南明离火
移动应用检测平台

ANDROID 静态分析报告

TikTok • v3.8.2

分析日期: 2024-05-31 07:17:21

应用概览

文件名称:	de7353f4ecd404958e3e7d57d270a004faf091c81758a738b6368990b3c67413.apk
文件大小:	28.1MB
应用名称:	TikTok
软件包名:	com.ticohb115.pucrxb115fab0.lubei
主活动:	com.pandora.o147.module.splash.SplashScreen
版本号:	3.8.2
最小SDK:	21
目标SDK:	30
加固信息:	未加壳
应用程序安全分数:	43/100 (中风险)
跟踪器检测:	1/432
杀软检测:	18 个杀毒软件报毒
MD5:	a79815ae3a6d78ea48616c67d25e29a5
SHA1:	9a9a2215084cfe2869cf69b5f6[illegible]ffa7c4e
SHA256:	de7353f4ecd404958e3e7d57d270a004faf091c81758a738b6368990b3c67413

分析结果严重性分布

高危	中危	信息	安全	关注
4	14	2	1	14

四大组件导出状态统计

Activity组件：18个，其中export的有： 0个
Service组件：5个，其中export的有： 1个
Receiver组件：8个，其中export的有： 1个
Provider组件：3个，其中export的有： 0个

应用签名证书信息

二进制文件已签名

v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=rgigc, ST=rgigc, L=rgigc, O=rgigc, OU=rgigc, CN=rgigc.com
签名算法: rsassa_pkcs1v15
有效期自: 2024-05-14 13:55:03+00:00
有效期至: 2051-09-30 13:55:03+00:00
发行人: C=rgigc, ST=rgigc, L=rgigc, O=rgigc, OU=rgigc, CN=rgigc.com
序列号: 0x30ad035b
哈希算法: sha256
证书MD5: 82689568537ab8ec5ea05fc75e4183fa
证书SHA1: 0dc440f4397e9f454509ebeb0567c62df69dd439
证书SHA256: 56c87cff01ffd63e711b9e414862b8ee101c51f6e08f1d7d2cca63a925a20dc3
证书SHA512:
745a580e060d060f111b5a61181f12bb88628c433c84c5de76cb031103a59f6ff8b55b7b5bb37cf9cb216c621e0fb92a8bc2020aeba2bba80f763980433e0de

公钥算法: rsa
密钥长度: 2048
指纹: 7120719329e5351a7ba652449a6be245cf4daef1a6e32789da65c51ff39536d2
找到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.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.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.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。
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.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.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。

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。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。
freemme.permission.msa	未知	未知权限	来自 android 引用的未知权限。
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.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。这将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）

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.pandora.o147.module.splash.SplashScreen	Schemes: lube://, Hosts: authorize,

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	应用程序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: **4** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.0-5.0.2[minSdk=21]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	应用程序已启用明文网络流量[android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。

3	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
4	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
5	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

代码安全漏洞检测

高危: **4** | 警告: **8** | 信息: **2** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	已启用远程WebView调试	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
3	WebView加载控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	升级会员：解锁高级权限
4	应用程序记录日志信息,不应记录敏感信息	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
5	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

6	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
7	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
8	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
9	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
10	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
11	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
12	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
13	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
14	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

本报告由南明离火移动安全分析平台生成

15	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	

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/librtmp-jni.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的堆缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

2	arm64-v8a/libtraeimp-rtmp.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用
3	arm64-v8a/libtxsdl.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

4	arm64-v8a/libtxsoundtouch.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	8/30	android.permission.READ_PHONE_STATE android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.WRITE_SETTINGS android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	9/46	android.permission.CHANGE_NETWORK_STATE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.BLUETOOTH android.permission.FLASHLIGHT 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

livepull.myqcloud.com	安全	是	**IP地址:** 101.226.153.18 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
tcdnsipv6.myqcloud.com	安全	否	No Geolocation information available.
playvideo.qcloud.com	安全	是	**IP地址:** 119.45.78.99 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783333 **经度:** 119.966667 **查看:** 高德地图
tcdns.myqcloud.com	安全	是	**IP地址:** 119.45.78.99 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
yingtaoapi.lubei10000.com	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** iTakedaTakefuTakeharaTakeleyTakeoTakestanTakhliTakiTakia BatpurTakikawa TakimachiTakkobuTakoma ParkTa **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
appconfig-1309110964.cos.accelerate.myqcloud.com	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
www.o147.com	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
exoplayer.dev	安全	否	**IP地址:** 61.160.148.90 **国家:** 美利坚合众国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图

v2api.3xx.info	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
v2api.3xx.live	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
livepullipv6.myqcloud.com	安全	是	**IP地址:** 119.147.190.45 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
astat.bugly.cros.wr.pvp.net	安全	否	**IP地址:** 70.106.118.26 **国家:** 美利坚合众国 **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
dashif.org	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
aomedia.org	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
astat.bugly.qcloud.com	安全	否	**IP地址:** 119.28.121.133 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
soconfig-1309110964.cos.accelerate.myqcloud.com	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图

tiktok.chinazhi.net	安全	否	**IP地址:** 104.18.6.32 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
vodreport.qcloud.com	安全	是	**IP地址:** 58.222.30.203 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
1255566655.vod2.myqcloud.com	安全	是	**IP地址:** 58.222.26.136 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://soconfig-1309110964.cos.accelerate.myqcloud.com/armeabi-v7a.zip	com/pandora/o147/module/splash/SplashScreen.java
• https://github.com/yyued/svgaplayer-android#cache • file:///assets/	e/h/a/h.java
• http://v2api.3xx.live	com/pandora/o147/app/MyApplication.java
• https://tiktok.chinazhi.net/mili/domain_mili.json • https://yingtaoapi.lubei10000.com • https://appconfig-1309110964.cos.accelerate.myqcloud.com/domain/domain_test.json • http://v2api.3xx.live • http://35.220.240.219:8091/mili/domain_mili.json • http://v2api.3xx.info	com/pandora/o147/utils/NetUtils.java
• https://www.o147.com	com/pandora/o147/app/AppInfo.java

• https://aomedia.org/emsg/id3 • http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff145649728185196 02447/master_playlist.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d • http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff145649728185196 02447/v.f240.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d • http://playvideo.qcloud.com/getplayinfo/v2 • www.baidu.com • https://exoplayer.dev/issues/player-accessed-on-wrong-thread • http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff1456497281851960244 7/imagesprite/1513156058_533711271_00001.jpg?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3b ecfa096613659c3 • https://soconfig-1309110964.cos.accelerate.myqcloud.com/armeabi-v7a.zip • http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff145649728185196 02447/v.f230.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d • http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff145649728185196 02447/v.f210.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d • file:///assets/ • https://tcdns.myqcloud.com/queryip • http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff145649728185196 02447/v.f220.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d • http://%s/%s/%s/timeshift.m3u8?starttime=%s&appid=%s&txkbps=0 • http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff145649728185196 02447/v.f10.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d • https://astat.bugly.qcloud.com/rqd/async • http://%s/timeshift/%s/%s/timeshift.m3u8?delay=0 • http://dashif.org/guidelines/last-segment-number • 223.5.5.5 • http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff145649728185196 02447/v.f20.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d • https://github.com/yyued/svgaplayer-android#cache • http://v2api.3xx.info • https://tiktok.chinazhi.net/mili/domain_mili.json • https://yingtaoapi.lubei10000.com • https://livepull.myqcloud.com/getpulladdr • https://cloud.google.com/kms/docs/reference/rest/v1/projects.locations.keyrings.cryptokeys#crypto key • data:cs:audiopurposecs:2007 • https://vodreport.qcloud.com/describecontrolinfos/v1 • http://v2api.3xx.live • http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff145649728185196 02447/coverbysnapshot/1513156403_1311093072.100_0.jpg?t=5c08d9fa&us=someus&sign=95f34beb 353fe32cfe7f8b5e79cc28b1 • http://35.220.240.219:8091/mili/domain_mili.json • https://www.o147.com • http://%s/timeshift/%s/%s/timeshift.m3u8?delay=%d • http://%s/%s/%s/timeshift.m3u8?delay=0&appid=%s&txkbps=0 • https://h.trace.qq.com/kv • file:mconfig.misdkvsupporthighprofile: • https://appconfig-1309110964.cos.accelerate.myqcloud.com/domain/domain_test.json • http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff1456497281851960244 7/uanxx0mlsaa.wmv?t=5c08d9fa&us=someus&sign=659af5dd3f27eb92dc4ed74eb561daa4 • https://playvideo.qcloud.com/getplayinfo/v2 • http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff1456497281851960244 7/imagesprite/1513156058_533711271.vtt?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096 613659c3 • https://tcdnsipv6.myqcloud.com/queryip • https://livepullipv6.myqcloud.com/getpulladdr • https://developer.apple.com/streaming/emsg-id3 • https://astat.bugly.cros.wr.pvp.net:8180/rqd/async	自研引擎-S

第三方SDK组件分析

SDK名称	开发者	描述信息
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。

腾讯云短视频 SDK	Tencent	腾讯云点播推出了短视频一站式解决方案，覆盖了视频生成、上传、处理、分发和播放在内的各个环节，帮助用户以最快速度实现短视频应用的上线。
腾讯云实时音视频	Tencent	腾讯实时音视频（Tencent Real-Time Communication，TRTC），将腾讯 21 年来在网络与音视频技术上的深度积累，以多人音视频通话和低延时互动直播两大场景化方案，通过腾讯云服务向开发者开放，致力于帮助开发者快速搭建低成本、低延时、高品质的音视频互动解决方案。
腾讯云实时音视频 SDK	Tencent	实时音视频（Tencent RTC）基于腾讯多年来在网络与音视频技术上的深度积累，以多人音视频通话和低延时互动直播两大场景化方案，通过腾讯云服务向开发者开放，致力于帮助开发者快速搭建低成本、低延时、高品质的音视频互动解决方案。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。
Matisse	Zhihu	一个设计精美的 Android 图片视频选择器。
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。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Jetpack Media	Google	与其他应用共享媒体内容和控件，已被 media2 取代。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

第三方追踪器检测

名称	类别	网址
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

敏感凭证泄露检测

可能的密钥
腾讯Bugly SDK的key->"BUGLY_APPID" : "b6d50d858c"
"user" : "user"
27eb683b73944771ce62fbdda628a9a4
0123456789abcdefABCDEF

免责声明及风险提示: