

■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

17 最小SDK:

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

2个杀毒软件报毒 杀软检测:

MD5: d3f40d77a006be8c16f2a

9a757588847649c0cach1 dbbcb29863de5fb4b SHA1:

SHA256: 28e2e601b8844af32c686d

♣ 高危	*//	中危	┇信息	✔ 安全	《 关注
44	XX	12	2		

其中export的有: 1个 Service组件

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:

5d802f24d6ac76c708a8e7afe28fd97e038f888cef6665fb9b4a92234c311d6ff42127ccb2eb5a898f4e7e4e553f6g.to.2d43d1a2ebae9f002a6598e72fd2d83

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_ST ATE	危险	允许接收WLAN多 播	允公克用程序接收并非直接向您的设备发送的数据包。这样 在查扎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	FALSO	完全互联网次和	允许应用程序创建网络套接字。
android.permission.ACCESS_NETWORK_STATE	普通	艾 敢网络》》态	允许应用程序查看所有网络的状态。
android.permission.READ_PHONE_STATE	危险	10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.ACSESS.WIR_STATE		查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
android.permiss to J. RLUE JOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.rk; mission.WRITE_EXTERNAL STOLAGE	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_IN_TAlt_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.per hissien.ACCESS_ALL_EXTERNAL_STOR AGE	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	

Ⅲ 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	- 1/1/	V. 675
己签名应用	信息	应用已使用代码签名证书进行签名。		17

Q Manifest 配置安全分析

高危: 42 | 警告: 3 | 信息: 0 | 屏蔽: 0

问题	严重程度	排述信息
应用已配置网络安全策略 [android:networkSecurityC onfig=@7F0F0003]	信息	网络安全配置: 沙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。可针对特定域名式应用范围进行灵活配置。
应用数据允许备份 [android:allowBackup=true]	HA PA	这点态允许通过 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。
Activity (com.bilibili.tv.u bangumi.BangumiDotaily ctiv. ty) 的启动模式非 taynay u	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。
Activity(to noil)illi.tv.ui.b ang uni Bang miDetailActi vit),Android Task Hij acking/StrandHogg 攻击		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。
Activity (com.biliblictv. lay r.PlayerActivity) 景型 Strand Hogg 2.0 域域	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。
Activity (vom.bilibili.tv.playe r.Pla er Altivity) 未受保护。 [andro.d:exported=true]	警告	检测到 Activity 己导出,未受任何权限保护,任意应用均可访问。
	应用已配置网络安全策略 [android:networkSecurityConfig=@7F0F0003] 应用数据允许备份 [android:allowBackup=true] Activity (com.bilibili.tv.u bangumi.BangumiDetailactivty) 的启动模式非气力。可以由于10个元的是10个元	应用已配置网络安全策略 [android:networkSecurityConfig=@7F0F0003] 应用数据允许备份 [android:allowBackup=true] Activity (com.bilibili.tv.u.bangumi.BangumiDotaib.ctiv.ty) 的启动模式非长tandaru Activity (torp.oil.bili.tv.ui.bangumi.Bang.miDetailActivit.vi.changumi.Bang.miDetailActivit.vi.chang.chandroid Task Hijacking/StrandHogg 攻击 Activity (com.bilibili.tv. la)vr.PlayerActivity) 引受 StrandHogg 2.0 攻抗 Activity (com.bilibili.tv.player.rla eNaltivity)未受保护。 警告

Service (com billiolit Auservi ce paper Live Managere vice 文文 限代				
Bader hotpug Activity Stuber	7	ce.paper.LiveWallpaperSer vice) 受权限保护,但应检查 权限保护级别。 Permission: android.permi ssion.BIND_WALLPAPER	警告	保护级别。若为 normal 或 dangerous,恶意应用可申请并与组件交互;若为 s
T.Loader-hotplugActiviyStu bsSSGTKStub_00	8	.loader.hotplug.ActivityStub s\$SGTKStub_00) 的启动模式	高危	vity,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
Joader.hotplug.ActivityStub standard	9	r.loader.hotplug.ActivityStu bs\$SGTKStub_00)易受 And roid Task Hijacking/Strand	高危	持(StrandHogg 1.0),易被钓鱼攻击。建议带富动模式设为 "singleInstance" 或 taskAffinity 设为空(taskAffinity=""),或类 ta sget SDK 版本(27) 升级
### Activity com.tencent.tinker loader.hotplug.ActivityStub sSSGTKStub_02) 的原动模式	10	.loader.hotplug.ActivityStub s\$SGTKStub_01) 的启动模式	高危	vity,导致其他应用可读取调片 'ni ent 内容。涉及敏感信息试应使用 "standard
12 I.loader.hotplug.ActivityStub s\$GTKStub_02) 的启动模式 非 standard Activity (com.tencent.tinke r.loader.hotplug.ActivityStub bs\$SGTKStub_02) 易受 And roid Task Hijacking/Strand Hogg 攻击 Activity (com.tencent.tinke r.loader.hotplug.ActivityStub s\$SGTKStub_02) 易受 And roid Task Hijacking/Strand Hogg 攻击 Activity (com.tence at Fake I.loader.hotplug.ActivityStub s\$SGTKStub_02) 易受 And roid Task Hijacking/Strand Hogg 攻击 Activity (com.tence at Fake I.loader.hotplug.ActivityStub s\$SGTKStub_02) 易受 And roid Task Hijacking/Strand Hogg 攻击 Activity (com.tence at Fake I.loader.hotplug.ActivityStub s\$SGTKStub_02) 易受 And roid Task Hijacking/Strand Hogg 攻击 Activity 启动模式。 Activity 自动模式。 Activity 自动模式。 Activity 自动模式。 Activity 自动模式。 Activity 自动模式。 Activity 自动模	11	r.loader.hotplug.ActivityStu bs\$SGTKStub_01)易受 And roid Task Hijacking/Strand	高危	持(Strand Hogg 1.0),易被钓鱼攻反。建议将启动模式设为 "singleInstance" 或 taskA in t,设为空(taskAffinity=""、. 或将 target SDK 版本(27)升级
13	12	.loader.hotplug.ActivityStub s\$SGTKStub_02) 的启动模式	高危	vity,导致其他应用可读耳调用 Intent 内容。涉及敏感信息时应使用 "standard
Activity 后动模式设置为 "single lask" 或 "single l	13	r.loader.hotplug.ActivityStu bs\$SGTKStub_02)易受 And roid Task Hijacking/Strand	A Pr	序(StranuHogg 1.0),易被钓鱼攻击。建议将启动模式设为 "singleInstance" 文字 kAffinity 设为空(taskAffinity=""),或将 target SDK 版本(27)升级
Activity 启动模式为 "single lask" 时,恶意应用可将自身置于核项,导致任务切持(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。 Activity (1 on ten cent.tinker load a hort ug ActivityStub st SCU s) ub 04) 的启动模式 高危 Activity 启动模式。 Activity 启动模式设置为 "single lask" 时,恶意应用可将自身置于核项,导致任务切持(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。 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" 自动模式	14	.loader.hotplug./ ct/vitystub s\$SGTKStu 07 的产动模式	高危	vity,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
Activity 启动模式 设直为 "single lask" 或 "single las	15	r.loadyr.hotplug.ActivityStu pspSGTKStub_03)易变 //nc roid Task Hijacking/Stsan	斯危	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
	16	.load_x.hotp ug.ActivityStub s*\$(、T/s ub_04) 的启动模式	高危	vity,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

17	Activity(com.tencent.tinke r.loader.hotplug.ActivityStu bs\$SGTKStub_04)易受 And roid Task Hijacking/Strand Hogg 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.ActivityStub s\$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.tinke r.loader.hotplug.ActivityStu bs\$SGTKStub_05)易受 And roid Task Hijacking/Strand Hogg 攻击。	高危	Activity 启动模式为 "singleTask" 时,恶意应用可将自身置了代订,导致任务劫持(StrandHogg 1.0),易被钓鱼攻击。建议将启奏模式设为 "singleInstance"或 taskAffinity 设为空(taskAffinity=""),或将 t (
20	Activity (com.tencent.tinker .loader.hotplug.ActivityStub s\$SGTKStub_06) 的启动模式 非 standard	高危	Activity 启动模式设置为 "singleTask" 这 singleInstance" 时,可能成为根 Activity,导致其他应用可读取调用 Intent 内容。涉及敏感信息时必使用 "standard " 启动模式。
21	Activity(com.tencent.tinke r.loader.hotplug.ActivityStu bs\$SGTKStub_06)易受 And roid Task Hijacking/Strand Hogg 攻击。	高危	Activity 启动模式为 "single lask" 时,恶意应用可将自身置于栈顶,导致任务劫持(StrandHdgg、0),易被钓鱼攻击。建义将产动模式设为 "singleInstance"或 taskAffinity 设 空(taskAffinity=""),近将 target SDK 版本(27)升级至 28 景久为以获得平台级防护。
22	Activity (com.tencent.tinker .loader.hotplug.ActivityStub s\$SGTKStub_07) 的启动模式 非 standard	高危	Activity 启动模式设置为 "sip, let ask" 或 "singleInstance" 时,可能成为根 Acti vity,导致其他应用可读平调用 Intent 内容。涉及敏感信息时应使用 "standard " 启动模式。
23	Activity(com.tencent.tinke r.loader.hotplug.ActivityStu bs\$SGTKStub_07)易受 And roid Task Hijacking/Strand Hogg 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(StrangHogg 1.0),易被钓鱼攻击。建议将启动模式设为 "singleInstance"或 task/If it ty 设为空(taskAffinity=""),或将 target SDK 版本(27)升级 至 18 及以上以获得平台级防护。
24	Activity (com.tencent.ti ne_r .loader.hotplug.Activity为tur s\$SGTKStub_08) 的 召录模式 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(torp:tencent.tinke r.lo der/hotp.ug.ActivityStu b\$.\$6 ¹ k.tub_08)易受 And roid lask Hijacking/Strat a Hogg 攻击。		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.tenzenztin er .loader.hotplag.ActivityStub s\$SGTKS (20.09),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	Acti ty com.tencent.tinke r loader.hotplug.ActivityStu \$\$SGTKStub_09)易受 And roid Task Hijacking/Strand Hogg 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。

28	Activity (com.tencent.tinker .loader.hotplug.ActivityStub s\$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.tinke r.loader.hotplug.ActivityStu bs\$SGTKStub_00_T)易受 A ndroid Task Hijacking/Stran dHogg 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.ActivityStub s\$SGTKStub_01_T) 的启动模 式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 場,可能成为根 Activity,导致其他应用可读取调用 Intent 内容。涉及象域信息时立使用 "standard" 启动模式。
31	Activity(com.tencent.tinke r.loader.hotplug.ActivityStu bs\$SGTKStub_01_T)易受 A ndroid Task Hijacking/Stran dHogg 攻击。	高危	Activity 启动模式为 "singleTask" 时,总意应从可将自身置于栈顶,导致任务劫持(StrandHogg 1.0),易被钓鱼(对,建议将启动模式设为 "singleInstance"或 taskAffinity 设为空(taskAffinity= ") 》 或将 target SDK 以本(27)升级至 28 及以上以获得平台级陈地。
32	Activity (com.tencent.tinker .loader.hotplug.ActivityStub s\$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,导致其他应引可读取调用 Intent 内容
33	Activity(com.tencent.tinke r.loader.hotplug.ActivityStu bs\$SGTKStub_02_T)易受 A ndroid Task Hijacking/Stran dHogg 攻击。	高危	Activity 启力模式为 "singleTask" 寸,恶意应用可将自身置于栈顶,导致任务劫势(Str) ndHogg 1.0),易,约是攻击。建议将启动模式设为 "singleInstance" 或 (askAffinity 设为空(tokAffinity="") ,或将 target SDK 版本(27)升级至 28 及以上以获得平台及队护。
34	Activity (com.tencent.tinker .loader.hotplug.ActivityStub s\$SIStub_00) 的启动模式非 s tandard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时,可能成为根 Activity,另创为他应用可读取调用 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.Activityst rd s\$SIStub_01) 的启动模式 课年 tandard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时,可能成为根 Acti vity,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 (contrencent tinker loader hotolog ActivityStub s\$S tun 02) 对启动模式非 stallfan		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.ActivityStub s\$SIStub_03) 的岸场地式	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 (controncent.tinker .lease thotplug.ActivityStub s\$\$) tub 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。
	×	ı	

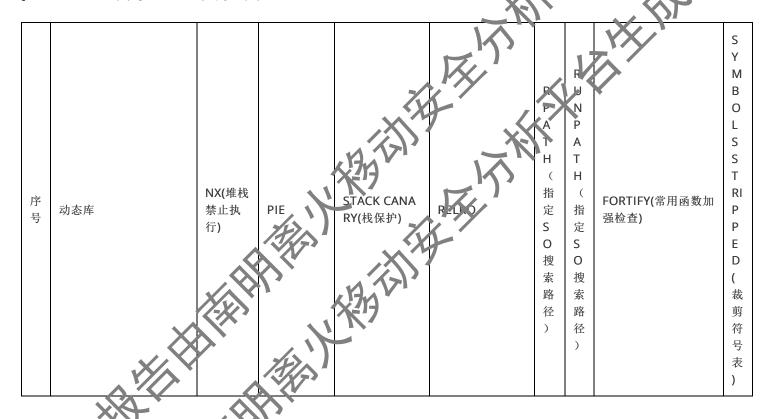
39	Activity (com.tencent.tinker .loader.hotplug.ActivityStub s\$SIStub_05) 的启动模式非 s tandard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时,可能成为根 Activity,导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
40	Activity (com.tencent.tinker .loader.hotplug.ActivityStub s\$SIStub_06) 的启动模式非 s tandard	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.ActivityStub s\$SIStub_07) 的启动模式非 s tandard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" b、 丁能成为根 Activity,导致其他应用可读取调用 Intent 内容。涉及敏感信息"仍定使用 "standard" 启动模式。
42	Activity (com.tencent.tinker .loader.hotplug.ActivityStub s\$SIStub_08) 的启动模式非 s tandard	高危	Activity 启动模式设置为 "singleTask" 或 "single instance" 时,可能成为根 Activity,导致其他应用可读取调用 Intent
43	Activity (com.tencent.tinker .loader.hotplug.ActivityStub s\$SIStub_09) 的启动模式非 s tandard	高危	Activity 启动模式设置为 "sing s Task" 或 "singleInstance" 脉,可能成为根 Activity,导致其他应用可读取调用 Intent 内容。涉及恢复危息时应使用 "standard" 启动模式。
44	Activity (com.tencent.tinker .loader.hotplug.ActivityStub s\$SIStub_00_T) 的启动模式 非 standard	高危	Activity 后动模式凌置为 "singleTask" 或 "singleInstance" 时,可能成为根 Activity,导《其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" "本效模式
45	Activity (com.tencent.tinker .loader.hotplug.ActivityStub s\$SIStub_01_T) 的启动模式 非 standard	高危	Activity 启动模式设置步 (si) gleTask" 或 "singleInstance" 时,可能成为根 Activity,导致其他应用可读耳调用 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.ActivityStub s\$SIStub_02_T) 的启动模式 非 standard	in de	Activity 唐夕模式设置为 "singleTask" 或 "singleInstance" 时,可能成为根 Acti wig 是致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard 方,模式。

序号	问题	等级	参考标准	文件位置
1	文用程序记录日志信息,不导。文極 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	应用是序使用SQLite数据库并执行 原外的企业海。原始SQL查询中不受 信任心用》输入可能会导致SQL注入 、到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: Cl ient Code Quality	升级会员:解锁高级权限

114 /11-1/1/	文全分析平台 技不分析报告	MDO: GOI	40d77a00bbe8c1bf2a	
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: In sufficient Cryptograp hy 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: In secure Data Storage OWASP MASVS: MSTG -STORAGE-2	升级会员:解锁高级校园
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: R everse Engineering OWASP MASVS: MSTG -STORAGE-14	力·級会员 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: CWF-64.9: 这較 于混淆或加密空色相关 输入间不进行完整性检 查 OWASP Top 10: M5: In cufficient Cryptograp hy OWASP MASVS: MTTG -CRYPTO-3	工业会员 解锁高级权限
8	SHA-1是已知存在吃煮冰少的弱哈希	警告	CWF: [WE-877] 使用 了破损 (本认为是不安 全化 可密 拿法 OWASP Top 10: M5: In sufficient Cryptograp hy OWASP MASVS: MSTG -CRYPTO-4	升级会员:解锁高级权限
9	<u>应用程序使用不安全的被机械生成</u> 器	警告	CWE: CWE-330: 使用 不充分的随机数 OWASP Top 10: M5: In sufficient Cryptograp hy 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: In sufficient Cryptograp hy 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



<u>南明</u>	离火安全分析平台 技术	分析报告	MD5: d3f40	0d77a006be8c16	f2a222f90ef5ae				
1	armeabi-v7a/libbili.so	True info 二件NX 标存可使者的工作的工作的工作的工作的工作的工作的工作的工作的工作的工作的工作的工作的工作的	动象 (DSO) info 共用构态地代得的编型可 态。 (DSO) info 李 - FPIC,用类这级 可 一种的启址码面编型 可 一种的启址码面编型 可 一种的,用类这级 (RO P) 难行。	True info 这个二进制文件在栈记进制文件在栈已进制了一人上哨会被的栈这回地置近前完全地上,当时,这一个大大小人,这一个一个,这一个一个,这一个一个,这一个一个,这一个一个,这一个一个,这一个一个	Full RELRO info 此共享对象已完全启用 RELRO。REL RO 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 (.g ot 和 .got.plt 两者)被标记为只读。	No ne info 二进制文件没有设置运行时搜索或径式RP TH	Noneinfo二进制文件没有设置FUAPAH	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,get s等)的缓冲区溢出检查。使用编译选项 -D_FOR TIFY_SOURCE=2 来加固 函数。这个检查对于 Da rt/Flutter 准%适用	Trueinfo符号被剥离
2	armeabi-v7a/libBilicastSer ver.so	True info 二件XX 向不可使者的量量。 这内不可使者的是不可能的。 在一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	动象(DSO) info 共用fo 共一fPIC,用关这多位,用关这多位,用关这多位,用关这多位,用关这多位。 有的使用,用关这多位。 有的使用。 有的使用。 有的使用。	True info 这个人,这个人,这个人,这个人,这个人,这个人,这个人,这个人,这个人,这一个人,这一	EnlikeUNO info 此共享对象已完全 启用 RELRO。 REURO 确保 GOT 不不在易受攻而的。ELI 二进制文件中被覆盖。在完整 HELRO中, 多个 GOT (.g ot 和 .got.plt 两者) 被标记为只读。	No Number of Number of No. No. Number of Numb	None in fo 二进制文件没有设置 R U N P A H	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,get s等)的缓冲区溢出检查。使用编译选项 -D_FOR TIFY_SOURCE=2 来加固 函数。这个检查对于 Da rt/Flutter 库不适用	Tr u e in fo 符号被剥离

南明	离火安全分析平台 技术	分析报告	MD5: d3f40	d77a006be8c16	f2a222f90ef5ae				
3	armeabi-v7a/libblog.so	True info 二件 NX 这内不,击的 C 产 人名 中	动象 (DSO) info 共用构标地代得的第二年的原是标。向程本址码面编攻靠 使表。向程本地地码面编攻靠 的,用关这返(RO P)难行。	True info 这个二进制文件在栈上添加工作人上添加工,以便它也地看到这种区覆,也是这个一个人。这个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一	Full RELRO info 此共享对象已完全 启用 RELRO。REL RO 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(.g ot 和 .got.plt 两者)被标记为只读。	No e info 二进制文件没有设置运行时搜索改役式RP TH	None in fo 二进制文件没有设置 R-J Z P AT H	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,get s等)的缓冲区溢出检查。使用编译选项 -D_FOR TIFY_SOURCE=2 来加固 函数。这个检查对于 Da rt/Flutter 库水适用	Tr u e in fo 符号被剥离
4	armeabi-v7a/libglrendere r.so	True info 二件NX 标存可使者的型位态。 有面行攻入后的数据,由于True 的。可能 的。可能 的。可能 的。可能 的。可能 的。可能 的。可能 的。可能	动象 (DSO) info 共用有标地代得的是标言,用是这多数,是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	True info 这件人工法院,了一个作品,是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	Full ReLico Info 此共享对象已完全 启用 RELRO。 RE RO 确保 GOT 不 在易受攻血的 ELI 二进制文件中級覆 盖。在完整 HELRO 中,每个 GOT (.g ot 和.got.plt 两者)被标记为只读。	No Di进制文件没有设置运行时搜索路径或 R AT H	Z o n e in fo 二进制文件没有设置 R U N P A H	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,get s等)的缓冲区溢出检查。使用编译选项 -D_FOR TIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	Tr u e in fo符号被剥离
	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX								

5	armeabi-v7a/libstatic-web p.so	True info 二件NX 标存可使者的 shellc ode 不,击的 shellc ode 不。	动象 (DSO) info 共用构态地代得的编文章 字-fPIC,用关这返(击地 传表这多(RO)的使用,用关这多(由于的,用关的,可能够够多。 P)对。	True info 这个二进制文件在技术是证明的一个工程,在技术是一个人们的一个人们的一个人们的一个人们的一个人们的一个人,这一个一个人,这一个一个人,这一个一个人,这一个一个人,这一个一个人,这一个一个人,就是一个一个人,就是一个一个一个一个一个人,就是一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	Full RELRO info 此共享对象已完全 启用 RELRO。 REL RO 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 (.g ot 和 .got.plt 两者) 被标记为只读。	No ne in o 二进制文件没有设置运行时搜索政役或RATH	Noneinfo二进制文件没有设置FJZPAH	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,get s等)的缓冲区溢出检查。使用编译选项 -D_FOR TIFY_SOURCE=2 来加固 函数。这个检查对于 Da rt/Flutter 库产适用	Tr u e in fo 符号被剥离
6	armeabi-v7a/libvideocach e.so	True info 二件设制置。 一件设位志页执得正确的不可使者的。 一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个	动象 (DSO) info 共 - fPIC ,用关这返 是 标该与的使型 ,用关这返 对 。	True info 这个人,从 个人 人,	F.M.Rel、O Info 此共享对象已完全 启用 RELRO。 RL RO 确保 GOT 不 在易受攻击的 ELF 二进制文件中發覆 盖。在完整 FELRO 中,整个GOT (.g ot 和 .got.plt 两者) 被标记为只读。	No. D.	None in fo 二进制文件没有设置 R U N P A H	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,get s等)的缓冲区溢出检查。使用编译选项 -D_FOR TIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	Trueinfo符号被剥离

♣ 应用行为分析

编号	(1)	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

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:解锁高级区限
00125	检查给定的文件路径是否存在	文件	升级全员: 解愈高级权限
00104	检查给定路径是否是目录	文件	升多 元 解锁高级权限
00063	隐式意图(查看网页、拨打电话等)	控制	升及会员: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	信息収集 电 5服务	<u>升级。负</u> 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 信息本集	升级会员:解锁高级权限
00117	获取 IMSI 和网络运营商名称	电位形务 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 目录疾取资源文件	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	YE接到 URL 并接收来自服务等等输入流	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 VivisSSD 及扫描结果	信息收集 WiFi	升级会员:解锁高级权限
00033	Fin MEI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:解锁高级和水
00091	从广播中检索数据	信息收集	升级会员, 解蒙高级权限
00043	计算WiFi信号强度	信息收集 WiFi	升之合同: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:解锁高级大限
00094	连接到 URL 并从中读取数据	új Z Nje	升级会员: 幹家高级权限
00108	从给定的 URL 读取输入流	网名 命令	升级 大九: 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	W.N.	升级会员:解锁高级权限
00054	从文件安装其他APK	及射	升级会员:解锁高级权限
00147	获取当前位置的时间 - 1/2	信息收集	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	求议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	查询己安装的包列表 - //	反射	升级会员:解锁高级权限
00112	获取日历事件的凸架	信息收集日历	升级会员:解锁高级权限
00177	检查是各种 权限并请求	权限	升级会员:解锁高级权限

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

Q 恶意域名威胁检测

	android.permission.WRITE_EXTERNAL_STORA android.permission.READ_EXTERNAL_STORA						
其它常用权限: 已知恶	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。						
域名		状态中	中国境內				
api.live.bilibili.com	X		IP地址: 61.147 236.193 国家: 中国地区: 中国北苏地区: 中国北苏地面 廖通 第31.980172 李寶: 120.894291				
bsbsb.top		安全	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	WALL TO SERVICE OF THE PARTY OF	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. ilibili.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.snm0510.qisee.t	v	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.基地図
account.bilibili.com	安全	是 人	IP此北: 183.131.147.30 国家: 中国 地区: 浙江 城市: 杭州 纬度: 30.274085 经度: 120.45507 查看: 高 鄭地區
data.bilibili.com	安全	E.	P. C. 183.131.155.11 国家: ◆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	至	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	P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	E.	IP地址: 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	3	E.	P地址: 14 23 222.172 国宗: 中国 地區: 中国江苏 坊店: 南京 纬度: 32.060255 全度: 118.796877 查看: 高德地图
hot.vrs.sohu.com	X	是	P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: 高徳地图

● URL 链接安全¥

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.bi/boli.com/v/deo/av	bl/aft.java
• http://119:2973.23/d?dn=	bl/acy.java
https://ap.n.we.bilibili.com/xlive/web-room/v2/index/getroomplayinfo	mybl/BiliLiveContent.java
http://bangumi.bilibili.com/anime/	bl/xt.java

 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	co'n (bilibh:///o/passport/BiliAuthService.j ava
https://app.bilibili.com	hl/jt.java
https://app.bilibili.com	com/bilibili/lib/mac//ModApiService.java
https://bangumi.bilibili.com	com/bil bi//b. ngumi/api/BangumiApiSer vice:java
• www.im9.com	bl/acha.java
http://api.bilibili.com/x/click-interface/click/now	bl/acf.java
• http://api.bilibili.com	com/bilibili/tv/player/report/HeartbeatA piService.java
http://api.bilibili.com	com/bilibili/tv/api/favorite/BiliFavoriteVid eoApiService.java
• http://api.bilibili.com	com/bilibili/tv/api/history/BiliPlayerHisto ryService.java
https://api.bilibili.com/pgc/view/weis/zy/list https://api.bilibili.com/x/pla_er/v.bi/v2 https://bsbsb.top/api/skipsegments	com/bilibili/tv/player/basic/context/Resol veResourceParams.java
http://data.bilibili.com/gv/	bl/aad.java
• 119.29.29.29	bl/acx.java
• http://pingra.qq.com:80/mstat/report	bl/awr.java
• 10.0.0.200	bl/avm.java
http://api.bilibili.com	bl/zl.java
https://app.wii.vii.com/x/v2/view/like/triple https://app.bi/ibili.com/x/v2/view/like https://app.bi/ibili.com/x/v2/view/coin/add https://app.bi/ibili.com/	mybl/MyBiliApiService.java

https://github.com/tootallnate/java-websocket/wiki/lost-connection-detection	org/java_websocket/AbstractWebSocket.j ava
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//īvApiService.java
https://api.bilibili.com/pugv/player/web/playurl	bl/ql2.java
http://bangumi.bilibili.com/anime/	com/bilib.i/t-//ui/bangumi/BangumiDetai Activicy.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/u.vir/VipActivity.java
• http://app.bilibili.com	com/bil bil /t /api/BiliApiService.java
 http://api.bilibili.com http://api.bilibili.com/x/v2/dm/post 	.com.biribilirtv/api/danmaku/BiliApiDanm aki/sonder.java
http://api.bilibili.com	bi//ke.java
https://api.bilibili.com/x/player/playurl	bl/ql.java
http://bangumi.bilibili.com/anime/	com/bilibili/tv/ui/bangumi/BangumiEpiso deFragment.java
• http://api.bilibili.com	com/bilibili/tv/api/search/BiliSearchApi.ja va
http://www.bilibili.comhttp://vipgift.biligame.com	bl/mi.java
• 127.0.0.1	bl/aya.java
http://live.bilibili.com/api/mayurl	bl/qj.java
• https://app.bij.foili.com	com/bilibili/tv/api/video/VideoApiService. java
https://api.bilibili.com/x/web-tinte-face/view/detail	com/bilibili/tv/api/video/BiliVideoDetail.j ava
• http://app.bilibili.com	com/bilibili/tv/api/rank/RankApiService.j ava
• http://arx.bilibili.com	com/bilibili/tv/api/search/BiliSearchSugg estApi.java
https://passport.bilibili.com/api/captcha?token=	com/bilibili/tv/ui/account/LoginActivity.ja va

• http://app.bilibili.com	com/bilibili/tv/api/auth/BiliSpaceApiServi ce.java
http://www.bilibili.com/video/av	com/bilibili/tv/ui/video/VideoDetailActivit y.java
 http://data.bilibili.com/log/mobile?android https://data.bilibili.com/log/mobile?android 	bl/ox.java
https://data.bilibili.com/vv/apphttp://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/a/ea/RegionService.jav a
• 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#=%3\$s&key=%4\$s 	自研引擎-S
• 233.233.233	lib/arm.abv7a/libBilicastServer.so

\$ 第三方 SDK 组件分析

SDK名称	开发者	描述信息 人名
Fresco	<u>Facebook</u>	Fresco 是一个用于管理图像及其使更为内存的 Android 库。
Bugly	Tencent	度,Rugly,为移动开发老摄伏卡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,同时全程产品运营动态,及时限进用户反馈。
GIFLIB	GIFUE -	The GIFLIB project in a mains the giflib service library, which has been pulling images out of G IFs since 1 (8). (1) deployed everywhere you can think of and some places you probably can't - graphics as olications and web browsers on multiple operating systems, game consoles, s martiplones, and likely your ATM too.
IJKPlayer	Bilibili	Just Blayer 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 人,、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	_403-41	一个 SharedPreferences 的包装器,真正支持跨多进程共享数据。
Tinker	<u>Tencent</u>	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。

■邮光地址敏感信息提取

EMAIL	源码文件
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 スト
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_/12*s_kplid=%3\$s"

"sohu_api_url_segment" : "http://%1\$s%2\$s/%3\$s?key=%4\$s&idq %5\$\$&n=1"

"sohu_api_url_p2purl": "http://%1\$s/p2p?new=%2\$s&nu_n=%3\$s&key=%4\$s"

"pref_key_choose_danmaku_engine" : "ChooseDan rake Engine"

"sohu_api_url_1" : "http://hot.vrs.sohu.col.v/\.s_ las \.action?vid=%1\$5&v r=%25\$&ref=0001"

6X8Y4XdM2Vhvn0KfzcEatGnWaNU

4kU71lN96TJUomD1vOU9lgj9\(\mathbf{J}\)+\(\mathbf{J}\)\(\mathbf{M}\)+zzjst5U=

258EAFA5-E914-47D*A 35.C*/-C5AB0DC85B11

03a976511e2cb23.7 26808fb7af3c05

d16ffded 5.5219d4ba3b2f9e70561

免责声明及风险提示:

本报告由南明离太多观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念负责。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。

南明离火移动文义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。

© 2025 南明离火 - 移动安全分析平台自动生成