaomi.net	安全	是	**IP地址:** 106.120.178.15 **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
api-push.in.meizu.com	安全	否	**IP地址:** 180.97.214.232 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 赫恩登 **纬度:** 38.978210 **经度:** -77.386993 **查看:** Google 地图
ranks.hao.360.com	安全	是	**IP地址:** 180.97.214.232 **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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

www.sina.com.cn	安全	是	**IP地址:** 61.160.227.105 **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
ulogs.umengcloud.com	安全	是	**IP地址:** 180.97.214.232 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.061668 **经度:** 118.77709 **查看:** 高德地图
exoplayer.dev	安全	否	No Geolocation information available.
appgallery.cloud.huawei.com	安全	是	**IP地址:** 49.4.35.16 **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
api.bilibili.com	安全	是	**IP地址:** 117.68.35.16 **国家:** 中国 **地区:** 安徽 **城市:** 六安 **纬度:** 31.650000 **经度:** 118.525002 **查看:** 高德地图
dashif.org	安全	否	No Geolocation information available.
www.zhihu.com	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://openmobile.qq.com/	ce/b.java
• https://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	ce/a.java
• https://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	ce/h$a.java
• https://tbsrecovery.imtt.qq.com/getconfig	le/t.java

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

• https://dns.alidns.com/dns-query • 180.76.76.76 • https://1.12.12.12/dns-query • 101.226.4.6 • 52.80.52.52 • https://223.5.5.5/dns-query • 117.50.10.10 • 223.5.5.5 • 210.2.4.8 • 119.29.29.29 • 1.2.4.8 • 218.30.118.6 • https://doh.360.cn/dns-query • https://doh.pub/dns-query • 223.6.6.6 • 119.28.28.28	a0/c.java
• https://ulogs.umengcloud.com	k.c.java
• 10.0.0.200	pb/x.java
• https://norma-external-collect.meizu.com/android/exchange/getpublickey.do	lb/a.java
• https://api-push.in.meizu.com/garcia/api/client/message/unregisterpush • https://api-push.in.meizu.com/garcia/api/client/message/unsubscribetags • https://api-push.in.meizu.com/garcia/api/client/message/getsubtags • https://api-push.in.meizu.com/garcia/api/client/message/unsuballtags • https://api-push.in.meizu.com/garcia/api/client/message/unsubscribealias • https://api-push.in.meizu.com/garcia/api/client/message/changeallswitch • https://api-push.in.meizu.com/garcia/api/client/message/subscribetags • https://api-push.in.meizu.com/garcia/api/client/message/registerpush • https://api-push.in.meizu.com/garcia/api/client/message/subscribealias • https://api-push.in.meizu.com/garcia/api/client/message/getregisterswitch • https://api-push.in.meizu.com/garcia/api/client/message/changeregisterswitch	uc/a.java
• 127.0.0.1	ld/b.java
• https://api.weixin.qq.com/ • https://graph.qq.com/	aa/k.java

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

• https://www.hao123.com/api/tnwhilte • https://www.zhihu.com/api/v4/search/top_search • https://www.hao123.com/api/getgoodthing • https://www.hao123.com/api/citymenu • https://photo.home.163.com/api/designer/pc/home/index/word • https://ranks.hao.360.com/shortvideo-api/hotnews • https://www.hao123.com/api/getgamedata • https://ac.dun.163.com/v3/d • https://www.hao123.com/api/gethitthecity • https://gw.m.163.com/search/api/v1/pc-wap/rolling-word • https://api.bilibili.com/x/web-interface/nav • https://www.hao123.com/api/sample • https://vd6.l.qq.com/proxyhttp • https://www.hao123.com/api/getgameboxindexdata • https://www.sina.com.cn/api/hotword.json	com/imacapp/messagevm/ChatRoomViewModel$a.java
• 10.38.162.35	ph/a4.java
• https://imgcache.qq.com/ptlogin/static/qzsjump.html?	ud/k$a.java
• https://openmobile.qq.com/oauth2.0/m_jump_by_version?	vd/a.java
• https://resolver.msg.xiaomi.net/psc/?t=a	ph/s0.java
• https://%1$s/gslb/?ver=5.0	ph/o0.java
• http://dashif.org/guidelines/last-segment-number	n1/c.java
• http://%s:%d/%s • 127.0.0.1	w/n.java
• 127.0.0.1	w/l.java
• javascript:window.jsbridge&&jsbridge.callback	yd/b$a.java
• http://%s:%d/%s • 127.0.0.1	w/f.java
• https://wspeed.qq.com/w.cgi	ae/j.java
• https://huatuocode.huatuo.qq.com?plugin=mobile.opensdk.com&cgi=opensdk&type=	ae/f.java
• https://exoplayer.dev/issues/player-accessed-on-wrong-thread	l0/l0.java
• https://appgallery.cloud.huawei.com/app/ • https://play.google.com/store • https://appgallery.cloud.huawei.com • https://play.google.com/store/apps/details?id=	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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。
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
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。
xCrash	iQIYI	xCrash 能为安卓 app 提供捕获 Java 崩溃，native 崩溃和 ANR 的能力，不需要 root 权限或任何系统权限。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。
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。
AgentWeb	Justson	AgentWeb 是一个基于 Android WebView，极其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。
XPopup	li-xiaojun	内置几种了常用弹窗，十几种良好的动画，将弹窗和动画的自定义设计的极其简单。
腾讯开放平台	Tencent	腾讯核心内部服务，二十年技术沉淀，助你成就更高梦想。
vivo Push	vivo	vivo 推送是 Funtouch OS 上系统级消息推送平台，帮助开发者在 vivo 平台有效提升活跃和留存。通过和系统的深度结合，建立稳定可靠、安全可控、高性能的消息推送服务，帮助不同行业的开发者挖掘更多的运营价值。
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。
Matisse	Zhihu	一个设计精美的 Android 图片视频选择器。
EasyPermissions	Google	EasyPermissions 是一个包装器库，用于简化针对 Android M 或更高版本的基本系统权限逻辑。
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。
AppGallery Connect	Huawei	为开发者提供移动应用全生命周期服务，覆盖全终端全场景，降低开发成本，提升运营效率，助力商业成功。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

HMS Core AAID	Huawei	华为推送服务开放能力合集提供的匿名设备标识(AAID) 实体类与令牌实体类包。异步方式获取的 AAID 与令牌通过此包中对应的类承载返回。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本的 Android 屏幕适配方案。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
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。
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
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
凭证信息=> "APP_ID" : "net.faifep.pmmg1b"
openinstall统计的=> "com.openinstall.APP_KEY" : "dw5ulh"
vivo推送的=> "local_iv" : "MzMsMzQsMzUsMzYsMzcsMzgsMzksNDAsNDEsMzIsMzgsMzcsMzYsMzUsMzQsMzMsI0AzNCwzMiwzMywzNywzMywzNCwzMiwzMywzMywzMywzNCw0MSwzNSwzNSwzMiwzMiwjQDMzLDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDMyLDM4LDM3LDMzLDM1LDM0LDM0LDMzLCNAMzQsMzIsMzMsMzMsMzcsMzMsMzQsMzIsMzMsMzMsMzQsNDEsMzUsMzIsMzIsMzI"
e01c0f9672fba0c035d981e5f9d0dd7f
MCwwDQYJKoZIhvcNAQEBBQADGwAwGAIRAMRB/Q0hTCD+XtnQ1pQIefUCAwEAAQ==
a4774df5c743013e61ebd22cfc865ce
d8391a394d4a179e6fe7bdb8a301258b
2A57086C86EF54370C1F6FB37BFC72B1
12345678909876543102
f6040d0e807aaec325ecf44823765544e02905158169f694b282bf17388632cf95a83bae7d2d235c1f039b0df1dcca5fda619b6f7f459f2ff8d70ddb7b601592fe29fcae58c028f319b3b2465e67aa5390942a997a8cb572c8030b2df5c2b622608bea02b0c3e5d4dff3f72c9e3204049a45c0760cd3604af8d57f0e0c693cc
L3N5cy9jbGFzcy9uZXQvd2xhbjAvYWRkcmVzcw==
2C61B7E5357D6AB71E1D9BA721FDE3D3
Y29tLnRlbmNlbnQuYW5kcm9pZC5xcWRvd25sb2FkZXI=
BCC35D4D3606F154F0402AB7634E8490C0B244C2675C3C6238986987024F0C02

本报告由南明离火移动安全分析平台生成

4a2ca769d79f4856bb3bd982d30de790
aHR0cHM6Ly8xMzQuMTc1LjcuODU6OTg1Mi9sb2dzL2t3ZTNpdTFzaGFn
f3423b38048b29b9e7bfec5c73e51ca1
aHR0cHM6Ly80Ny4xMTMuMTEzLjEzMDo5ODUyL2xvZ3Mva3dlM2l1MXNoYWc=
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

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。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成