南明离火
移动应用检测平台

ANDROID 静态分析报告

码库 • v3.0.6

分析日期: 2024-08-25 08:07:42

应用概览

文件名称:	码库.apk
文件大小:	13.69MB
应用名称:	码库
软件包名:	xyz.axse.ybrbql
主活动:	com.uetoken.cn.activity.SplashActivity
版本号:	3.0.6
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	38/100 (高风险)
跟踪器检测:	2/432
杀软检测:	2 个杀毒软件报毒
MD5:	dcf7945eb77ddeb54cf5fbe261af1798
SHA1:	c002a07bfc16c955226121eb3f1a6b4ccd5c03fc
SHA256:	be5091a6cd07f9afcf9cefda98a69e15ebb550471d9dd238d25f0e26a08cb581

分析结果严重性分布

高危	中危	信息	安全	关注
8	0	2	1	12

四大组件导出状态统计

Activity组件：93个，其中export的有：3个
Service组件：6个，其中export的有：3个
Receiver组件：1个，其中export的有：1个
Provider组件：1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: False
v3 签名: False
v4 签名: False
主题: C=China, ST=China, L=China, O=China, OU=China, CN=China
签名算法: rsassa_pkcs1v15
有效期自: 2023-11-22 09:20:54+00:00
有效期至: 2078-08-25 09:20:54+00:00
发行人: C=China, ST=China, L=China, O=China, OU=China, CN=China
序列号: 0xc34153799caddb55
哈希算法: sha256
证书MD5: 43aaa293442e768d7288e1142799e873
证书SHA1: c9a086d9dfa901b78444cf1c6cb632a106d598af
证书SHA256: 0390d45dbbb910a64fd9965da3316f425f9605612279048c842d03c5c7a18f61
证书SHA512:
ba01ae1aee68536f3ba190a3bfcfc0678a6dc72a812de2c9cd4664e366670a60a21264f0d1c19313ef38b5c01ebad38d1d2c7a8ff76c91a05693b2a4d038da61

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.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.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.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
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.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.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.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.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.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_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.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.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.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.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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如图片，聊天图片。
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.startForegr ound，用于podcast播放（播放悬浮播放，锁屏播放）
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.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
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.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
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。
android.permission.SET_DEBUG_APP	危险	启用应用程序调试	允许应用程序启动对其他应用程序的调试。恶意应用程序可借此终止其他应用程序。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
com.fingerprints.service.ACCESS_FINGERPRINT_MANAGER	未知	未知权限	来自 android 引用的未知权限。
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集，但对即时应用程序公开。
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.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
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。
getui.permission.GetuiService.com.uetoken.cn	未知	未知权限	来自 android 引用的未知权限。

com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
com.uetoken.cn.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.uetoken.cn.activity.SplashActivity	Schemes: ue://, uepay://,

网络通信安全风险分析

高危: **1** | 警告: **0** | 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。

证书安全合规分析

高危: **1** | 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
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名。如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的影响。在安卓5.0-7.0上运行且使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也将存在漏洞。

Manifest 配置安全分析

高危: **4** | 警告: **11** | 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]	警告	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	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。
5	Activity (com.uetoken.cn.activity.SplashActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
6	Activity设置了TaskAffinity属性 (com.igexin.sdk.PushActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
7	Activity设置了TaskAffinity属性 (com.igexin.sdk.GActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
8	Activity (com.igexin.sdk.GActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
9	Activity (com.igexin.sdk.GActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
10	Activity (com.uetoken.cn.wxapi.WXEntryActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
11	Activity (com.uetoken.cn.wxapi.WXEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
12	Activity (com.uetoken.cn.wxapi.WXPayEntryActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
13	Activity (com.uetoken.cn.wxapi.WXPayEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
14	Broadcast Receiver (com.igexin.sdk.PushReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
15	Service (com.uetoken.cn.getui.GTuiPushService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

16	Service (com.igexin.sdk.PushService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
17	Service (com.taobao.sophix.aidl.DownloadService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

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
2	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
3	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
4	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
5	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
6	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

7	SHA-1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
8	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
9	应用程序使用带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
10	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
11	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
12	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

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/libJniUtil.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	True info 二进制文件有以下加固函数: ['__strlen_chk', '__vsprintf_chk']	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	13/30	android.permission.CAMERA android.permission.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED android.permission.VIBRATE android.permission.GET_TASKS android.permission.MODIFY_AUDIO_SETTINGS android.permission.RECORD_AUDIO android.permission.READ_CONTACTS android.permission.READ_PHONE_STATE android.permission.SYSTEM_ALERT_WINDOW
其它常用权限	14/46	android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_AUDIO android.permission.READ_MEDIA_VIDEO com.google.android.gms.permission.AD_ID android.permission.FLASHLIGHT

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

url.cn	安全	是	**IP地址:** 115.227.15.233 **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
s-gt.getui.com	安全	是	**IP地址:** 115.227.15.13 **国家:** 中国 **地区:** 浙江 **城市:** 嘉兴 **纬度:** 30.752199 **经度:** 120.750000 **查看:** 高德地图
mikepenz.com	安全	否	**IP地址:** 104.21.[redacted]7.65 **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
mpush-api.aliyun.com	安全	是	**IP地址:** 115.227.15.233 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
ue.dtwy.xyz	安全	否	**IP地址:** 13.33.183.61 **国家:** 印度 **地区:** 泰米尔纳德邦 **城市:** 金奈 **纬度:** 13.087898 **经度:** 80.278481 **查看:** Google 地图
log.umsns.com	安全	是	**IP地址:** 115.227.15.233 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
c-hzgt2.getui.com	安全	是	**IP地址:** 115.227.15.233 **国家:** 中国 **地区:** 浙江 **城市:** 嘉兴 **纬度:** 30.752199 **经度:** 120.750000 **查看:** 高德地图
c.umsns.com	安全	是	**IP地址:** 115.227.15.233 **国家:** 中国 **地区:** 广东 **城市:** 惠州 **纬度:** 39.509766 **经度:** 116.693001 **查看:** 高德地图

sdk.open.inc2.igexin.com	安全	否	No Geolocation information available.
sdk.open.amp.igexin.com	安全	是	**IP地址:** 115.227.15.233 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
sdk.open.lbs.igexin.com	安全	是	**IP地址:** 115.227.15.233 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
sdk.open.phone.igexin.com	安全	是	**IP地址:** 115.227.15.233 **国家:** 中国 **地区:** 浙江 **城市:** 嘉兴 **纬度:** 30.752199 **经度:** 120.750000 **查看:** 高德地图
pre-c.umsns.com	安全	是	**IP地址:** 203.119.252.86 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
d.gt.igexin.com	安全	否	No Geolocation information available.
user-upay.ckv-test.sulink.cn	安全	是	**IP地址:** 47.97.231.117 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
ulogs.umengcloud.com	安全	是	**IP地址:** 115.227.15.233 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.061668 **经度:** 118.777992 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://github.com/kongzue/dialogx	q5/a.java
• https://mpush-api.aliyun.com/v2.0/a/audid/req/	w8/h.java

• http://user-upay.ckv-test.sulink.cn/license/userinfo.aspx	com/uetoken/cn/activity/AboutUsActivity.java
• 2.6.4.13	c0/d.java
• 2.6.4.13	q/a.java
• https://github.com/kongzue/dialogx/wiki	com/kongzue/dialogx/interfaces/k.java
• http://adash.man.aliyuncs.com:80/man/api?ak=23356390&s=	g0/a.java
• https://url.cn/5tzz8ic	com/uetoken/cn/activity/WebDebugActivity.java
• https://github.com/kongzue/dialogx/wiki	i5/a.java
• http://47.97.254.231:8001 • http://sg-ue.oss-ap-southeast-1.aliyuncs.com/ue/%s_test.json • https://sg-ue.oss-ap-southeast-1.aliyuncs.com/ue/%s.json • https://ue.dtwy.xyz	e9/a.java
• 2.6.4.13	c0/t.java
• https://github.com/kongzue/dialogx	n5/a.java
• https://github.com/kongzue/dialogx	com/kongzue/dialogx/interfaces/BaseDialog.java

• 42.62.120.14 • https://api.weixin.qq.com/sns/userinfo?access_token= • https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079 • https://github.com/mikepenz/materialize • http://sg-ue.oss-ap-southeast-1.aliyuncs.com/ue/%s_test.json • https://sg-ue.oss-ap-southeast-1.aliyuncs.com/ue/%s.json • http://sdk.open.lbs.igexin.com/api.htm • http://sdk.open.amp.igexin.com/api.htm • http://sdk.open.phone.igexin.com/api.php • https://debugx5.qq.com • https://debugtbs.qq.com • http://user-upay.ckv-test.sulink.cn/license/userinfo.aspx • https://log.umsns.com/ • https://pre-c.umsns.com/ulink/getrtc • http://s-gt.getui.com/api.php • https://github.com/mikepenz/android-iconics • http://config • 10.0.0.172 • https://c.umsns.com/ulink/getrtc • https://api.weixin.qq.com/sns/oauth2/refresh_token?appid= • https://url.cn/5tzz8ic • www.qq.com • http://adash.man.aliyuncs.com:80/man/api?ak=23356390&s= • https://github.com/kongzue/dialogx • http://d.gt.igexin.com/api.htm • https://tbs.imtt.qq.com/plugin/debugplugin_v2.tbs • http://mikepenz.com/ • https://api.weixin.qq.com/sns/oauth2/refresh_token? • http://sdk.open.inc2.igexin.com/api.php • https://debugtbs.qq.com?10000 • https://log.umsns.com/link/weixin/download/ • 2.6.4.13 • https://github.com/mikepenz/fastadapter • https://pms.mb.qq.com/rsp204 • 127.0.0.1 • https://github.com/kongzue/dialogx/wiki • 10.101.84.136 • http://47.97.254.231:8001 • http://log.umsns.com/link/weixin/download/ • https://mpush-api.aliyun.com/v2.0/a/auth/rsp/ • http://c-hzgt2.getui.com/api.php • https://api.weixin.qq.com/sns/oauth2/access_token? • https://github.com/mikepenz/materialdrawer • https://ulogs.umengcloud.com • https://ue.dtwy.xyz • https://mdc.html5.qq.com/mi?channel_id=50079&u= • 3.3.2.2 • https://cfg.imtt.qq.com/tbs?v=2&mk= • https://log.umsns.com/link/qq/download/	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
岳鹰全景监控	Alibaba	岳鹰全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。
个推	个推	SDK 快速集成，免费注册使用。智能推送+场景推送，有效提升用户活跃度与粘性。
RenderScript	Android	RenderScript 是用于在 Android 上以高性能运行计算密集型任务的框架。RenderScript 主要用于数据并行计算，不过串行工作负载也可以从中受益。RenderScript 运行时可在设备上提供的多个处理器（如多核 CPU 和 GPU）间并行调度工作。这样您就能够专注于表达算法而不是调度工作。RenderScript 对于执行图像处理、计算摄影或计算机视觉的应用来说尤其有用。

阿里移动热修复	Aliyun	移动热修复（Mobile Hotfix）是面向Android、iOS 平台应用提供的在线热修复服务方案，产品基于阿里巴巴首创的 Hotpatch 技术，提供细粒度热修复能力，无需等待发版即可实时修复应用线上问题，用户全程无感知。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
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。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

邮箱地址敏感信息提取

EMAIL	源码文件
x5tbs@tencent.com	自研引擎-S

第三方追踪器检测

名称	类别	网址
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Crash reporting, Analytics	https://reports.exodus-privacy.eu.org/trackers/448

敏感凭证泄露检测

可能的密钥
个推-推送服务的=> "PUSH_APPKEY" : "JP8B58lA[illegible]3EYLm6mhq7"
个推-推送服务的=> "PUSH_APPID" : "h[illegible]ji8pHTUBwot608"
个推-推送服务的=> "PUSH_APPSECRET" : "ajwZNDA56hAl3uROFJTjo"
百度地图的=> "com.baidu.lbsapi.API_KEY" : "Oc4roLT3pwbi1oGWOqzpwMTi51rafQFm"
"library_materialunpacker_authorWebsite" : "http://mikepenz.com/"
"str_authorization_dialog" : "OK."
"library_materialize_authorWebsite" : "http://mikepenz.com/"
"verify_dialog_loginPwd_weak_content" : "OK."

"verify_dialog_payPwd_weak_content" : "OK."
"verify_dialog_loginPwd_lock_btn" : "Understood"
"str_authorization_title" : "Authorize"
"library_fastadapter_authorWebsite" : "http://mikepenz.com/"
"library_AndroidIconics_authorWebsite" : "http://mikepenz.com/"
QrMgt8GGYI6T52ZY5AnhtxkLzb8egpFn3j5JELI8H6wtACbUnZ5cc3aYTsTRbmkAkRJeYbtx92LPBWm7nBO9UIl7y5i5MQNmUZNf5QEN0xF5tGyo7yJ2G0MBjWvy6iAtlAbacKP0SwOUeUWx5dsBdyhxa7Id1APtybSdDgicBDuNjI0mlZFUzZSS9dmN8lBD0WTVOMz0pRZbR3cysomRXOO1ghqjJdTqyDIx2NNAEszN8RMGjrzyU7Hjbmwi6YNK
5bbaf584b465f592c90000ae
16594f72217bece5a457b4803a48f2da
QrMgt8GGYI6T52ZY5AnhtxkLzb8egpFn
840c18270dc7042b7b5df5a3c61f0a7f
2e916ff767facd6e07c9803f14196b16

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。本平台不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。