南明离火
移动应用检测平台

ANDROID 静态分析报告

吉享花

享花就花

吉享花 • v3.3.1 安

分析日期: 2024-03-28 16:20:42

应用概览

文件名称:	jxh3.3.12.apk
文件大小:	40.54MB
应用名称:	吉享花
软件包名:	com.lvxin.jxh
主活动:	com.lvxin.jxh.aty.LauchActivity
版本号:	3.3.12
最小SDK:	26
目标SDK:	30
加固信息:	爱加密 加固
应用程序安全分数:	50/100 (中风险)
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	0009faa84158bcc3f8a9a1a309f756a9
SHA1:	0ccf87952f7af68565129e055f819e1fe48ec0bc
SHA256:	3234e4e43cf7461411f29231404b0f0244209303377432d72c442fd81c070fc3

分析结果严重性分布

高危	中危	信息	安全	关注
1	19	10	1	6

四大组件导出状态统计

Activity组件：63个，其中export的有：6个
Service组件：18个，其中export的有：6个
Receiver组件：6个，其中export的有：2个
Provider组件：10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: True
v2 签名: True

v3 签名: False
v4 签名: False
主题: C=CN, ST=guangdong, L=shenzhen, O=lvxin, OU=lvxin, CN=lvxin
签名算法: rsassa_pkcs1v15
有效期自: 2020-03-23 10:59:29+00:00
有效期至: 2045-03-17 10:59:29+00:00
发行人: C=CN, ST=guangdong, L=shenzhen, O=lvxin, OU=lvxin, CN=lvxin
序列号: 0x610ffc62
哈希算法: sha256
证书MD5: 2c0eb7c1fb50415a494014cfa278645d
证书SHA1: c1b073d6c975f75cf6554f93ab2eaca94e2911c5
证书SHA256: f97f9381581de2fe7561e2d10dd26417676fb97df9cedba32d0fd5f9a2330525
证书SHA512:
f89ad05a7d189ccf29853abfdf80f174b5ea3f2022ee115a0bc3219ca06652ee0e686fda9f9e99d1caad6c454a5034695eb27a7fec4eee4b72ebabfc8267a684

公钥算法: rsa
密钥长度: 2048
指纹: d7fa398753a534eab86f6e73b4e5afce39f7a74980451278df509f9b0ba31294
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.READ_PRIVILEGED_PHONE_STATE	未知	未知权限	来自 android 引用的未知权限。
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.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
android.permission.READ_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_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
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错略的经纬度信息，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.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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。

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。
com.lvxin.jxh.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.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.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.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.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。恶意应用程序可能会发现有关其他应用程序的保密信息。
android.permission.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
getui.permission.GetuiService.com.lvxin.jxh	未知	未知权限	来自 android 引用的未知权限。
com.vivo.notification.permission.BADGE_ICON	普通	桌面图标角标	vivo平台桌面图标角标，接入vivo平台后需要用户手动开启，开启完成后收到新消息时，在已安装的应用桌面图标右上角显示“数字角标”。
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.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。
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.lvxin.jxh.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
com.lvxin.jxh.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.lvxin.jxh.aty.MainActivity	Schemes: jixianghuaapp://,

网络通信安全风险分析

高危: **1** | 警告: **0** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

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	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	警告	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

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

序号	问题	严重程度	描述信息
1	应用程序可以安装在存在漏洞的 Android 版本上 Android 8.0, minSdk=26]	警告	该应用程序可以安装在具有多个漏洞的旧版本 Android 上。支持 Android 版本 => 10，API 29 以接收合理的安全更新。
2	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
3	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	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。
4	Activity (com.lvxin.jxh.aty.MainActivity) 未被保护。存在一个intent-filter。	警告	发现 Activity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Activity是显式导出的。
5	Activity (com.lvxin.jxh.wxapi.WXEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。

6	Service (com.xiaomi.mipush.sdk.PushMessageHandler) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.xiaomi.xmsf.permission.MIPUSH_RECEIVE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
7	Broadcast Receiver (com.lvxin.jxh.widget.XIAOMIPUSH) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
8	Activity (com.igexin.sdk.PushActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
9	Activity设置了TaskAffinity属性 (com.igexin.sdk.GActivity)	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
10	Activity (com.igexin.sdk.GActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
11	Service (com.igexin.sdk.GTIntentService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
12	Service (com.igexin.sdk.GService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
13	Activity (com.igexin.sdk.GetuiActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
14	Service (com.igexin.assist.control.stp.StpService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.getui.vendor.push.permission [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
15	Broadcast Receiver (com.igexin.sdk.MiuiPushReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
16	Activity (com.xiaomi.mipush.sdk.NotificationClickedActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。

17	Service (com.vivo.push.sdk.service.CommandClientService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.push.permission.UPSTAGESERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
18	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.lvxin.jxh.permission.PROCESS_PUSH_MSG protectionLevel: signatureOrSystem [android:exported=true]	信息	发现一个 Broadcast Receiver 被导出，但受权限保护。然而，权限的保护级别设置为 signatureOrSystem。建议使用 signature 级别来代替。signature 级别应该适用于大多数情况，并且不依赖于应用程序在设备上的安装位置。
19	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.lvxin.jxh.permission.PROCESS_PUSH_MSG protectionLevel: signatureOrSystem [android:exported=true]	信息	发现一个 Broadcast Receiver 被导出，但受权限保护。然而，权限的保护级别设置为 signatureOrSystem。建议使用 signature 级别来代替。signature 级别应该适用于大多数情况，并且不依赖于应用程序在设备上的安装位置。
20	Service (com.huawei.hms.support.api.push.service.HmsMsgService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
21	Content Provider (com.huawei.hms.support.api.push.PushProvider) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.lvxin.jxh.permission.PUSH_PROVIDER protectionLevel: signatureOrSystem [android:exported=true]	信息	发现一个 Content Provider 被导出，但受权限保护。然而，权限的保护级别设置为 signatureOrSystem。建议使用 signature 级别来代替。signature 级别应该适用于大多数情况，并且不依赖于应用程序在设备上的安装位置。

代码安全漏洞检测

序号	问题	等级	参考标准	文件位置

Native 库安全加固检测

本报告由南明离火移动安全分析平台生成

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/libdetect.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。		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	False warning 符号可用

2	arm64-v8a/libluban.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。		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	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
3	arm64-v8a/libwb_emulator_check.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。		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	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

4	arm64-v8a/libweffmpeg.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。		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 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
5	arm64-v8a/libweyuv.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。		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	False warning 符号可用

6	arm64-v8a/libYTNextCV.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。		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	False warning 符号可用
7	arm64-v8a/libzxprotect.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。		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	False warning 符号可用

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

恶意软件常用权限	11/30	android.permission.READ_CONTACTS android.permission.READ_PHONE_STATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.SYSTEM_ALERT_WINDOW android.permission.CAMERA android.permission.WAKE_LOCK android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.GET_TASKS
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.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.ACCESS_BACKGROUND_LOCATION android.permission.READ_EXTERNAL_STORAGE android.permission.CHANGE_WIFI_STATE android.permission.FOREGROUND_SERVICE android.permission.CHANGE_NETWORK_STATE

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
appgallery.cloud.huawei.com	安全	是	**IP地址:** 49.4.35.16 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
store.hispace.hicloud.com	安全	是	**IP地址:** 49.4.47.241 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
zxid-m.mobileservice.cn	安全	是	**IP地址:** 115.231.163.69 **国家:** China **地区:** Zhejiang **城市:** Jiaxing **纬度:** 30.752199 **经度:** 120.750000 **查看:** 高德地图

id6.me	安全	是	**IP地址:** 42.123.76.150 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
nisportal.10010.com	安全	是	**IP地址:** 123.125.99.214 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
msg.cmpassport.com	安全	是	**IP地址:** 120.232.74.115 **国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.127361 **经度:** 113.264252 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://data-drcn.push.dbankcloud.com • https://data-dre.push.dbankcloud.com • https://store1.hispace.hicloud.com/hwmarket/api/ • https://data-drru.push.dbankcloud.com • https://store3.hispace.hicloud.com/hwmarket/api/ • https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/ • https://grs.dbankcloud.eu • https://data-dra.push.dbankcloud.com • https://grs.dbankcloud.com • https://store-drru.hispace.hicloud.com/hwmarket/api/ • https://metrics1.data.hicloud.com • https://grs.dbankcloud.asia • http://crt.trust-provider.cn/IrustAsiaRSADVTLSCAG2.crt0 • https://store2.hispace.hicloud.com/hwmarket/api/ • https://metrics2.data.hicloud.com • https://metrics5.data.hicloud.com • http://ocsp.trust-provider.cn • https://grs.dbankcloud.cn • https://sectigo.com/CPS0 • https://metrics-dra.dt.hicloud.com	自研引擎分析结果
• https://appgallery.cloud.huawei.com • https://store.hispace.hicloud.com/hwmarket/api/	自研引擎分析结果
• https://nisportal.10010.com:9001 • https://zxid-kt.mobileservice.cn/sdk/said/ping • https://msg.cmpassport.com/h5/getmobile • https://[redacted]/gw/preuniq.do	lib/arm64-v8a/libzxprotect.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
岳鹰全景监控	Alibaba	岳鹰全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。
极光认证 SDK	极光	极光认证整合了三大运营商的网关认证能力，为开发者提供了一键登录和号码认证功能，优化用户注册/登录、号码验证的体验，提高安全性。
爱加密	北京智游网安科技有限公司	针对目前移动应用普遍存在的破解、篡改、劫持、盗版、数据窃取、钓鱼欺诈等各类安全风险，通过行业领先的第六代加固技术，爱加密为用户提供全面的移动应用加固加密技术和攻击防范服务。
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。
腾讯优图 SDK	Tencent	腾讯优图 AI 开放平台提供 AI + 互联网、金融、教育等多元化的人工智能服务和行业解决方案，包括人脸核身、人脸防伪、内容安全等领域的产品和案例。

敏感凭证泄露检测

可能的密钥
友盟统计的 "UMENG_CHANNEL" : "jxh"
华为HMS Core 应用ID的 "com.huawei.hms.client.appid" : "appid=102234077"
卓信ID SDK的 "ZX_CHANNEL_ID" : "C01-GEztJH0JLdBC"
个推SDK的 "PUSH_APPID" : "0CqEWTmzeXAlUL[illegible]ZTSmvq8"
个推SDK的 "GETUI_APPID" : "0CqEWTmzeXA[illegible]ZTSmvq8"
华为HMS Core 应用ID的 "com.huawei.hms.client.appid" : "102234077"
"pwd" : "密码"
"gt_one_login_auth_btn" : "一键登录"
"gt_one_login_auth_btn": "一鍵登錄"

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。