南明离火
移动应用检测平台

ANDROID 静态分析报告

蒙太奇 • v1.0.5

分析日期: 2025-08-27 16:13:16

应用概览

文件名称:	mtq.1.0.5.apk
文件大小:	48.83MB
应用名称:	蒙太奇
软件包名:	com.uponhere.android.miuun
主活动:	com.uponhere.android.miuun.MainActivity
版本号:	1.0.5
最小SDK:	21
目标SDK:	30
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	42/100 (中风险)
跟踪器检测:	5/432
杀软检测:	2 个杀毒软件报毒
MD5:	04d671a13dd20ebb954682dda41d7f61
SHA1:	de8b1678bf5633fb277eaea5aa01f4823f3267a
SHA256:	fcbbfd09e01259ff2e272b4106674d8e40ae74f98bcfa139c590bbca6c1943c7

分析结果严重性分布

高危	中危	信息	安全	关注
7	21	2	2	0

四大组件导出状态统计

Activity组件：10个，其中export的有： 4个
Service组件：20个，其中export的有： 2个
Receiver组件：9个，其中export的有： 1个
Provider组件：18个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: CN=miuun, OU=miuun, O=miuun, L=miuun, ST=miuun, C=miuun
签名算法: rsassa_pkcs1v15
有效期自: 2025-02-06 08:22:13+00:00
有效期至: 2125-01-13 08:22:13+00:00
发行人: CN=miuun, OU=miuun, O=miuun, L=miuun, ST=miuun, C=miuun
序列号: 0x1
哈希算法: sha256
证书MD5: df7f7ce8875f5d45b5f0f49d47b29ac9
证书SHA1: 48e57d85e3f2b53edab531b21ff333a46abc9169
证书SHA256: 3d6bbc5bf1d5d497cd07cbe98c6bc6df9f7e641e45a68715d8c83d33a7e221d5
证书SHA512:
9ce548a8eab8e531ad1ae4ec41ed85b75cc01eb171ff757931dd576698ffa0a90459760c9bdcb897cf18e40cd22a711c290e918190a62[illegible]ff8a6bea5b24c60

公钥算法: rsa
密钥长度: 2048
指纹: 08a361e474d46a842976b398dacbc6e8ee9fdf089999838a798468a1e224e004
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.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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。
android.permission.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.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.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.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_MULTICAST_STATE	危险	允许接收WLAN多播	允许应用程序接收并非直接向您的设备发送的数据包。这样在查找附近提供的服务时很有用。这种操作所耗电量大于非多播模式。
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.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_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.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_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.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.uponhere.android.miuun.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。
freemme.permission.msa	未知	未知权限	来自 android 引用的未知权限。
com.uponhere.android.miuun.openadsdk.permission.TT_PANGOLIN	未知	未知权限	来自 android 引用的未知权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
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。
com.uponhere.android.miuun.permission.KWSDK_BROADCAST	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_PRIVILEGED_PHONE_STATE	签名(系统)	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.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
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。

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: **10** | 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，改使用加密协议。
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	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
4	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
5	Activity (com.bytedance.android.openliveplugin.stub.activity.DouyinAuthorizeActivityProxy) 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。
6	Activity (com.bytedance.android.openliveplugin.stub.activity.DouyinAuthorizeActivityLiveProcessProxy) 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 (cn.hzjizhun.admin.h5.AdSdkH5Activity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
8	Activity (cn.hzjizhun.admin.h5.VideoPlayActivity) 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。
9	Service (com.kwad.sdk.api.proxy.VideoWallpaperService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_WALLPAPER [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。
10	高优先级 Intent（1000） -{1} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

高危: **6** | 警告: **10** | 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
2	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
3	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
4	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

5	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
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	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
8	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
9	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
10	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
11	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

12	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
13	启用了调试配置。生产版本不能是可调试的	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
14	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
15	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
16	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: MSTG-RESILIENCE-1	升级会员：解锁高级权限
17	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
18	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
19	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置易受到填充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

20	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

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)	SYMBOLSSTRIPPED(裁剪符号表)

1	arm64-v8a/libapp.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	Not Applicable info RELRO 检查不适用于 Flutter/Dart 二进制文件	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 info 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
2	arm64-v8a/libcn_nanzhun_admin_base.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	arm64-v8a/libdevInfo.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	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__memmove_chk']	True info 符号被剥离
4	arm64-v8a/libMt-base.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	True info 二进制文件有以下加固函数: ['__read_chk', '__vsnprintf_chk', '__strlcpy_chk', '__strchr_chk', '__strlen_chk', '__strcpy_chk', '__strncpy_chk', '__memmove_chk']	True info 符号被剥离

5	arm64-v8a/libsaasCorePlayer.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	True info 二进制文件有以下加固函数: ['__strchr_chk', '__snprintf_chk', '__sprintf_chk', '__strlen_chk', '__strcpy_chk']	True info 符号被剥离
6	arm64-v8a/libsaasDownloader.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

7	arm64-v8a/libsgcore.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
8	arm64-v8a/libti-monitor.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	True info 二进制文件有以下加固函数: ['__memcpy_chk', '__vsnprintf_chk', '__memset_chk', '__strlen_chk']	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
00163	创建新的 Socket 并连接到它	socket	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
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
00107	将IMSI号码写入文件	信息收集 电话服务 文件 命令	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
00033	查询IMEI号	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
00067	查询IMSI号码	信息收集	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
00054	从文件安装其他APK	反射	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
00121	创建目录	文件 命令	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
00162	创建 InetSocketAddress 对象并连接到它	socket	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
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
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
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

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
00056	修改语音音量	控制	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
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
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
00066	查询ICCID号码	信息收集	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
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
00153	通过 HTTP 发送二进制数据	http	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
00052	删除内容 URI 指定的媒体（SMS、CALLLOG、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
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
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
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

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
00028	从assets目录中读取文件	文件	升级会员：解锁高级权限
00053	监视给定内容 URI 标识的数据更改（SMS、MMS 等）	短信	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	9/30	android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.REQUEST_INSTALL_PACKAGES android.permission.GET_TASKS android.permission.RECEIVE_BOOT_COMPLETED android.permission.SET_WALLPAPER
其它常用权限	11/46	android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.REORDER_TASKS com.google.android.gms.permission.AD_ID 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
i.snssdk.com	安全	是	**IP**地址: 58.216.14.168 国家: 中国 地区: 中国江苏 城市: 南京 纬度: 32.060255 经度: 118.796877 查看: 高德地图

www.dbunit.org	安全	否	**IP地址:** 74.220.199.51 **国家:** 美国 **地区:** 犹他州 **城市:** 普罗沃 **纬度:** 40.233807 **经度:** -111.658585 **查看:** Google 地图
sdk.spstmind.com	安全	是	**IP地址:** 58.220.52.253 **国家:** 中国 **地区:** 中国江苏 **城市:** 南京 **纬度:** 32.060255 **经度:** 118.796877 **查看:** 高德地图
changemaker.hzsanjiaomao.com	安全	是	**IP地址:** 82.157.26.175 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
adservice.sigmob.cn	安全	是	**IP地址:** 182.92.170.207 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
webaddress.elided	安全	否	No Geolocation information available.
api.ipify.org	安全	否	**IP地址:** 172.67.74.152 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
apps.bytesfield.com	安全	是	**IP地址:** 58.215.50.243 **国家:** 中国 **地区:** 中国江苏 **城市:** 南京 **纬度:** 32.060255 **经度:** 118.796877 **查看:** 高德地图
sdk.hzsanjiaomao.com	安全	是	**IP地址:** 58.218.215.77 **国家:** 中国 **地区:** 中国江苏 **城市:** 南京 **纬度:** 32.060255 **经度:** 118.796877 **查看:** 高德地图

api.spstmind.com	安全	是	**IP地址:** 121.199.61.218 国家: 中国 地区: 浙江 城市: 杭州 纬度: 30.274085 经度: 120.15507 查看: 高德地图
www.toutiaopage.com	安全	是	**IP地址:** 180.101.199.188 国家: 中国 地区: 中国江苏 城市: 南京 纬度: 32.060255 经度: 118.796877 查看: 高德地图
apps.oceanengine.com	安全	是	**IP地址:** 58.215.50.242 国家: 中国 地区: 中国江苏 城市: 南京 纬度: 32.060255 经度: 118.796877 查看: 高德地图
www.sec.co.kr	安全	否	**IP地址:** 112.106.187.200 国家: 大韩民国 地区: 首尔teukbyeolsi 城市: 首尔 纬度: 37.566311 经度: 126.977203 查看: Google 地图
c.tobidad.cn	安全	是	**IP地址:** 39.96.184.178 国家: 中国 地区: 浙江 城市: 杭州 纬度: 30.274085 经度: 120.15507 查看: 高德地图
dc.sigmob.cn	安全	是	**IP地址:** 112.126.7.24 国家: 中国 地区: 中国北京 城市: 北京 纬度: 39.904211 经度: 116.407395 查看: 高德地图
whatwg.org	安全	否	**IP地址:** 165.227.248.76 国家: 美国 地区: 新泽西州 城市: 克利夫顿 纬度: 40.858585 经度: -74.163605 查看: Google 地图

www.chengzijianzhan.com	安全	是	**IP地址:** 121.228.130.192 国家: 中国 地区: 中国江苏 城市: 南京 纬度: 32.060255 经度: 118.796877 查看: 高德地图
inner.shunchangzhixing.com	安全	是	**IP地址:** 123.249.45.71 国家: 中国 地区: 中国北京 城市: 北京 纬度: 39.904211 经度: 116.407395 查看: 高德地图
ad.shunchangzhixing.com	安全	是	**IP地址:** 123.249.106.132 国家: 中国 地区: 中国北京 城市: 北京 纬度: 39.904211 经度: 116.407395 查看: 高德地图
www.samsungapps.com	安全	否	**IP地址:** 54.229.225.161 国家: 爱尔兰 地区: 都柏林 城市: 都柏林 纬度: 53.344151 经度: -6.267249 查看: Google 地图
apps.bytesfield.com	安全	是	**IP地址:** 222.186.18.241 国家: 中国 地区: 中国江苏 城市: 南京 纬度: 32.060255 经度: 118.796877 查看: 高德地图
www.googleapis.cn	安全	否	**IP地址:** 142.250.68.35 国家: 美国 地区: 加利福尼亚 城市: 洛杉矶 纬度: 34.052570 经度: -118.243904 查看: Google 地图
sf6-ttcdn-tos.pstatp.com	安全	是	**IP地址:** 36.250.233.6 国家: 中国 地区: 福建 城市: 厦门市 纬度: 24.479834 经度: 118.089425 查看: 高德地图

URL 链接安全分析

URL信息	源码文件
• https://n.sigmob.cn/mraid/prod/6662/6662.c7506a07.css • https://n.sigmob.cn/mraid/prod/6662/6662.a336d5e1.js	自研引擎-A
• javascript:window.mraidbridge.firereadyevent	com/mbridge/msdk/mbsignalcommon/mraid/a.java
• https://www.samsungapps.com/appquery/appdetail.as?appid=	com/ss/android/downloadlib/g/h.java
• http://api.spstmind.com/api/staevent	j2/d.java
• 1.2.3.4 • http://webaddress.elided	aegon/chromium/base/PiiElider.java
• https://api.ipify.org	w1/f.java
• https://c.tobidad.cn/w/config • https://adservice.sigmob.cn/waterfall/v1 • https://dc.sigmob.cn/log • https://adservice.sigmob.cn/strategy/v6 • https://adservice.sigmob.cn/w/config • https://adservice.sigmob.cn/w/config? • https://adservice.sigmob.cn/extconfig? • https://c.tobidad.cn/w/config?	com/windmill/sdk/strategy/WMSdkConfig.java
• https://play.google.com/store/apps/details?id=	com/mbridge/msdk/foundation/webview/a.java
• https://ad.shunchangzhixing.com/base/ • https://ad.shunchangzhixing.com • https://inner.shunchangzhixing.com	cn/hzjizhun/admin/api/ApiManager.java
• https://ad.shunchangzhixing.com • https://ad.shunchangzhixing.com/keeny.aue/	i/c.java
• javascript:window.navigator.vibrate	com/mbridge/msdk/click/p.java
• 127.0.0.1	com/mbridge/msdk/advanced/view/a.java
• http://www.dbunit.org/properties/datatypeFactory	org/seamless/util/dbunit/H2DBUnitOperations.java
• https://i.snssdk.com/	com/ss/android/downloadad/api/constant/AdBaseConstants.java
• 1.1.1.1 • 9.9.9.9 • 149.112.112.112 • 8.8.4.4 • 8.8.8.8 • 1.0.0.1	aegon/chrome/net/AndroidNetworkLibrary.java
• 3.4.0.3	com/kwai/video/player/BuildConfig.java
• http://inner.shunchangzhixing.com	cn/hzjizhun/admin/base/z.java

• http://sdk.hzsanjiaomao.com/sspconfig/%s.txt • http://changemaker.hzsanjiaomao.com:6688/105009	l1/a.java
• https://gist.github.com/atk/1020396 • http://whatwg.org/html/common-microsyntaxes.html#space-character • http://whatwg.org/html/webappapis.html#dom-windowbase64-btoa • http://whatwg.org/html/webappapis.html#dom-windowbase64-atob • http://whatwg.org/c#alphanumeric-ascii-characters	com/mbridge/msdk/c/b/c.java
• https://play.google.com/	com/mbridge/msdk/click/b.java
• http://www.sec.co.kr/dlna	c6/d.java
• 239.255.255.250	i6/i.java
• https://d.alipay.com	q3/b.java
• http://sdk.spstmind.com/sjmconfig/%s_e.json	m3/c.java
• 239.255.255.250	i6/d.java
• 127.0.0.1	o5/w.java
• file:////android_asset/mbridge_jscommon_authtext.html	com/mbridge/msdk/a.java
• https://play.google.com	com/mbridge/msdk/mbsignalcommon/windvane/WindVaneWebView.java
• https://apps.bytesfield.com • https://apps.bytesfield-b.com	com/ss/android/downloadlib/addownload/compliance/f.java
• www.toutiaopage.com/tetris/page • www.chengzijianzhan.com • https://apps.oceanengine.com/customer/api/app/pkg_info?	com/ss/android/downloadlib/addownload/compliance/b.java
• https://d.alipay.com	a2/a.java
• https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html	com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java
• http://www.google.com? • http://www.google.com	y1/a.java
• https://play.google.com/store/apps/details?id= • https://play.google.com/	com/mbridge/msdk/foundation/tools/aj.java

• file:dash1 • https://live.aliyuncs.com/ • https://videocloud.cn-hangzhou.log.aliyuncs.com/logstores/newplayer/track • file:isoff-main:2011 • file:dash:isoff-basic-on-demand:cm • file:isoff-live:2012 • file:isoff-ondemand:2011 • file:mp2t-simple:2011 • www.googleapis.cn • file:isoff-on-demand:2011 • file:full:2011 • file:mp2t-main:2011 • file:isoff-live:2011	lib/arm64-v8a/libsaasCorePlayer.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
MSA SDK	移动安全联盟	移动智能终端补充设备标识体系统一调用SDK，由中国信息通信研究院泰尔终端实验室、移动安全联盟整合提供，知识产权归中国信息通信研究院所有。
阿里云短视频 SDK	Alibaba	阿里云短视频 SDK 依赖的第三方库
Flutter	Google	Flutter 是谷歌的移动 UI 框架，可以快速在 iOS 和 Android 上构建高质量的原生用户界面。
Pangle SDK	ByteDance	穿山甲是巨量引擎旗下全球应用变现与增长平台，合作优质媒体超 30,000 家，日请求突破 607 亿，日均展示达 100 亿，覆盖 7 亿日活用户，为全球应用和广告主提供高效的用户增长和变现解决方案。
阿里聚安全	Alibaba	阿里聚安全是面向开发者，以移动应用安全为核心的开放平台。
移动统计分析	Umeng	友盟+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。
移动应用推广 SDK	Baidu	百度移动推广SDK(Android)是百度官方推出的移动推广 SDK 在 Android 平台上的版本
快手广告 SDK	快手	快手信息流广告，为您和用户搭建桥梁。
腾讯广告 SDK	Tencent	腾讯广告汇聚腾讯公司全量的应用场景，拥有核心行业数据、营销技术与专业服务能力。
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 WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
xxx@email.elided	aegon/chrome/base/PiiElider.java

第三方追踪器检测

名称	类别	网址
Baidu Mobile Ads		https://reports.exodus-privacy.eu.org/trackers/100
IAB Open Measurement	Advertisement, Identification	https://reports.exodus-privacy.eu.org/trackers/328
Mintegral	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/200
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
"dyStrategy.privateAddress" : "privateAddress"
DFKwWgtuDkKwLZPwD+z8H+N/xj26Vjcdx5KyVj5GxVN=
DFK/HrQgJ+zQW+xUhoPwJ7JgY7K0DkeAWrfXYN==
YkRXhr5AWBPfNgzuH7JQ+2Ha
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
h7KsLkfPW+xUhoPBD+QqJk2MWrfXYN==
LdxThdi1WBKUL75ULBPwJ7JgY7K0DkeAWrfXYN==
936dcbdd57fe235fd7c[illegible]1c2e93da3c4
50e2326ac25aa[illegible]f45493dea50631eb8[illegible]
h7KsLkf[illegible]+xUhoPwJ7JgY7K0DkeAWrfXYN==
258EAFA5-E914-47DA-95CA-C5[illegible]C83B11
DFeuWkH0W+xUhoPwJ7JgY7K0DkeAWrfXYN==
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALjMT+wA6DuUbhfoa6y048s5MXW+8F6nq6LsoaZ1cCuRt08KSFhgy0bjwujKVLKymgQRQQaFRHEjavi3Wwo/PocCAwEAAQ==
DFKwWgtuDkKwLZPwD+z8H+N/xj26Vjcdx5KanjKnxVN=
Y7c14Z2TDbv/Y+xgHFeXDrcshBPUYFT=

0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
6214227cd0a1f50c2d7cde0837359bf496afaf3a
DFK/HrQgJ+zQW+xUhoPBD+QqJk2MWrfXYN==
0cdcc6158160790658d1f033d3db873603250124-
DFKwWgtuDkKwLZPwD+z8H+N/xjQZxVfV+T2SZVe6V2xS5c5n
DkPtYdQTLkfAW+xUhoPwJ7JgY7K0DkeAWrfXYN==
LdxThdi1WBKUL75ULBPBD+QqJk2MWrfXYN==
DFKwWgtuDkKwLZPwD+z8H+N/xjK+n3eyNVx6ZVPn5jcincKZx5f5ncN=

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。