南明离火
移动应用检测平台

ANDROID 静态分析报告

蜜桔 • v3.1.84

分析日期: 2024-03-19 16:09:26

应用概览

文件名称:	156562178_sign.apk
文件大小:	45.17MB
应用名称:	蜜桔
软件包名:	mros.zgrdbkuc.ontdvjraxj
主活动:	com.yunbao.phonelive.activity.LauncherActivity
版本号:	3.1.84
最小SDK:	26
目标SDK:	29
加固信息:	未加壳
应用程序安全分数:	52/100 (中风险)
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	70409876646c2a6ce5bb7da371e4c32e
SHA1:	abe90845df46dce993436a8c34fef9212c3aa5ce
SHA256:	3e46322e816f8ec46d23ddc70c1[illegible]3fba78e88a33205c627276a46d2576b984

分析结果严重性分布

高危	中危	信息	安全	关注
1	7	1	1	1

四大组件导出状态统计

Activity组件：36个，其中export的有： 1个
Service组件：3个，其中export的有：0个
Receiver组件：1个，其中export的有： 1个
Provider组件：6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: False
v2 签名: True
v3 签名: False

v4 签名: False
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2024-03-19 07:59:05+00:00
有效期至: 2078-12-21 07:59:05+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0xa36ef444bb01
哈希算法: sha256
证书MD5: b47df3279ece4a019ce8cdcda2f1ad05
证书SHA1: 886ee4138036a333b1c5ba21738c8c4c1ed0efe7
证书SHA256: 2fc8a9717ed52c9241287f6a16ebab28de5feb086edd1cbd548a9a4ddbfc225a
证书SHA512:
c4e43e113fb4ed8ddddf63036aacf8e2d7b2c995a7dcbb468958687415440da479689dde2af4ef70db7b38c88784e9223219654c86024a2aa36b7eddd9cace10

公钥算法: rsa
密钥长度: 2048
指纹: 79c26627994ce791fdd33d4fbc598d06094022931c12c02a5cb5231e3c316cdb
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.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.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
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.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_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WiFi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.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
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.NETWORK_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
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错略的经纬度信息，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.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。

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_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
android.permission.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
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.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加、删除帐户及删除其密码之类的操作。
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.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.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.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.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）
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.yunbao.common.arouter.SchemeFilterActivity	Schemes: guming://, Hosts: com.guming,

网络通信安全风险分析

高危: **1** | 警告: **1** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述

1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。
2	*	警告	基本配置配置为信任系统证书。

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存在漏洞的 Android 版本上 Android 8.0, minSdk=26]	警告	该应用程序可以安装在具有多个漏洞的旧版本 Android 上。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	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
4	Activity (com.yunbao.common.arouter.SchemeFilterActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity 与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
5	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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: **0** | 警告: **1** | 信息: **1** | 安全: **0** | 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

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/libclinkapi-lib.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 二进制文件中被重写。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	armeabi-v7a/libcloudclink-lib.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	armeabi-v7a/libdownloadproxy.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	armeabi-v7a/libijkhlscache-master.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 shell code 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
5	armeabi-v7a/libnetmobsec-4.4.6.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 shell code 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

6	armeabi-v7a/libtpcore-master.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
7	armeabi-v7a/libtpthirdparties-master.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

本报告由南明离火移动安全分析平台生成

恶意软件常用权限	12/30	android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.SYSTEM_ALERT_WINDOW android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.VIBRATE android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.GET_TASKS android.permission.RECEIVE_BOOT_COMPLETED android.permission.WRITE_SETTINGS android.permission.MODIFY_AUDIO_SETTINGS
其它常用权限	15/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.FLASHLIGHT android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.WRITE_EXTERNAL_STORAGE android.permission.CHANGE_WIFI_STATE android.permission.REORDER_TASKS android.permission.CHANGE_NETWORK_STATE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.FOREGROUND_SERVICE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_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
www.xiaohongshu.com	安全	是	**IP地址:** 81.69.116.87 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://img.hcharts.cn/highcharts/highcharts.js • https://img.hcharts.cn/highcharts/themes/dark-unica.js • https://img.hcharts.cn/highcharts/highcharts-more.js	自研引擎分析结果
• https://api.hcharts.cn/highcharts	自研引擎分析结果
• https://www.highcharts.com	自研引擎分析结果

本报告由南明离火移动安全分析平台生成

• http://mibailive.mbym.xyz/20200202114004_dc5a92769ef8f91c8cae1bcb42338ec3?imageView2/2/w/200/h/200 • https://qq2054970171.oss-cn-hangzhou.aliyuncs.com/207.mp4 • http://mibailive.mbym.xyz/20200202114204_863760b0c869a0b561014726e801fcd3?imageView2/2/w/600/h/600 • http://mibailive.mbym.xyz/20200201113103_f5330b2330166a71bd2ec6886a3dd07b?imageView2/2/w/200/h/200 • http://qn.zilctvp.cn/FnigmyLAFQTVP2pip5kQvlfU5xTd.jpg • http://mibailive.mbym.xyz/20200203230020_a772132866c4e13e9f37ff9df105624c?imageView2/2/w/200/h/200 • https://qq2054970171.oss-cn-hangzhou.aliyuncs.com/208.mp4 • https://qq2054970171.oss-cn-hangzhou.aliyuncs.com/203.mp4 • http://mibailive.mbym.xyz/20200201222958_599eb77b79445630947de254fc8d9e25?imageView2/2/w/600/h/600 • http://mibailive.mbym.xyz/admin/20200324/04b22c109fd941a1512d075db3d0b720.png • http://mibailive.mbym.xyz/20200203230636_ac80b702d1087355814f2c96a66d090e?imageView2/2/w/600/h/600 • http://mibailive.mbym.xyz/20200203230636_ac80b702d1087355814f2c96a66d090e?imageView2/2/w/200/h/200 • https://qq2054970171.oss-cn-hangzhou.aliyuncs.com/206.mp4 • http://qn.zilctvp.cn/FixMFpDoeOnf-46tuYS0wVFLh4yq.jpg • http://dh.fir8.vip • https://qq2054970171.oss-cn-hangzhou.aliyuncs.com/204.mp4 • http://mibailive.mbym.xyz/20200203230100_1be07997ad94c77d2acf9adb7a59274e?imageView2/2/w/200/h/200 • https://qq2054970171.oss-cn-hangzhou.aliyuncs.com/202.mp4 • http://qn.zilctvp.cn/Fp3lbdcpflxtdU08NojDBqZFRnHG.jpg • http://qn.zilctvp.cn/FtgAKaTgMZwQH6akEm-4dOxeTnRi.jpg • http://zb.brdfqs.cn/default.jpg • http://mibailive.mbym.xyz/20200201113103_f5330b2330166a71bd2ec6886a3dd07b?imageView2/2/w/600/h/600 • http://mibailive.mbym.xyz/20200202113639_67afed74ea303b3b82cf446d5c1313e3?imageView2/2/w/200/h/200 • http://qn.zilctvp.cn/Fh7xiC17NV59OJWt2dvlqedJtmkP.jpg • http://ivi.bupt.edu.cn/hls/cctv6hd.m3u8 • https://qq2054970171.oss-cn-hangzhou.aliyuncs.com/205.mp4 • http://mibailive.mbym.xyz/admin/20200324/238c3d55c37ff1205e1cd8c40171f964.png • http://mibailive.mbym.xyz/20200202114204_863760b0c869a0b561014726e801fcd3?imageView2/2/w/200/h/200 • http://mibailive.mbym.xyz/20200201222958_599eb77b79445630947de254fc8d9e25?imageView2/2/w/200/h/200 • http://mibailive.mbym.xyz/20200202114004_dc5a92769ef8f91c8cae1bcb42338ec3?imageView2/2/w/600/h/600 • http://mibailive.mbym.xyz/20200203230540_aeaa7aa95cc8ff2b33156bde19fe8c3f?imageView2/2/w/600/h/600 • http://mibailive.mbym.xyz/20200203230540_aeaa7aa95cc8ff2b33156bde19fe8c3f?imageView2/2/w/200/h/200 • http://mibailive.mbym.xyz/20200202114101_566260c6deba63da483e0aa3fcbbf3f5?imageView2/2/w/200/h/200 • http://mibailive.mbym.xyz/20200202132555_f91b33657fca8d69a4d63550d637772d?imageView2/2/w/200/h/200 • http://mibailive.mbym.xyz/20200202113639_67afed74ea303b3b82cf446d5c1313e3?imageView2/2/w/600/h/600 • http://zb.brdfqs.cn/default_thumb.jpg • http://mibailive.mbym.xyz/20200203230100_1be07997ad94c77d2acf9adb7a59274e?imageView2/2/w/600/h/600 • http://mibailive.mbym.xyz/20200202132555_f91b33657fca8d69a4d63550d637772d?imageView2/2/w/600/h/600 • http://mibailive.mbym.xyz/20200203230020_a772132866c4e13e9f37ff9df105624c?imageView2/2/w/600/h/600 • https://qq2054970171.oss-cn-hangzhou.aliyuncs.com/201.mp4 • http://mibailive.mbym.xyz/20200202114101_566260c6deba63da483e0aa3fcbbf3f5?imageView2/2/w/600/h/600	自研引擎分析结果
• https://static.meiqia.com/widget/loader.js	自研引擎分析结果

• https://www.xiaohongshu.com/experience/home?fullscreen=true	pr2/h.java
• https://www.xiaohongshu.com/api/hawking/h5/redirect?scene_code=COOPER_CENTER	pr2/j.java
• www.xiaohongshu.com/user/shopping_cart?isRN=true&rnName=shopping-cart&rnPath=user/shopping_cart	pr2/z.java
• https://www.xiaohongshu.com/login/otherquestion	te2/n.java
• www.xiaohongshu.com/user/shopping_cart?isRN=true&rnName=shopping-cart&rnPath=user/shopping_cart	tr2/a0.java
• https://www.xiaohongshu.com/experience/home?fullscreen=true	tr2/i.java
• https://www.xiaohongshu.com/api/hawking/h5/redirect?scene_code=COOPER_CENTER	tr2/k.java
• www.xiaohongshu.com/user/shopping_cart?isRN=true&rnName=shopping-cart&rnPath=user/shopping_cart • https://www.xiaohongshu.com/api/hawking/h5/redirect?scene_code=COOPER_CENTER • https://github.com/vinc3m1 • https://www.xiaohongshu.com/login/otherquestion • https://www.xiaohongshu.com/experience/home?fullscreen=true • https://github.com/vinc3m1/RoundedImageView • https://github.com/vinc3m1/RoundedImageView.git	自研引擎分析结果
• 1.3.0.2	lib/armeabi-v7a/libcloudclink-lib.so
• data:%lld,%lld,	lib/armeabi-v7a/libdownloadproxy.so

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，及时获知用户反馈。
AntiFakerAndroidChecker	happylishang	Android 模拟器检测，检测 Android 模拟器，作为可信 DeviceID，应对防刷需求等。
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。
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。
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。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
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。

敏感凭证泄露检测

可能的密钥
"find_pwd_forget" : "忘记密码"

"login_auth_ing" : "正在授权登录"

"main_live_type_pwd" : "密码"

"pref_key_enable_surface_view" : "pref.enable_surface_view"

"cash_input_bank_user_name" : "请输入持卡人姓名"

"pref_key_using_android_player" : "pref.using_android_player"

"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

"mobile_authentication" : "手机认证"

"pref_key_using_opensl_es" : "pref.using_opensl_es"

"reg_input_pwd_2" : "请确认密码"

"pref_key_media_codec_handle_resolution_change" : "pref.media_codec_handle_resolution_change"

"live_input_password" : "请输入房间密码"

"login_auth_cancle" : "授权取消"

"input_payment_password" : "请输入支付密码(6位纯数字)"

"login_auth_failure" : "授权失败"

"pref_key_pixel_format" : "pref.pixel_format"

"promotion_user" : "用户"

"find_pwd" : "找回密码"

"login_forget_pwd" : "忘记密码"

"payment_password" : "支付密码"

"pref_key_enable_background_play" : "pref.enable_background_play"

"withdraw_pwd_str" : "提现密码"

"find_pwd_find" : "立即找回"

"modify_pwd" : "重置密码"

"emotion_status_secret" : "保密"

"auth_completed" : "手机已认证"

"pref_key_using_media_codec_auto_rotate" : "pref.using_media_codec_auto_rotate"

"live_type_pwd" : "密码房间"

"pref_key_using_media_codec" : "pref.using_media_codec"

"reg_input_pwd_1" : "请填写密码"

"phone_auth" : "手机绑定"

"login_auth_success" : "登录成功"

"pref_key_last_directory" : ""
"pref_key_enable_no_view" : "pref.enable_no_view"
"reg_input_pwd_3" : "邀请码(选填)"
"dun_key" : "BvyoNmnTUIqvZufrqyuGPczZF/obbz8wLUQZMPRjS0yO7ir5gj50GehaWU0RTNUDhVpt1KCmUN4guzu85MNwqw1EJfBeolyVsWgSFhVFR/Wy6bmdTe6rST/xQu/nTbMKPQwMQrFVY4MeAihOWgT160KJvcWU6DqWxBfxzuQxpYPWDnT+h4s="
"follow_author" : "关注主播"
"enter_withdraw_pwd" : "请输入提现密码"
"live_set_pwd" : "请设置房间密码"
"pref_key_using_mediadatasource" : "pref.using_mediadatasource"
"login_input_pwd" : "请输入密码"
"pref_key_player" : "pref.player"

免责声明及风险提示: