南明离火
移动应用检测平台

ANDROID 静态分析报告

君客 • v6.5.8

分析日期: 2025-05-16 16:50:48

应用概览

文件名称:	君客 v6.5.8.apk
文件大小:	57.35MB
应用名称:	君客
软件包名:	com.xy.jf.junke.apk
主活动:	com.stardust.auojs.inrt.SplashActivity
版本号:	6.5.8
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	49/100 (中风险)
杀软检测:	2 个杀毒软件报毒
MD5:	9208d873d8dbb18fc11b81c1601cea71
SHA1:	e5a074cee846bdcdc63f1e85faf1[illegible]6b5d86003f
SHA256:	084190943722668cc07de8[illegible]3aadbb67f4234625d3[illegible]ea25[illegible]0f77c70e4b7b9

分析结果严重性分布

高危	中危	信息	安全	关注
3	14	2	2	1

四大组件导出状态统计

Activity组件：9个，其中export的有：0个
Service组件：11个，其中export的有：0个
Receiver组件：2个，其中export的有：0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: False
v4 签名: False
主题: CN=junke, OU=junke, O=junke, L=junke, ST=junke, C=junke
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-20 01:25:45+00:00
有效期至: 2085-03-05 01:25:45+00:00
发行人: CN=junke, OU=junke, O=junke, L=junke, ST=junke, C=junke
序列号: 0x1
哈希算法: sha256
证书MD5: d5d870e09227aa4097d41ebf51d94348
证书SHA1: 33f18a0047a5f8f24c0f1c5f3beab923a1df74c7
证书SHA256: 0d4d77d5504c5e58cee128346cd816c5c52b3d38c1a0bc5640f61bc5282f2243
证书SHA512:
9905615154ebbdf4b3f182de7d8dae78e8abbec13ebe6bc821bcd517f9af8ee5aa3cf244b1129be57fbb588064769b18ed0583a1[illegible]a9c17089a7aa11ebd5dc47

公钥算法: rsa
密钥长度: 2048
指纹: 887c3ece5005a3f031f0661d17c890a917e006997526337c04127b736971e671
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.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_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
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。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
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。
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.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.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.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.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	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.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.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.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。
com.termux.permission.RUN_COMMAND	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。
android.permission.WRITE_SECURE_SETTINGS	签名(系统)	修改安全系统设置	允许应用程序修改系统的安全设置数据。普通应用程序不能使用此权限。
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.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。

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: **1** | 警告: **3** | 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	Activity (com.stardust.autojs.inrt.SplashActivity) 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（28）升级至 29 及以上，从平台层面修复该漏洞。
3	Activity 设置了 TaskAffinity 属性 (com.stardust.autojs.core.permission.PermissionRequestActivity)	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）。

4	Activity 设置了 TaskAffinity 属性 (com.stardust.autojs.core.image.capture.ScreenCaptureRequestActivity)	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）。

代码安全漏洞检测

高危: **2** | 警告: **10** | 信息: **2** | 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	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
3	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
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	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
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	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
8	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

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
10	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
11	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
12	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
13	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
14	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
15	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

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/libhiai.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

2	arm64-v8a/libhiai_ir.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']	True info 符号被剥离
3	arm64-v8a/libhiai_ir_build.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	arm64-v8a/libjackpal-androidterm5.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	arm64-v8a/libjackpal-termexec2.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

6	arm64-v8a/libjpeg.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: ['__vsprintf_chk']	True info 符号被剥离
7	arm64-v8a/libleptonica.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: ['__vsprintf_chk', '__vsnprintf_chk', '__strlen_chk']	True info 符号被剥离

8	arm64-v8a/libNative.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: ['__memmove_chk', '__memset_chk', '__memcpy_chk']	True info 符号被剥离
9	arm64-v8a/libpaddle_light_api_shared.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

10	arm64-v8a/libpng.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']	True info 符号被剥离
11	arm64-v8a/libtesseract.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', '__memmove_chk', '__strncpy_chk', '__memset_chk', '__strlen_chk', '__vsprintf_chk', '__vsnprintf_chk', '__read_chk', '__memcpy_chk']	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
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
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
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
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
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
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	升级会员：解锁高级权限
00208	捕获设备屏幕的内容	信息收集 屏幕	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
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
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
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
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
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
00173	获取 AccessibilityNodeInfo 屏幕中的选择并执行操作	无障碍服务	升级会员：解锁高级权限
00045	查询当前运行的应用程序名称	信息收集 反射	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
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
00130	获取当前WIFI信息	WiFi 信息收集	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

00056	修改语音音量	控制	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
00192	获取短信收件箱中的消息	短信	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
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
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
00067	查询IMSI号码	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	6/30	android.permission.SYSTEM_ALERT_WINDOW android.permission.RECEIVE_BOOT_COMPLETED android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.WRITE_SETTINGS android.permission.GET_TASKS
其它常用权限	9/46	android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.FOREGROUND_SERVICE android.permission.REORDER_TASKS

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
mk.autoxjs.com	安全	是	**IP地址:** 120.25.164.233 **国家:** 中国 **地区:** 广东 **城市:** 深圳 **纬度:** 22.545673 **经度:** 114.068108 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://github.com/tj/co/blob/master/Readme.md • https://css-tricks.com/debouncing-throttling-explained-examples • https://travis-ci.org/lodash-archive/lodash-cli • https://github.com/tj/co • https://wzkeimgs.oss-cn-hangzhou.aliyuncs.com/wx/shipinhao1.jpg • https://mdn.io/rest_parameters • https://mathiasbynens.be/notes/javascript-unicode • https://mdn.io/isNaN • https://github.com/lodash/lodash • https://wzkeimgs.oss-cn-hangzhou.aliyuncs.com/%E6%90%9C%E7%B4%A2-%E7%94%A8%E6%88%B72.jpg • https://github.com/mafintosh/end-of-stream • https://mdn.io/Number/isSafeInteger • https://mdn.io/Array/reverse • http://wonko.com/post/html-escaping • http://peter.michaux.ca/articles/lazy-function-definition-pattern • https://github.com/beatgammit/base64-js/issues/42 • https://mdn.io/Number/isNaN • http://wzkeimgs.oss-cn-hangzhou.aliyuncs.com/BZ.jpg • https://github.com/TypeStrong/typedoc/issues/1616 • https://github.com/feross/buffer/pull/148 • https://github.com/slevithan/xregexp/blob/95eeebeb8fac8754d54eafe2b4743661ac1cf028/src/xregexp.js • https://bugzilla.mozilla.org/show_bug.cgi?id=695438 • http://bluebirdjs.com/docs/api/promise.coroutine.html • http://dom.spec.whatwg.org • https://github.com/nodejs/node/blob/v10.8.0/lib/internal/errors.js • http://underscorejs.org/LICENSE • https://dom.spec.whatwg.org • https://openjsf.org • http://www.whatwg.org/specs/web-apps/current-work/multipage/parsing.html • https://mdn.io/String/split • https://img.shields.io/npm/v/bluebird-co.svg?style=flat • https://travis-ci.org/lodash/lodash • https://www.lanzous.com/b05gilch • https://cheerio.js.org • https://github.com/pkaminski • https://feross.org/opensource • http://stackoverflow.com/a/22747272/680742 • https://mths.be/he • https://github.com/feross/buffer/issues/154 • http://goo.gl/rRqMUw • https://github.com/mafintosh/pump • https://github.com/petkaantonov/bluebird • https://github.com/Jonathanzy/bluebird-co/tree/master/benchmark • http://bluebirdjs.com/docs/api/promise.coroutine.addyieldhandler.html • https://github.com/feross/buffer/issues/211 • https://github.com/jharb/object.assign/issues/17 • http://www.whatwg.org/specs/web-apps/current-work/multipage/tree-construction.html • http://javascript.crockford.com/ismin.html • http://underscorejs.org • http://requirejs.org/docs/errors.html • http://babeljs.io/docs/plugins/transform-async-to-module-method • http://mathiasbynens.be/notes/javascript-encoding • http://www.ecma-international.org/ecma-262/7.0 • https://mdn.io/toLowerCase • https://html.spec.whatwg.org/multipage/scripting.html • http://goo.gl/MqrFmXu000au000a • https://saucelabs.com/u/lodash • https://github.com/mathiasbynens/he/blob/36afe179392226cf1b6ccdb16ebbb7a5a844d93a/src/he.js • https://github.com/sindresorhus/p-is-promise/blob/cda35a513bda03f977ad5cde3a079d237e82d7ef/index.js • https://html.spec.whatwg.org/multipage/form-elements.html	自研引擎-A

• https://github.com/bnjmnt4n/lodash-cli.git • https://html.spec.whatwg.org/multipage/parsing.html • https://ark.cn-beijing.volces.com/api/v3/bots/chat/completions • http://eev.ee/blog/2015/09/12/dark-corners-of-unicode • https://github.com/fb55/boolbase • http://creativecommons.org/publicdomain/zero/1.0 • https://github.com/feross/buffer/issues/166 • https://wzkeimgs.oss-cn-hangzhou.aliyuncs.com/%E6%88%91%E7%9A%84-%E7%B2%89%E4%B8%9D%E5%88%97%E8%A1%A8.jpg • https://wzkeimgs.oss-cn-hangzhou.aliyuncs.com/%E8%A7%86%E9%A2%91%E9%A1%B5.jpg • https://wzkeimgs.oss-cn-hangzhou.aliyuncs.com/%E7%9B%B4%E6%92%AD%E6%88%AA%E6%B5%81.jpg • https://mdn.io/Number/isInteger • https://mdn.io/setTimeout • https://github.com/fb55/css-select/pull/43 • https://mdn.io/iteration_protocols • http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd • https://admin.syjfs.com • https://html.spec.whatwg.org/multipage/semantics-other.html • https://npmjs.org/package/bluebird-co • https://github.com/olado/doT • https://github.com/lodash/lodash/blob/4.17.15/dist/lodash.js • https://www.wandoujia.com/apps/7461948/history_v320201 • http://goo.gl/MqrFmXu000a • https://mdn.io/Object/assign • https://v.douyin.com • http://bluebirdjs.com/docs/api-reference.html • https://github.com/WebReflection/get-own-property-symbols/issues/4 • http://www.html5rocks.com/en/tutorials/developertools/sourcemaps • https://img.shields.io/npm/l/bluebird-co.svg?style=flat • https://mdn.io/Structured_clone_algorithm • http://ejohn.org/blog/javascript-micro-templating • https://lodash.com/license • https://github.com/tc39/proposal-shadowrealm/pull/384 • https://travis-ci.org/novacrazy/bluebird-co • https://github.com/nodejs/node/commit/112cc7c27551254aa2b17098fb774867f05ed0d5 • https://github.com/novacrazy/bluebird-co/issues • https://lodash.com/custom-builds • https://github.com/lodash/lodash.git • https://mdn.io/Array/slice • https://img.shields.io/npm/dm/bluebird-co.svg?style=flat • http://wzkeimgs.oss-cn-hangzhou.aliyuncs.com/XHS.jpg • https://mdn.io/String/replace • https://github.com/tj/co/issues/180 • https://github.com/novacrazy/bluebird-co • https://mdn.io/clearTimeout • https://developer.chrome.com/extensions/sandboxingEval • https://mdn.io/Number/isFinite • https://mdn.io/round • https://lodash.com/icon.svg • https://github.com/lodash/lodash/tree/4.17.21-npm • https://mdn.io/toUpperCase • https://mdn.io/spread_operator • https://travis-ci.org/novacrazy/bluebird-co.svg?branch=master • https://github.com/jashkenas/underscore/pull/1247 • http://ecma-international.org/ecma-262/7.0 • https://feross.org • https://lodash.com/ • https://goo.gl/f5i56i • https://mathiasbynens.be/notes/ambiguous-ampersands • https://wzkeimgs.oss-cn-hangzhou.aliyuncs.com/banner_pink.jpg	
• http://127.0.0.1	com/stardust/autojs/rhino/debug/Dim.java

本报告由南明离火移动安全分析平台生成

• http://mk.autoxjs.com/pages/ykapp/choisefeature	com/stardust/auojs/inrt/FeatureActivity.java
• file:/android_asset/ • file:/android_asset • file:/android_asset/modules/npm • file:/android_asset/modules	com/stardust/autojs/engine/module/AssetAndUrlModuleSourceProvider.java
• http://120.25.164.233:8080/appstore/app/checkversion?id=22	com/stardust/auojs/inrt/util/UpdateUtil.java
• 112.74.161.35	com/stardust/auojs/inrt/SplashActivity$onCreate$1.java
• http://jackpal.github.com/android-terminal-emulator/help/index.html • https://github.com/vinc3m1/roundedimageview • https://github.com/vinc3m1 • https://github.com/vinc3m1/roundedimageview.git	自研引擎-S
• https://github.com/opencv/opencv/issues/16739	lib/arm64-v8a/libNative.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
HiAI Foundation	HUAWEI	芯片能力开放，快速转化和迁移已有模型，借助异构调度和 NPU 加速，实现更佳性能、更低功耗。
C++ 共享库	Android	在 Android 应用中运行原生代码。
LibJPEG	Independent JPEG Group	This package contains C software to implement JPEG image encoding, decoding, and transcoding. JPEG is a standardized compression method for full-color and grayscale images.
Paddle Lite	Baidu	Paddle Lite 是一个高性能、轻量级、灵活性强且易于扩展的深度学习推理框架，定位于支持包括移动端、嵌入式以及边缘端在内的多种硬件平台。当前 Paddle Lite 不仅在百度内部业务中得到全面应用，也成功支持了众多外部用户和企业的生产任务。
OpenCV	OpenCV	OpenCV 是一个跨平台的计算机视觉库，可用于开发实时的图像处理、计算机视觉以及模式识别程序。
AndroidP7zip	hzy3774	An Android decompress and extract library, P7Zip port for Android.
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
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。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。

敏感凭证泄露检测

可能的密钥

"pref_controlkey_default" : "5"
"key_use_volume_control_running" : "key_use_volume_control_running"
"key_stable_mode" : "key_stable_mode"
"key_enable_floating_window" : "key_enable_floating_window"
"key_print_java_stack_trace" : "key_print_java_stack_trace"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"key_dont_show_main_activity" : "key_dont_show_main_activity"
"key_keep_running_with_foreground_service" : "key_keep_running_with_foreground_service"
"pref_fnkey_default" : "4"
"special_keys" : "Spezialtasten"
"key_enable_accessibility_service_by_root" : "key_enable_accessibility_service_by_root"
"key_enable_accessibility_service" : "key_enable_accessibility_service"

免责声明及风险提示: