南明离火
移动应用检测平台

ANDROID 静态分析报告

哔哩哔哩 • v1.6.6

分析日期: 2025-10-12 19:05:18

应用概览

文件名称:	bilibilitv1.6.6-repair-v10.0.apk
文件大小:	7.83MB
应用名称:	哔哩哔哩
软件包名:	com.bilibili.tv
主活动:	com.bilibili.tv.ui.splash.SplashActivity
版本号:	1.6.6
最小SDK:	17
目标SDK:	27
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	12/100 (重大风险)
跟踪器检测:	3/432
杀软检测:	2 个杀毒软件报毒
MD5:	d3f40d77a006be8c16f2a222f90ef5ae
SHA1:	9a757588847649c0cacb1adbbcb29863de5fb4bc
SHA256:	ea8eedf7f255a0faf91ab2fe9582e227f34627b21e28e2e601b8844af32c686d

分析结果严重性分布

高危	中危	信息	安全	关注
44	12	2	1	0

四大组件导出状态统计

Activity组件：82个，其中export的有： 1个
Service组件：10个，其中export的有： 1个
Receiver组件：0个，其中export的有： 0个
Provider组件：8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:
5d802f24d6ac76c708a8e7afe28fd97e038f888cef6665fb9b4a92234c311d6ff42127ccb2eb5a898f4e7e4e553f6e6d2d43d1a2ebae9f002a6598e72fd2d83

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.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.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.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_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.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.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.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.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.ACCESS_ALL_EXTERNAL_STORAGE	未知	未知权限	来自 android 引用的未知权限。
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.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.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。

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: **42** | 警告: **3** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已配置网络安全策略 [android:networkSecurityConfig=@7F0F0003]	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。
2	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。
3	Activity (com.bilibili.tv.ui.bangumi.BangumiDetailActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
4	Activity（com.bilibili.tv.ui.bangumi.BangumiDetailActivity）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。
5	Activity (com.bilibili.tv.player.PlayerActivity) 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（27）升级至 29 及以上，从平台层面修复该漏洞。
6	Activity (com.bilibili.tv.player.PlayerActivity) 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	Service (com.bilibili.tv.service.paper.LiveWallpaperService) 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。
8	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_00) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
9	Activity（com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_00）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。
10	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_01) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
11	Activity（com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_01）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。
12	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_02) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
13	Activity（com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_02）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。
14	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_03) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
15	Activity（com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_03）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。
16	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_04) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。

17	Activity（com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_04）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。
18	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_05) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
19	Activity（com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_05）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。
20	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_06) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
21	Activity（com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_06）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。
22	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_07) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
23	Activity（com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_07）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。
24	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_08) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
25	Activity（com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_08）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。
26	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_09) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
27	Activity（com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_09）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。

本报告由南明离火移动安全分析平台生成

28	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_00_T) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
29	Activity（com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_00_T）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。
30	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_01_T) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
31	Activity（com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_01_T）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。
32	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_02_T) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
33	Activity（com.tencent.tinker.loader.hotplug.ActivityStubs$SGTKStub_02_T）易受 Android Task Hijacking/StrandHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时，恶意应用可将自身置于栈顶，导致任务劫持（StrandHogg 1.0），易被钓鱼攻击。建议将启动模式设为 "singleInstance" 或 taskAffinity 设为空（taskAffinity=""），或将 target SDK 版本（27） 升级至 28 及以上以获得平台级防护。
34	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SIStub_00) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
35	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SIStub_01) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
36	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SIStub_02) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
37	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SIStub_03) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
38	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SIStub_04) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。

39	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SIStub_05) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
40	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SIStub_06) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
41	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SIStub_07) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
42	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SIStub_08) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
43	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SIStub_09) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
44	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SIStub_00_T) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
45	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SIStub_01_T) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
46	Activity (com.tencent.tinker.loader.hotplug.ActivityStubs$SIStub_02_T) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。

代码安全漏洞检测

高危: **2** | 警告: **7** | 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,不得包含敏感信息	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	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

3	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
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	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	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
8	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
9	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

10	使用弱加密算法	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-4	升级会员：解锁高级权限
11	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
12	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

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	armeabi-v7a/libbili.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	armeabi-v7a/libBilicastServer.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	armeabi-v7a/libblog.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	armeabi-v7a/libglrenderer.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	armeabi-v7a/libstatic-webp.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	armeabi-v7a/libvideocache.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

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	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
00189	获取短信内容	短信	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成

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
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
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
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
00104	检查给定路径是否是目录	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
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
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
00171	将网络运算符与字符串进行比较	网络	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
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
00067	查询IMSI号码	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
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
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
00042	查询WiFi BSSID及扫描结果	信息收集 WiFi	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
00116	获取当前WiFi MAC地址并放入JSON中	WiFi 信息收集	升级会员：解锁高级权限

00076	获取当前WiFi信息并放入JSON中	信息收集 WiFi	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
00163	创建新的 Socket 并连接到它	socket	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
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
00012	读取数据并放入缓冲流	文件	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
00043	计算WiFi信号强度	信息收集 WiFi	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
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
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
00191	获取短信收件箱中的消息	短信	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
00147	获取当前位置的时间	信息收集 位置	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	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
00035	查询已安装的包列表	反射	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
00177	检查是否授予权限并请求	权限	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	4/30	android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.WAKE_LOCK android.permission.ACCESS_COARSE_LOCATION
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE

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
api.live.bilibili.com	安全	是	**IP地址:** 61.147.236.103 **国家:** 中国 **地区:** 中国江苏 **城市:** 南通 **纬度:** 31.980172 **经度:** 120.894291 **查看:** 高德地图
bsbsb.top	安全	是	**IP地址:** 115.190.32.254 **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
live.bilibili.com	安全	是	**IP地址:** 114.230.222.173 **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
comment.bilibili.com	安全	是	**IP地址:** 117.21.179.18 **国家:** 中国 **地区:** 江西 **城市:** 南昌市 **纬度:** 28.687547 **经度:** 115.8540042 **查看:** 高德地图
api.snm0516.misee.tv	安全	是	**IP地址:** 114.230.222.172 **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.im9.com	安全	否	No Geolocation information available.
passport.bilibili.com	安全	是	**IP地址:** 61.147.236.102 **国家:** 中国 **地区:** 中国江苏 **城市:** 南通 **纬度:** 31.980172 **经度:** 120.894291 **查看:** 高德地图
api.bilibili.com	安全	是	**IP地址:** 117.21.179.20 **国家:** 中国 **地区:** 江西 **城市:** 南昌市 **纬度:** 28.687547 **经度:** 115.8540042 **查看:** 高德地图
account.bilibili.com	安全	是	**IP地址:** 183.131.147.30 **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
data.bilibili.com	安全	是	**IP地址:** 183.131.155.11 **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
my.tv.sohu.com	安全	是	**IP地址:** 61.151.225.49 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
big.bilibili.com	安全	是	**IP地址:** 117.21.179.20 **国家:** 中国 **地区:** 江西 **城市:** 南昌市 **纬度:** 28.687547 **经度:** 115.8540042 **查看:** 高德地图
app.bilibili.com	安全	是	**IP地址:** 61.147.236.101 **国家:** 中国 **地区:** 中国江苏 **城市:** 南通 **纬度:** 31.980172 **经度:** 120.894291 **查看:** 高德地图

bangumi.bilibili.com	安全	是	**IP地址:** 117.21.179.20 **国家:** 中国 **地区:** 江西 **城市:** 南昌市 **纬度:** 28.687547 **经度:** 115.8540042 **查看:** 高德地图
app.snm0516.aisee.tv	安全	是	**IP地址:** 117.85.70.230 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.0607 **经度:** 118.763 **查看:** 高德地图
vipgift.biligame.com	安全	是	**IP地址:** 111.160.192.99 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.0607 **经度:** 118.763 **查看:** 高德地图
www.bilibili.com	安全	是	**IP地址:** 14.236.222.172 **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
hot.vrs.sohu.com	安全	是	**IP地址:** 101.89.55.28 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• 10.0.0.172 • 10.0.0.200	bl/axo.java
• https://app.bilibili.com	bl/kh.java
• 127.0.0.1	bl/wy.java
• http://www.bilibili.com/video/av	bl/aft.java
• http://119.29.29.29/d?dn=	bl/acy.java
• https://api.live.bilibili.com/xlive/web-room/v2/index/getroomplayinfo	mybl/BiliLiveContent.java
• http://bangumi.bilibili.com/anime/	bl/xt.java

本报告由南明离火移动安全分析平台生成

• http://api.bilibili.com/x/v1/dm/list.so • http://comment.bilibili.com • http://api.bilibili.com/x/v2/dm/list.so	bl/ym.java
• https://api.bilibili.com/pgc/player/web/playurl	bl/qh.java
• http://116.62.182.15/http_dns	bl/acq.java
• https://api.bilibili.com/x/resource/ip	bl/afm2.java
• https://account.bilibili.com	bl/me.java
• https://bangumi.bilibili.com	bl/kg.java
• https://api.live.bilibili.com	bl/aeh.java
• https://passport.bilibili.com	com/bilibili/lib/passport/BiliAuthService.java
• https://app.bilibili.com	bl/jt.java
• https://app.bilibili.com	com/bilibili/lib/mod/ModApiService.java
• https://bangumi.bilibili.com	com/bilibili/bangumi/api/BangumiApiService.java
• www.im9.com	bl/acn.java
• http://api.bilibili.com/x/click-interface/click/now	bl/acf.java
• http://api.bilibili.com	com/bilibili/tv/player/report/HeartbeatApiService.java
• http://api.bilibili.com	com/bilibili/tv/api/favorite/BiliFavoriteVideoApiService.java
• http://api.bilibili.com	com/bilibili/tv/api/history/BiliPlayerHistoryService.java
• https://api.bilibili.com/pgc/view/web/ep/list • https://api.bilibili.com/x/player/wbi/v2 • https://bsbsb.top/api/skipsegments	com/bilibili/tv/player/basic/context/ResolveResourceParams.java
• http://data.bilibili.com/gv/	bl/aad.java
• 119.29.29.29	bl/acx.java
• http://pingma.qq.com:80/mstat/report	bl/awr.java
• 10.0.0.200	bl/avm.java
• http://api.bilibili.com	bl/zl.java
• https://app.bilibili.com/x/v2/view/like/triple • https://app.bilibili.com/x/v2/view/like • https://app.bilibili.com/x/v2/view/coin/add • https://api.bilibili.com/	mybl/MyBiliApiService.java

• https://github.com/tootallnate/java-websocket/wiki/lost-connection-detection	org/java_websocket/AbstractWebSocket.java
• https://app.bilibili.com/x/v2/view/vip/playurl	bl/qp.java
• https://api.live.bilibili.com/xlive/web-room/v1/index/getdanmuinfo	mybl/DanmakuClient.java
• 203.107.1.34 • 203.107.1.33 • 203.107.1.66 • 203.107.1.65	bl/no.java
• http://api.snm0516.aisee.tv	com/bilibili/tv/api/TvApiService.java
• https://api.bilibili.com/pugv/player/web/playurl	bl/ql2.java
• http://bangumi.bilibili.com/anime/	com/bilibili/tv/ui/bangumi/BangumiDetailActivity.java
• http://app.bilibili.com	bl/kd.java
• https://big.bilibili.com/mobile/publicpay?appid=61&app_sub_id=&panel_type=normal	com/bilibili/tv/ui/vip/VipActivity.java
• http://app.bilibili.com	com/bilibili/tv/api/BiliApiService.java
• http://api.bilibili.com • http://api.bilibili.com/x/v2/dm/post	com/bilibili/tv/api/danmaku/BiliApiDanmakuSender.java
• http://api.bilibili.com	bl/ke.java
• https://api.bilibili.com/x/player/playurl	bl/ql.java
• http://bangumi.bilibili.com/anime/	com/bilibili/tv/ui/bangumi/BangumiEpisodeFragment.java
• http://api.bilibili.com	com/bilibili/tv/api/search/BiliSearchApi.java
• http://www.bilibili.com • http://vipgift.biligame.com	bl/mi.java
• 127.0.0.1	bl/aya.java
• http://live.bilibili.com/api/playurl	bl/qj.java
• https://app.bilibili.com	com/bilibili/tv/api/video/VideoApiService.java
• https://api.bilibili.com/x/web-interface/view/detail	com/bilibili/tv/api/video/BiliVideoDetail.java
• http://app.bilibili.com	com/bilibili/tv/api/rank/RankApiService.java
• http://api.bilibili.com	com/bilibili/tv/api/search/BiliSearchSuggestApi.java
• https://passport.bilibili.com/api/captcha?token=	com/bilibili/tv/ui/account/LoginActivity.java

• http://app.bilibili.com	com/bilibili/tv/api/auth/BiliSpaceApiService.java
• http://www.bilibili.com/video/av	com/bilibili/tv/ui/video/VideoDetailActivity.java
• http://data.bilibili.com/log/mobile?android • https://data.bilibili.com/log/mobile?android	bl/ox.java
• https://data.bilibili.com/vv/app • http://data.bilibili.com/vv/app	bl/ou.java
• http://app.snm0516.aisee.tv/x/v2/param	bl/nc.java
• http://app.bilibili.com	com/bilibili/tv/api/area/RegionService.java
• 10.0.0.172	u/a/v/al.java
• http://my.tv.sohu.com/play/videonew.do?vid=%1$s_%2$s&plid=%3$s • http://hot.vrs.sohu.com/vrs_flash.action?vid=%1$s&ver=%2$s&ref=0001 • http://%1$s%2$s/%3$s?key=%4$s&idc=%5$s&n=1 • http://%1$s/p2p?new=%2$s&num=%3$s&key=%4$s	自研引擎-S
• 233.233.233.233	lib/armeabi-v7a/libBilicastServer.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Fresco	Facebook	Fresco是一个用于管理图像及其使用的内存的 Android 库。
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。
GIFLIB	GIFLIB	The GIFLIB project maintains the giflib service library, which has been pulling images out of GIFs since 1989. It is deployed everywhere you can think of and some places you probably can't - graphics applications and web browsers on multiple operating systems, game consoles, smartphones, and likely your ATM too.
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。
烈焰弹幕使	Bilibili	烈焰弹幕使是 Android 上开源的弹幕解析绘制引擎项目。
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。
Xpref	Bilibili	一个 SharedPreferences 的包装器，真正支持跨多进程共享数据。
Tinker	Tencent	Tinker 是适用于 Android 的热更新程序库，它支持无需重新安装 apk 来更新 dex，库和资源。

邮箱地址敏感信息提取

EMAIL	源码文件

bbcallen@gmail.com	bl/aad.java
ctwap@mycdma.cn	bl/avm.java
bbcallen@gmail.com	com/bilibili/tv/MainApplication.java

第三方追踪器检测

名称	类别	网址
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
友盟统计的=> "UMENG_APPKEY" : "53d2412e56240b8a6500dd63"
凭证信息=> "FAWKES_APP_KEY" : "android"
"sohu_api_url_2" : "http://my.tv.sohu.com/play/videonew.do?vid=%1$s_%2$s&plid=%3$s"
"sohu_api_url_segment" : "http://%1$s%2$s/%3$s?key=%4$s&idc=%5$s&n=1"
"sohu_api_url_p2purl" : "http://%1$s/p2p?new=%2$s&num=%3$s&key=%4$s"
"pref_key_choose_danmaku_engine" : "ChooseDanmakuEngine"
"sohu_api_url_1" : "http://hot.vrs.sohu.com/vrs_flash.action?vid=%1$s&ver=%2$s&ref=0001"
6X8Y4XdM2Vhvn0KfzcEatGnWaNU=
4kU71lN96TJUomD1vOU9lgj9U+kkmxDPLVM+zzjst5U=
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
03a976511e2bbe3a7f26808fb7af3c05
d16ffded[illegible]a5319d4ba3b2f9e70561f0

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。