南明离火
移动应用检测平台

ANDROID 静态分析报告

漫天星 • v3.0.2

分析日期: 2025-10-08 07:52:53

应用概览

文件名称:	漫天星3.0.2v5修复版.apk
文件大小:	31.59MB
应用名称:	漫天星
软件包名:	com.ljh.lingjiehui
主活动:	com.junyue.novel.ui.SplashActivity
版本号:	3.0.2
最小SDK:	24
目标SDK:	29
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:	5/432
杀软检测:	AI评估：可能有安全隐患
MD5:	874be0353e2642b468b31f65c4adb315
SHA1:	408b9b80de06b53503dea715045ea61dadeef578
SHA256:	277689af2089218...

分析结果严重性分布

高危	中危	信息	安全	关注
5	27	3	1	0

四大组件导出状态统计

Activity组件：390个，其中export的有： 5个
Service组件：23个，其中export的有： 3个
Receiver组件：0个，其中export的有： 3个
Provider组件：21个，其中export的有： 1个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=cn, L=cn, CN=zhou
签名算法: rsassa_pkcs1v15
有效期自: 2017-04-21 10:13:03+00:00
有效期至: 2019-06-18 10:13:03+00:00
发行人: C=cn, L=cn, CN=zhou
序列号: 0x12f8bfa
哈希算法: sha1
证书MD5: 71c7b4ab43cbaf4fd934b8492ce260e1
证书SHA1: ff6ddfdd55c912fc722fb03fe97f31e5defc540f
证书SHA256: 745393ccd8d25240f2cb4b8af42737c5cf00864cc3301b56d772d86cc36dc341
证书SHA512:
384cfc9fe4ad5c4d42330eb30f9b56472a63ea3983571d39a18936dbc4d5dfbb704891bd38727f3d53a27eee25d2b90c0bfb307c0b514aeb260b745ae044b9d9

公钥算法: rsa
密钥长度: 2048
指纹: d671f9f607ba3f8233a3bbe9e4312fea01df70160a7ee8a43c110c46273cc265
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_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.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.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_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。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标	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.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。
com.ljh.lingjiehui.permission.JPUSH_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
android.permission.RECEIVE_USER_PRESENT	普通	允许程序唤醒机器	允许应用可以接收点亮屏幕或解锁广播。
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。
com.ljh.lingjiehui_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.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.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.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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
com.ljh.lingjiehui_ android.permission.ACCESS_FINE_LOCATION	未知	未知权限	来自 android 引用的未知权限。
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.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.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，在手机屏幕关闭后台进程仍然运行。
com.ljh.lingjiehui_com.google.android.gms.permission.AD_ID	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	允许应用将长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.ljh.lingjiehui_com.asus.msa.SupplementaryDID.ACCESS	未知	未知权限	来自 android 引用的未知权限。
com.ljh.lingjiehui.openadsdk.permission.TT_PANGOLIN	未知	未知权限	来自 android 引用的未知权限。
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）

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: **17** | 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	应用已配置网络安全策略 [android:networkSecurityConfig=@7F14000F]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
3	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
4	Activity (cn.jpush.android.ui.PopWinActivity) 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。
5	Service (cn.jpush.android.service.PushService) 未受保护。 存在 intent-filter。	警告	检测到 Service 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Service 被显式导出，存在安全风险。
6	Service (cn.jpush.android.service.DaemonService) 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。
7	Activity 设置了 TaskAffinity 属性 (cn.jpush.android.service.DActivity)	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）。
8	Activity (cn.jpush.android.service.DActivity) 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	Content Provider (cn.jpush.android.service.DownloadProvider) 未受保护。 [android:exported=true]	警告	检测到 Content Provider 已导出，未受任何权限保护，任意应用均可访问。
10	Broadcast Receiver (cn.jpush.android.service.PushReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
11	Broadcast Receiver (com.junyue.push.CustomPushMessageReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
12	Broadcast Receiver (com.junyue.push.PushMessageReceiver) 未受保护。 存在 intent-filter。	警告	检测到 Broadcast Receiver 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Broadcast Receiver 被显式导出，存在安全风险。
13	Activity 设置了 TaskAffinity 属性 (cn.jpush.android.service.JNotifyActivity)	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）。

本报告由南明离火移动安全分析平台生成

14	Activity (cn.jpush.android.service.JNotifyActivity) 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	Service (com.junyue.push.PushService) 未受保护。 存在 intent-filter。	警告	检测到 Service 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Service 被显式导出，存在安全风险。
16	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。
17	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。
18	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: **4** | 警告: **9** | 信息: **3** | 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	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
3	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
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	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
6	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
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	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
9	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
10	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
11	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
12	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

13	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
14	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
15	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
16	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
17	使用弱加密算法	高危	CWE: CWE-327: 使用已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/libavmdl_lite.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/libfcore.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', '__strlen_chk', '__strlcpy_chk', '__strcpy_chk', '__vsnprintf_chk', '__umask_chk']	True info 符号被剥离

3	arm64-v8a/libhiyori.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', '__memcpy_chk']	True info 符号被剥离
4	arm64-v8a/libmaparmor.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/libpanglearmor.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: ['__strlen_chk', '__read_chk', '__vsprintf_chk', '__strcpy_chk']	True info 符号被剥离
6	arm64-v8a/libPglbizssdk_ml.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', '__memmove_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	True info 符号被剥离

7	arm64-v8a/libplt-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
8	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

9	arm64-v8a/libstub.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', '__strlen_chk', '__vsnprintf_chk']	True info 符号被剥离
10	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

11	arm64-v8a/libttmplayer_lite.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
12	arm64-v8a/libtt_ugen_layout.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

13	arm64-v8a/libxfcsud.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', '__vsprintf_chk', '__fgets_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__strchr_chk']	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
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
00024	Base64解码后写入文件	反射 文件	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
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
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
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
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
00191	获取短信收件箱中的消息	短信	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
00189	获取短信内容	短信	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
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、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
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
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
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
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
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
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
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
00056	修改语音音量	控制	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
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
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
00153	通过 HTTP 发送二进制数据	http	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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00177	检查是否授予权限并请求	权限	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
00112	获取日历事件的日期	信息收集 日历	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
00054	从文件安装其他APK	反射	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

00130	获取当前WIFI信息	WiFi 信息收集	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
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

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.REQUEST_INSTALL_PACKAGES android.permission.READ_PHONE_STATE android.permission.CAMERA android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.ACCESS_COARSE_LOCATION android.permission.GET_TASKS android.permission.MODIFY_AUDIO_SETTINGS android.permission.WAKE_LOCK
其它常用权限	11/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_BACKGROUND_LOCATION android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.CHANGE_NETWORK_STATE android.permission.REORDER_TASKS android.permission.FOREGROUND_SERVICE

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
apps.bytesfield.com	安全	是	**IP地址:** 121.228.130.195 **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.lingzhenmm.com	安全	否	**IP地址:** 8.212.69.44 **国家:** 香港 **地区:** 香港,香港 **城市:** 香港 **纬度:** 22.276022 **经度:** 114.1751471 **查看:** Google 地图

px.ucweb.com	安全	是	**IP地址:** 106.8.130.181 **国家:** 中国 **地区:** 河北 **城市:** 石家庄 **纬度:** 38.042307 **经度:** 114.51486 **查看:** 高德地图
game-mj-1252954235.cos.ap-chengdu.myqcloud.com	安全	是	**IP地址:** 183.66.100.19 **国家:** 中国 **地区:** 重庆 **城市:** 重庆 **纬度:** 29.56301 **经度:** 106.551556 **查看:** 高德地图
static.chuangmanke.com	安全	是	**IP地址:** 112.83.241.243 **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
apmplus.volces.com	安全	是	**IP地址:** 180.97.248.210 **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:** 180.97.251.52 **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.chengzijianzhan.com	安全	是	**IP地址:** 121.228.130.195 **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.bytefield-b.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
sf6-ttcdn-tos.pstatp.com	安全	是	**IP地址:** 218.92.226.121 **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.toutiaopage.com	安全	是	**IP地址:** 221.231.47.223 **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.ietf.org	安全	否	**IP地址:** 104.16.45.99 **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
img.chuangmanke.com	安全	是	**IP地址:** 116.130.199.3 **国家:** 中国 **地区:** 中国天津 **城市:** 天津 **纬度:** 39.084158 **经度:** 117.200983 **查看:** 高德地图
www.samsungapps.com	安全	否	**IP地址:** 54.229.93.135 **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

URL 链接安全分析

URL信息	源码文件
• https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj_assets/shake.webp • https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj_assets/swipe_right.webp • https://sf3-fe-tos.pglstatp-toutiao.com/obj/csj-sdk-static/csj_assets/shake_text.png	自研引擎-A
• https://www.samsungapps.com/appquery/appdetail.as?appId=	com/ss/android/downloadlib/st/i.java
• https://api.lingzhenmh.com • http://manhua2023r2.oss-cn-shanghai.aliyuncs.com • http://static.chuangmanke.com • http://img.chuangmanke.com	f/d/a/a.java
• 2.10.42.103	com/bykv/vk/component/ttvideo/port/BuildConfig.java
• 2.10.42.103	com/bykv/vk/component/ttvideo/player/TTVersion.java
• http://47.112.248.236:9998	f/p/g/g/d/a.java
• https://%s/q?host=%s	com/bykv/vk/component/ttvideo/network/DnsHelper.java
• http://127.0.0.1	com/bykv/vk/component/ttvideo/DataLoaderHelper.java

• http://47.112.248.236:9998	e/b/c/l/a.java
• https://api.lingzhenmh.com • http://static.chuangmanke.com • http://img.chuangmanke.com	f/p/c/f/a.java
• https://img1.baidu.com/it/u=1729653691,1351107558&fm=26&fmt=auto&gp=0.jpg	e/a/a/b/d/b.java
• 1.4.6.31	com/bykv/vk/component/ttvideo/VideoLiveManager.java
• https://apps.bytesfield.com • https://apps.bytesfield-b.com	com/ss/android/downloadlib/addownload/compliance/h.java
• www.toutiaopage.com/tetris/page • www.chengzijianzhan.com • https://apps.oceanengine.com/customer/api/app/pkg_info?	com/ss/android/downloadlib/addownload/compliance/c.java
• https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html	com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java
• 1.4.6.31	com/bykv/vk/component/ttvideo/BuildConfig.java
• https://px.ucweb.com/upload	com/nirvana/tools/crash/BuildConfig.java
• 127.0.0.1	f/p/d/c/e.java
• http://127.0.0.1	com/bykv/vk/component/ttvideo/medialoader/MediaLoaderWrapper.java
• 1.1.37.41	com/bykv/vk/component/ttvideo/mediakit/medialoader/BuildConfig.java
• http://175.178.96.110:8080/api/v1/ • http://124.223.0.123:5208 • https://game-mj-1252954235.cos.ap-chengdu.myqcloud.com/	f/p/e/a/d/b.java
• https://apmplus.volces.com/monitor/collector/session • https://apmplus.volces.com/apm/collect/crash	f/i/a/a/g/a.java
• 2.1.1.4	com/byted/live/api/BuildConfig.java
• 1.4.6.31	com/bykv/vk/component/ttvideo/log/LiveLoggerService.java
• http://manhua20230225.oss-cn-shanghai.aliyuncs.com/	f/p/g/b.java
• tcp://%s • 1.1.37.4 • 127.0.0.1	lib/arm64-v8a/libavmdl_lite.so
• https://manhua20230225.oss-cn-shanghai.aliyuncs.com/static/koharu_new.png	lib/arm64-v8a/libhiyori.so
• data:%p,width:%d,height:%d,stride:%d,ret:%d • 2.10.42.103	lib/arm64-v8a/libttmplayer_lite.so
• 127.0.0.1 • 8.8.8.8 • http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01	lib/arm64-v8a/libxfcsud.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
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。
C++ 共享库	Android	在 Android 应用中运行原生代码。
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。
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。
libYUV	Google	libYUV 是 Google 开源的 yuv 图像处理库，实现对各种 yuv 数据之间的转换，包括数据转换，裁剪，缩放，旋转。
极光推送	极光	JPush 是经过考验的大规模 App 推送平台，每天推送消息数超过 5 亿条。 开发者集成 SDK 后，可以通过调用 API 推送消息。同时，JPush 提供可视化的 web 端控制台发送通知，统计分析推送效果。 JPush 全面支持 Android, iOS, Winphone 三大手机平台。
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，为您和用户连接桥梁。
腾讯广告 SDK	Tencent	腾讯广告汇聚腾讯公司全量的应用场景，拥有核心人群数据、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 Media	Google	用于其他应用共享媒体内容和控件。已被 media2 取代。

邮箱地址敏感信息提取

EMAIL	源码文件
this@loadintousefitwidthnormal.getlayou this@loadintousefitwidth.getlayou	f/p/c/z/a1.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
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363
TalkingData	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/293

敏感凭证泄露检测

可能的密钥
"anythink_myoffer_feedback_violation_of_laws" : "Illegal"
TGNvbS9Ib29rL0Zha2VJQmluZGVyOw==
W8UoP2DS4JH8hqmAN9l7FutKeim5BE0zJy28fvYHJuA=
Q2xhc3NOYW1lU3Bvb2Zpbmd8fExhbmRyb2lkL2NvbnRlbnQvQ29udGV4dDs=
QXBrUGF0aFNwb29maW5nfHxMYW5kcm9pZC9jb250ZW50L0NvbnRleHQ7fHxMamF2YS9sYW5nL1N0cmluZzs=
bXx8TGphdmEvbGFuZy9UaHJvd2FibGU7fHxMamF2YS9sYW5nL1Rocm93YWJsZTs=
TGNvbS9Ib29rL0FwcGxpY2F0aW9uTmFtZVNwb29maW5nOw==
8ED210B263B04D8883ED5B4CAB9099B2
SG9va0luaXR8fExhbmRyb2lkL2NvbnRlbnQvQ29udGV4dDs=
TGNvbS9zcnAvcGF0Y2gvSW5pdCQkRXh0ZXJuYWxTeW50aGV0aWNCYWNrcG9ydDA7
36f7412b83104271e447c242a0948b5cb891c7bc
Z2V0SW50fHxMamF2YS9sYW5nL1N0cmluZzs=

免责声明及风险提示: