南明离火
移动应用检测平台

ANDROID 静态分析报告

Buddy Token - v1067

分析日期: 2025-07-06 09:36:40

应用概览

文件名称:	Buddy Token v1067.apk
文件大小:	12.63MB
应用名称:	Buddy Token
软件包名:	com.qqyyhtv.fyijgwm
主活动:	.main
版本号:	1067
最小SDK:	14
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	51/100 (中风险)
杀软检测:	11 个杀毒软件报毒
MD5:	24e6609d52cabea21ab92187b96470c2
SHA1:	37c9aa140689fb9ee02e4ab119c03b03afcf2abc
SHA256:	efd1ff7eb9bf8b57bf4e0f1a386684eebbb40fd019e2967d59577921c9db1ee7

分析结果严重性分布

高危	中危	信息	安全	关注
1	60	1	2	0

四大组件导出状态统计

Activity组件：18个，其中export的有： 17个
Service组件：15个，其中export的有： 15个
Receiver组件：19个，其中export的有： 19个
Provider组件：1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: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-04-15 22:40:50+00:00
有效期至: 2035-09-01 22:40:50+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0xb3998086d056cffa
哈希算法: md5
证书MD5: 8ddb342f2da5408402d7568af21e29f9
证书SHA1: 27196e386b875e76adf700e7ea84e4c6eee33dfa
证书SHA256: c8a2e9bccf597c2fb6dc66bee293fc13f2fc47ec77bc6b2b0d52c11f51192ab8
证书SHA512:
5d802f24d6ac76c708a8e7afe28fd97e038f888cef6665fb9b4a92234c311d6ff42127ccb2eb5a898f4e7e4a558f6ef602d43d1a2ebae9f002a6598e72fd2d83

公钥算法: rsa
密钥长度: 2048
指纹: 65ba0830722d5767f8779e37d0d9c67562f03ec63a2889af655ee9c59effb434
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.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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
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.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.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.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.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.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.SYSTEM_ERROR_WINDOW	未知	未知权限	来自 android 引用的未知权限。

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.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入手机或 SIM 卡中存储的短信。恶意应用程序可借此删除您的信息。
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.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_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录。
android.permission.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。且不被允许拨打紧急电话。
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.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.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.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.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.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.FOREGROUND_SERVICE_MEDIA_PLAYBACK	普通	启用用于媒体播放的前台服务	允许常规应用程序使用类型为“mediaPlayback”的 Service.startForeground。
android.permission.ACCESS_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可。
com.android.alarm.permission.SET_ALARM	未知	未知权限	来自 android 引用的未知权限。
android.permission.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。
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.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.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.ACTION_MANAGE_OVERLAY_PERMISSION	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。
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.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。
android.permission.FOREGROUND_SERVICE_LOCATION	普通	允许前台服务与位置使用	允许常规应用程序使用类型为“location”的 Service.startForeground。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
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.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。

可浏览 Activity 组件分析

ACTIVITY	INTENT
.main	Schemes: sms://, smsto://, mms://, mmsto://,

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: **53** | 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	应用数据存在泄露风险 未设置[android:allowBackup]标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。
3	Broadcast Receiver (anywheresoftware.b4a.objects.AdminReceiver2) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_DEVICE_ADMIN [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。
4	Service (.asdsa_retop) 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。
5	Broadcast Receiver (.asdsa_retop$asdsa_retop_BR) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
6	Activity (.asdsawqe_sq) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
7	Activity (.asdsda_edqwewq) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
8	Service (.backgroundservice) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
9	Broadcast Receiver (.backgroundservice$backgroundservice_BR) 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。
10	Activity (.asdsa_edwqeq) 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。
11	Activity (.dasdsa_wqewqfby 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 (.daskj_dasdsa_aa) 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 (.ddsa_ewqiuewq) 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 (.dsadas_dsadsa) 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 (.dsadas_rewq) 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 (.dsadsa_dsadsa) 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。
17	Activity (.dsadsa_tytrpo) 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	Service (.dsadsoper_mnfg) 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。
19	Broadcast Receiver (.dsadsoper_mnfg$dsadsoper_mnfg_BR) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
20	Activity (.dsadwq_rewqwe) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
21	Service (.dsda_reiwurew) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
22	Broadcast Receiver (.dsda_reiwurew$dsda_reiwurew_BR) 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。
23	Service (.dsdas_klfdgfd) 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。
24	Broadcast Receiver (.dsdas_klfdgfd$dsdas_klfdgfd_BR) 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。
25	Activity (.dsdsa_qweqwewq) 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。

26	Service (.dsdsaiuewq_wqwe) 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。
27	Broadcast Receiver (.dsdsaiuewq_wqwe$dsdsaiuewq_wqwe_BR) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
28	Service (.dtrsbnotisuntilactv) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
29	Broadcast Receiver (.dtrsbnotisuntilactv$dtrsbnotisuntilactv_BR) 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。
30	Activity (.forc_activateacc) 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	Activity (.gfdgfd_gewrtre) 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。
32	Activity (.homescreen) 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。
33	Service (.managerservice) 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。
34	Broadcast Receiver (.managerservice$managerservice_BR) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
35	Service (.mediaprojectionbackservice) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
36	Broadcast Receiver (.mediaprojectionbackservice$mediaprojectionbackservice_BR) 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。
37	Broadcast Receiver (.myreceiver) 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。
38	Service (.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。

本报告由南明离火移动安全分析平台生成

39	Broadcast Receiver (.notificationservice$notificationservice_BR) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
40	Activity (.perm_writesys) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
41	Service (.service1) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
42	Broadcast Receiver (.service1$service1_BR) 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。
43	Service (.service2) 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。
44	Broadcast Receiver (.service2$service2_BR) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BROADCAST_WAP_PUSH [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
45	Service (.service3) 受权限保护，但应检查权限保护级别。 Permission: android.permission.SEND_RESPOND_VIA_MESSAGE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
46	Broadcast Receiver (.service3$service3_BR) 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。
47	Service (.service4) 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。
48	Broadcast Receiver (.service4$service4_BR) 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。

49	Broadcast Receiver (.startatbootreceiver) 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。
50	Service (.starter) 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。
51	Broadcast Receiver (.starter$starter_BR) 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。
52	Activity (.wakeupdv) 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。
53	Broadcast Receiver (.httputils2service) 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。

代码安全漏洞检测

高危: **1** | 警告: **6** | 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
2	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
3	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
4	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

5	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
6	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
7	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
8	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
9	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

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/libacnatilib.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

本报告由南明离火移动安全分析平台生成

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
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
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
00036	从 res/raw 目录获取资源文件	反射	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
00191	获取短信收件箱中的消息	短信	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
00025	监视要执行的一般操作	反射	升级会员：解锁高级权限
00204	获取默认铃声	信息收集	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
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	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
00209	从最新渲染图像中获取像素	信息收集	升级会员：解锁高级权限
00210	将最新渲染图像中的像素复制到位图中	信息收集	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
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
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
00054	从文件安装其他APK	反射	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
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
00056	修改语音音量	控制	升级会员：解锁高级权限
00167	使用辅助功能服务执行在活动窗口中获取 root 的操作	无障碍服务	升级会员：解锁高级权限

00160	使用辅助服务执行通过视图 ID 获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00161	对可访问性节点信息执行可访问性服务操作	无障碍服务	升级会员：解锁高级权限
00206	检查视图的文本是否包含给定的字符串	无障碍服务	升级会员：解锁高级权限
00159	使用辅助服务执行通过文本获取节点信息的操作	无障碍服务	升级会员：解锁高级权限
00207	检查视图的资源名称是否包含给定的字符串	无障碍服务	升级会员：解锁高级权限
00168	使用辅助服务执行全局操作，通过文本获取节点信息	无障碍服务	升级会员：解锁高级权限
00169	使用辅助服务执行全局操作，通过视图 ID 获取节点信息	无障碍服务	升级会员：解锁高级权限
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	升级会员：解锁高级权限
00002	打开相机并拍照	相机	升级会员：解锁高级权限
00128	查询用户账户信息	信息收集 账号	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	19/30	android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.READ_SMS android.permission.WRITE_SMS android.permission.READ_CONTACTS android.permission.READ_CALL_LOG android.permission.CALL_PHONE android.permission.SEND_SMS android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.RECEIVE_BOOT_COMPLETED android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.REQUEST_INSTALL_PACKAGES android.permission.WRITE_CALL_LOG android.permission.RECEIVE_SMS android.permission.WRITE_CONTACTS

其它常用权限	9/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NOTIFICATION_POLICY android.permission.READ_EXTERNAL_STORAGE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.ACCESS_BACKGROUND_LOCATION

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。

URL 链接安全分析

URL信息	源码文件
• 127.0.0.1	anywheresoftware/b4a/objects/SocketWrapper.java
• 127.0.0.1 • 194.61.120.177	com/qqyyhtv/fyijgwm/globalparameters.java
• 194.61.120.177 • https://www.google.com	com/qqyyhtv/fyijgwm/main.java
• 194.61.120.177	com/qqyyhtv/fyijgwm/backgroundservice.java
• https://invalid-url/	com/qqyyhtv/fyijgwm/httpjob.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Jetpack Test	Google	在 Android 中进行测试。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

敏感凭证泄露检测

可能的密钥

Y29tLmFuZHJvaWQuc3lzdGVtdWk6aWQvdml2b19waW5fZWRpdHRleHQ=
YW5kcm9pZC5pbnRlbnQuYWN0aW9uLklOU1RBTExfUEFDS0FHRQ==
aHR0cHM6Ly9hcGkucGF3YW4ua3JkL2d0cmFuc2xhdGU/ZnJvbT1lbiZ0bz0=
Y29tLmFuZHJvaWQuc3lzdGVtdWkuc3RhdHVzYmFyLnBob25lLlN5c3RlbVVJRGlhbG9n
YW5kcm9pZC5pbnRlbnQuYWN0aW9uLkNMT1NFX1NZU1RFTV9ESUFMT0dT
OjUxMTQ0L2luamVjdGlvbnN1cGxvYWQvemlwcGVkL2V4dHJhZmlsZXMuemlw
Y29tLm1pdWkuc2VjdXJpdHljZW50ZXI6aWQvY2hlY2tfYm94
YW5kcm9pZC5pbnRlbnQuY2F0ZWdvcnkuSE9NRQ==
Y29tLmFuZHJvaWQuc3lzdGVtdWk6aWQvcGFzc3dvcmRFbnRyeQ==
Y29tLmFuZHJvaWQuc3lzdGVtdWk=
Y29tLm1pdWkuc2VjdXJpdHljZW50ZXI6aWQvaW50ZXJjZXB0X3dhcm5fY29udGVudF9lbmQ=
YW5kcm9pZC5zZXR0aW5ncy5hY3Rpb24uTUFOQUdFX09WRVJMQVlfUEVSTUlTU0lPTg==
aXNOb3RpZmljYXRpb25Qb2xpY3lBY2Nlc3NHcmFudGVk
Y29tLm1pdWkuaG9tZS5sYXVuY2hlci51bmluc3RhbGwuRGVsZXRlRGlhbG9n
YW5kcm9pZC50ZWxlcGhvbnkuU21zTWVzc2FnZQ==
Y29tLmFuZHJvaWQuc3lzdGVtdWk6aWQvZGVsZXRlX2J1dHRvbg==
Q2xzX1Blcm1fTm90aWZpY2F0aW9uIHRpbWVyQ2xhc3I9UaWNr
Y29tLmFuZHJvaWQuc2V0dGluZ3M6aWQvYWM0aW9uX2J1dHRvbg==
Q2xzX1Blcm1fU3lzV3J0ZSB0aW1lckNoZWNrZXJfVGljaw==
Y29tLmFuZHJvaWQuc3lzdGVtdWk6aWQva2V5
Y29tLmFuZHJvaWQuc3lzdGVtdWk6aWQvdml2b19laWQpdF90ZXh0
YXBwbGljYXRpb24vdm5kLmFuZHJvaWQudGFia2FnZS1hcmNoaXZl
YW5kcm9pZC5zZXR0aW5ncy5hY3Rpb24uUFOQUdFX1dSSVRFX1NFVFRJTkdT
UG93ZXIgLS0tLT4gUmVhbF9DaGVja2VyIA==
YW5kcm9pZC5wcm92aWRlci5UZWxlcGhvbnkuU01TX1JFQ0VJVkVE
YW5kcm9pZC5zZXR0aW5ncy5BQ1RJT05fTk9USUZJQ0FUSU9OX0xJU1RFTkVSX1NFVFRJTkdT
Y29tLmFuZHJvaWQubGF1bmNoZXI6aWQvYnRuX25lZ2F0aXZl
YW55d2hlcmVzb2Z0d2FyZS5iNGEuSU9uQWN0aXZpdHlSZXN1bHQ=

YW5kcm9pZC5zZXR0aW5ncy5SRVFVRVNUX0lHTk9SRV9CQVRURVJZX09QVElNSVpBVElPTlM=
d3NfR2V0X0RldmljZV9DYWxsTG9ncw==
Y29tLm1pdWkuYXBwbWFuYWdlci5BcHBsaWNhdGlvbnNEZXRhaWxzQWN0aXZpdHk=
Y29tLmFuZHJvaWQuc3lzdGVtdWk6aWQvZml4ZWRQaW5FbnRyeQ==
Y29tLmFuZHJvaWQuc3lzdGVtdWk6aWQvY29sb3JMb2NrUGF0dGVyblZpZXc=
Y29tLmFuZHJvaWQuc2V0dGluZ3M6aWQvYnV0dG9uMg==
U2VuZF9JbXBvcnRhbnRfVmlld3NfT25seQ==
d3NfSGlkZV9BcHBEYXRhX0luZm8=
Y29tLm1pdWkuaG9tZTppZC91bmluc3RhbGxfZHJvcF90YXJnZXQ=
YW5kcm9pZC5zZXR0aW5ncy5OT1RJRklDQVRJT05fUE9MSUNZX0FDQ0VTU19TRVRUSU5HUw==
Y29tLmFuZHJvaWQucGFja2FnZWluc3RhbGxlcjppZC9wZXJtaXNzaW9uX2FsbG93X2J1dHRvbg==
U2VuZF9VbmlucHN0YWxsX0NlcnRhaW5BcHA=
Y29tLm1pdWkuc2VjdXJpdHljZW50ZXI6aWQvaW50ZXJjZXB0X3dhcm5fYWxsb3c=
U2VuZF9UZXh0X0Zyb21QQ1RvQW5kcm9pZERldmljZQ==
OjUxMTQ0L2luamVjdGlvbnN1cGxvYWQv
U2VuZF9HbG9iYWxBY3Rpb25fRnJvbVBDVG9BZHJvaWQ=
Y29tLmFuZHJvaWQuc3lzdGVtdWk6aWQvbG9jazFhcdHRkcm5WaWV3
aXNBdXRvU3lzdERhbG9nQ2xrZXIgOiA=
YW5kcm9pZC52aWV3LldpbmRvdzpbmHnZXIkTGF5b3V0UGFyYW1z
Y29tLmFuZHJvaWQucGVybWlzc2lvbmNvbnRyb2xsZXI6aWQvcGVybWlzc2lvbl9hbGxvd19idXR0b24=
Y29tLmFuZHJvaWQuc2V0dGluZ3M6aWQvbG9jazFhdHRcm4=
YW5kcm9pZC5wcm92aWRlci5UZWxlcGhvbnkuU31z
Y29tLm9wcG9uby5GF1bmNoZXI6aWQvZGVuF9zaG9ydGN1dHNfY29udGFpbmVy
YW5kcm9pZC5hcHAuU3RhdHVzQnFyTWFuYWdlcg==
VGVsZXBob255LlNtcV5jbnXhnRzLkVYVFJBX1BBQ0tBR0VfTkFNRQ==
U2VuZF9DbGlja1Sgm0tUENUb0FuZHJvaWREZXZpY2U=
YW5kcm9pZC5wcm92aWRlci5UZWxlcGhvbnkuQUNUSU9OX0NIQU5HRV9ERUZBVUxU
U2VuZF9VbkxvY2tTY3JlZW5fT3ZlcmxheQ==

d3NfU2VuZF9VbmIuc3RhbGxfQ2VydGFpbkFwcA==
Y29tLmFuZHJvaWQuc3lzdGVtdWk6aWQvcGluRW50cnk=
YW5kcm9pZC5pbnRlbnQuYWN0aW9uLk1BSU4=
Y29tLmFuZHJvaWQuc3lzdGVtdWk6aWQvc2VjX2Znc19tYW5hZ2VyX3JlY3ljbGVyX3ZpZXc=
Y29tLmFuZHJvaWQuc2V0dGluZ3M6aWQvYWxsb3dfYnV0dG9u
U2VuZF9TaG93X1BhdHRyZW5fQnV0dG9ucw==
U2VuZF9DYWxsUGhvbmVOdW1iZXI=
c2VuZF9jdXN0b21fZnVsbGJyaWdodA==
U2VuZF9EZXZpY2VTY3JlZW5TaG90X1Blcm1pc3Npb24=
Q2xzX1Blcm1fRHJhdyB0aW1lckNoZWNrZXJfVGljaw==
YW5kcm9pZC5zZXR0aW5ncy5NQU5BR0VfVU5LTk9XTl9BUFBfU09VUkNFUw==
YW5kcm9pZC5pbnRlbnQuYWN0aW9uLkRFTEVURQ==
TW96aWxsYS81LjAgKFdpbmRvd3MgTlQgMTAuMDsgV2luNjQ7IHg2NCkgQXBwbGVXZWJLaXQvNTM3LjM2IChLSFRNTCwgbGlrZSBHZWNrbykgQ2hyb21lLzEyMy4wLjAuMCBTYWZhcmkvNTM3LjM2
Y29tLmFuZHJvaWQubGF1bmNoZXI6aWQvdHh0X3VuaW5zdGFsbF9tYWluX3RpdGxl
UmVxdWVzdF9IVk5DX1RhYmxlVGV4dHNfRnJvbUFuZHJvaWQ=
YW5kcm9pZC5wcm92aWRlci5DYWxsTG9nJENhbGxz
Y29tLmFuZHJvaWQuc3lzdGVtdWk6aWQvZGlhbGVyV4dA==

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。