南明离火
移动应用检测平台

ANDROID 静态分析报告

翔明办公协同管理系统 • v4.6.6

分析日期: 2024-06-17 19:09:50

应用概览

文件名称:	unijiagucn.xmkj.oa_0612113416.apk
文件大小:	25.85MB
应用名称:	翔明办公协同管理系统
软件包名:	cn.xmkj.oauniapp
主活动:	io.dcloud.PandoraEntry
版本号:	4.6.6
最小SDK:	19
目标SDK:	30
加固信息:	未加壳
应用程序安全分数:	46/100 (中风险)
杀软检测:	AI评估：可能有安全隐患
MD5:	b1d97572582ca6973bb25d979e4792da
SHA1:	700408da914ffbcff8d9098b3c90b66f45ba[illegible]c5
SHA256:	f6c2f67b23b6950cb8ace984[illegible]e87c567fd8a4acd35[illegible]257c1421833652

分析结果严重性分布

高危	中危	信息	安全	关注
3	6	0	1	4

四大组件导出状态统计

Activity组件：18个，其中export的有：1个
Service组件：16个，其中export的有：7个
Receiver组件：5个，其中export的有：1个
Provider组件：6个，其中export的有：1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=cn, ST=guizhou, L=guiyang, O=jsb, OU=xmkj, CN=WU
签名算法: rsassa_pkcs1v15
有效期自: 2020-09-08 07:22:17+00:00
有效期至: 2120-08-15 07:22:17+00:00
发行人: C=cn, ST=guizhou, L=guiyang, O=jsb, OU=xmkj, CN=WU
序列号: 0x7fca590a
哈希算法: sha256
证书MD5: e68373d8157a282cf9b8114efc830d67
证书SHA1: 70fc029a01dcc54f2242862f80e202c351505a09
证书SHA256: 28cf930ef58a7b5f0e7168c11482bb455247db85a89b22740b2a0fba3d4e277e
证书SHA512:
fbce0564f7dfa447afe22756e248ab5fb19238fc6d9710c4bb5b07b043f31cc05b93cdeb5125848a642efca828a70ef961726ae2d6e67a[illegible]358cfce7e399b5dc

公钥算法: rsa
密钥长度: 2048
指纹: c58a811d486931a4bd0b1a67208806cafcc4c70a9554bcbd01a30ed7cad5261b
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.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.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.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.INSTALL_PACKAGES	签名(系统)	请求安装APP	允许应用程序安装全新的或更新的 Android 包。恶意应用程序可能会借此添加其具有任意权限的新应用程序。
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.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.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.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.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.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.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.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.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.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.BROADCAST_PACKAGE_ADDED	签名	接收新增APP的通知	它允许一个应用程序接收到其他应用程序添加新包（即新安装的可执行文件）的广播消息。
android.permission.BROADCAST_PACKAGE_CHANGED	签名	接收APP变化的通知	它允许一个应用程序接收到其他应用程序变化（安装、卸载、修改）的广播消息。
android.permission.BROADCAST_PACKAGE_INSTALL	签名	接收APP安装的通知	它允许一个应用程序接收到其他应用程序安装新包（即新安装的可执行文件）的广播消息。
android.permission.BROADCAST_PACKAGE_REPLACED	签名	接收APP替换的通知	它允许一个应用程序接收到其他应用程序被覆盖安装的广播消息。
android.permission.RESTART_PACKAGES	普通	重启进程	允许程序自己重启或重启其他程序
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。
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。
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_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_MEDIA_VISUAL_USER_SELECTED	危险	允许从外部存储读取用户选择的图像或视频文件	允许应用程序从用户通过权限提示照片选择器选择的外部存储中读取图像或视频文件。应用程序可以检查此权限以验证用户是否决定使用照片选择器，而不是授予对 READ_MEDIA_IMAGES 或 READ_MEDIA_VIDEO 的访问权限。它不会阻止应用程序手动访问标准照片选择器。应与 READ_MEDIA_IMAGES 和/或 READ_MEDIA_VIDEO 一起请求此权限，具体取决于所需的媒体类型。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	普通	桌面图标角标	vivo平台桌面图标角标，接入vivo平台后需要用户手动开启，开启完成后收到新消息时，在已安装的应用桌面图标右上角显示“数字角标”。
getui.permission.GetuiService.cn.xmkj.oauniapp	未知	未知权限	来自 android 引用的未知权限。
android.permission.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
cn.xmkj.oauniapp.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
cn.xmkj.oauniapp.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	未知权限	来自 android 引用的未知权限。

本报告由南明离火移动安全分析平台生成

com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
cn.xmkj.oauniapp.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
freemme.permission.msa	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
io.dcloud.PandoraEntry	Schemes: unipush://, xmnewapp://, Hosts: io.dcloud.unipush, Paths: /,

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: **3** | 警告: **15** | 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 4.4-4.4.4, [minSdk=19]	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	Activity (io.dcloud.PandoraEntryActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。

4	Activity (com.igexin.sdk.PushActivity) 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。
5	Activity (io.dcloud.WebAppActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
6	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
7	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。
8	Service (com.igexin.sdk.GTIntentService) 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。
9	Service (com.igexin.sdk.GService) 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。
10	Activity (com.igexin.sdk.GetuiActivity) 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。
11	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护。 Permission: cn.xmkj.oauniapp.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	发现 Broadcast Receiver被导出，但受权限保护。
12	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护。 Permission: cn.xmkj.oauniapp.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	发现 Broadcast Receiver被导出，但受权限保护。
13	Service (com.huawei.hms.support.api.push.service.HmsMsgService) 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。
14	Content Provider (com.huawei.hms.support.api.push.PushProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider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.igexin.sdk.OppoPushService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE [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。
16	Service (com.igexin.sdk.OppoAppPushService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.heytap.mcs.permission.RECIEVE_PUSH_MESSAGE [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。
17	Service (com.vivo.push.sdk.service.CommandClientService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.push.permission.UPSTAGESERVICE [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。
18	Service (com.xiaomi.mipush.sdk.PushMessageHandler) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.xiaomi.xmsf.permission.MIPUSH_RECEIVE [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。
19	Broadcast Receiver (com.igexin.sdk.MiuiPushReceiver) 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。
20	Activity (com.xiaomi.mipush.sdk.NotificationClickedActivity) 的启动模式不是 standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
21	Activity (com.xiaomi.mipush.sdk.NotificationClickedActivity) 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。

代码安全漏洞检测

序号	问题	等级	参考标准	文件位置

Native 库安全加固检测

本报告由南明离火移动安全分析平台生成

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/libashield.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

2	arm64-v8a/libashieldAdapter.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/libenvid-ashield-sdk.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/liblamemp3.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
5	arm64-v8a/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。		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: ['__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__memmove_chk', '__vsprintf_chk']	False warning 符号可用

6	arm64-v8a/libzxprotect.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.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_FINE_LOCATION android.permission.CAMERA android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.ACCESS_COARSE_LOCATION android.permission.READ_PHONE_STATE android.permission.GET_TASKS
其它常用权限	10/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.FLASHLIGHT android.permission.CHANGE_NETWORK_STATE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.ACCESS_BACKGROUND_LOCATION

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

lame.sf.net	安全	否	**IP地址:** 104.18.34.154 **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
id6.me	安全	是	**IP地址:** 42.123.76.150 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397103 **查看:** 高德地图
nisportal.10010.com	安全	是	**IP地址:** 42.123.76.150 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397103 **查看:** 高德地图
msg.cmpassport.com	安全	是	**IP地址:** 42.123.76.150 **国家:** 中国 **地区:** 安徽 **城市:** 合肥 **纬度:** 31.863815 **经度:** 117.280830 **查看:** 高德地图
zxid-m.mobileservice.cn	安全	是	**IP地址:** 42.123.76.150 **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

URL 链接安全分析

URL信息	源码文件
• https://xmoa.xmkj.cn/m/privacy/service/ • http://feross.org • https://ide.dcloud.net.cn/uni-app/uni.webview.1.5.2.js • https://xmoa.xmkj.cn/m/privacy/privacy/ • https://service.dcloud.net.cn/uniapp/feedback.html	自研引擎-A
• 3.3.5.0	自研引擎-M
• http://lame.sf.net	lib/arm64-v8a/liblamemp3.so

• https://nisportal.10010.com:9001 • https://msg.cmpassport.com/h5/getmobile • https://id6.me/gw/preuniq.do • https://zxid-m.mobileservice.cn/sdk/said/ping	lib/arm64-v8a/libzxprotect.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
MSA SDK	[移动安全联盟]()	移动智能终端补充设备标识体系统一调用 SDK 由中国信息通信研究院泰尔终端实验室、移动安全联盟整合提供，知识产权归中国信息通信研究院所有。
Fresco	[Facebook]()	Fresco 是一个用于管理图像及其使用的内存的 Android 库。
C++ 共享库	[Android]()	在 Android 应用中运行原生代码。
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.
android-gif-drawable	[koral--]()	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
Weex	[Alibaba]()	Weex 致力于使开发者能基于通用跨平台的 Web 开发语言和开发经验，来构建 Android、iOS 和 Web 应用。简单来说，在集成了 WeexSDK 之后，你可以使用 JavaScript 语言和前端开发经验来开发移动应用。

敏感凭证泄露检测

可能的密钥
个推–推送服务的=> "PUSH_APPKEY" : "pn[illegible]Qrpe67BKa50Qltp5"
华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "104460573"
凭证信息=> "app_id" : "1[illegible]5523340"
卓信ID-SDK的=> "ZX_CHANNEL_ID" : "C01-G[illegible]ztjH0JLdBC"
UniPush推送的=> "MIPUSH_APPKEY" : "XM_5232010527817"
凭证信息=> "api_key" : "c29214[illegible]5c[illegible]df94ee77eeb3ca051536f3"
UniPush推送的=> "MIPUSH_APPID" : "XM_2882303761520105817"
华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "appid=104460573"
vivo推送的=> "local_iv" : "MzMsMzQsMzUsMzYsMzcsMzgsMzksNDAsNDEsMzIsMzgsMzcsMzYsMzUsMzQsMzMsI0AzNCwzMiwzMywzNywzMywzNCwzMiwzMywzMywzMywzNCw0MSwzNSwzNSwzMiwzMiwjQDMzLDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDMyLDM4LDM3LDMzLDM1LDM0LDMzLCNAMzQsMzIsMzMsMzcsMzMsMzQsMzIsMzMsMzMsMzMsMzQsNDEsMzUsMzIsMzIsMzI"
个推–推送服务的=> "PUSH_APPID" : "25J0H4lqAC9DPuaYBxn9v6"

个推-推送服务的=> "GETUI_APPID" : "25J0H4lqAC9DPuaYBxn9v6"
UniPush推送的=> "OPPOPUSH_APPKEY" : "OP_5fa10d898a6b4526b09bf019e9befcbb"
UniPush推送的=> "OPPOPUSH_APPSECRET" : "OP_c12e038a17f64877b0c12a8ffc4883a1"
个推-推送服务的=> "PUSH_APPSECRET" : "B8F6jNH9BM6WNlCHXtnnH4"
卓信ID-SDK的=> "ZX_APPID_GETUI" : "913e6a50-c3b6-4989-8ac6-1ecb53649be3"
DCLOUD的 "APPID" : "__UNI__cn.xmkj.oa"
DCLOUD的 "ApplicationId" : "cn.xmkj.oauniapp"
DCLOUD的 "DCLOUD_STREAMAPP_CHANNEL" : "cn.xmkj.oauniapp|__UNI__cn.xmkj.oa|127598130810|"
DCLOUD的 "AD_ID" : "127598130810"
"dcloud_tips_certificate" : "certificate"
"dcloud_permissions_reauthorization" : "reauthorize"
YW5kcm9pZC5jb250ZW50LnBtLlBhY2thZ2VQYXJzZXIkUGFja2FnZQ==

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。