



MoGua

中保 null.APK 分析报告



APP名称:

中保

包名:	kcm.FMP56717X0
域名线索:	6条
URL线索:	17条
邮箱线索:	0条
分析日期:	2025年4月23日
分析平台:	摸瓜APK反编译平台

文件名: base.apk
文件大小: 27.87MB
MD5值: da2c0510da7859089a06f61b19bf7b9d
SHA1值: 4ad8846b77acd82cf74b9fc6c93049626bf4c04d
SHA256值: c74b0cfa8235b704cdfcc5eef696d5022ec05345cdf807f50dd5b6c4c00bdc66

i APP 信息

App名称: 中保
包名: kcm.FMP56717X0
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: null
安卓版本:

🔍 域名线索

域名	服务器信息
er.dcloud.io	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.
ask.dcloud.net.cn	IP: 101.72.254.86 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
m3w.cn	IP: 119.188.44.177 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223

er.dcloud.net.cn	IP: 43.142.57.168 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
schemas.android.com	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/283	io/dcloud/feature/utsplugin/ProxyModule.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/p/r.java

https://ask.dcloud.net.cn/article/283	io/dcloud/p/h1.java
https://er.dcloud.io/rv	io/dcloud/p/d0.java
https://er.dcloud.net.cn/rv	io/dcloud/p/d0.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java

邮箱线索

手机线索

签名证书

APK已签名

v1 签名: False

v2 签名: True

v3 签名: False

找到 1 个唯一证书

主题: C=catgllfwcoedzw, ST=ltvytwyrknvnnkq, L=wksbqsgbfirxtmb, O=wow1744101872616, OU=jsz1744101872616, CN=Xfsb1744101872616

签名算法: rsassa_pkcs1v15

有效期自: 2025-04-08 08:44:32+00:00

有效期至: 2075-03-27 08:44:32+00:00

发行人: C=catgllfwcoedzw, ST=ltvytwyrknvnnkq, L=wksbqsgbfirxtmb, O=wow1744101872616, OU=jsz1744101872616, CN=Xfsb1744101872616

序列号: 0x5b4e388e

哈希算法: sha1
md5值: c49b4699ed2bd49157728404b13b52db
sha1值: 7fdf59b317b515fc30851138f1260c6f22661046
sha256值: e676ea492707fe53e7ce6dc4cda970d0735aed58583944ae834bd36f644d7e16
sha512值: 9edd68e8e41c1a37cc545992627ff1062e9987cb143a522fadd774db94594a9e7dcf2d2104b21c1fc64efca4bbb4c36727ca8177197be042deeb3020e2b939f5
公钥算法: rsa
密钥长度: 1024
指纹: 8dbf801c84e1709d4c9963176df604757fbc1b79b001ef0eff00a6c705e7696a

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

	是否		
--	----	--	--

向手机申请的权限	危险	类型	详细情况
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_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
kcm.FMP56717X0_com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	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。
kcm.FMP56717X0 com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference

	知	permission	
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
kcm.FMP56717X0.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	正常	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	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
android.permission.ACCESS_CHECKIN_PROPERTIES	系统需要	访问登记属性	允许对登记服务上传的属性进行读/写访问。不供普通应用程序使用
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.CALL_PRIVILEGED	系统需要	直接拨打任何电话号码	允许应用程序拨打任何电话号码,包括紧急电话号码,而无需您的干预。恶意应用程序可能会向紧急服务发出非必要和非法的呼叫

android.permission.CAPTURE_AUDIO_OUTPUT	系统需要		允许应用程序捕获音频输出。
android.permission.CAPTURE_SECURE_VIDEO_OUTPUT	正常		允许应用程序捕获安全视频输出
android.permission.CAPTURE_VIDEO_OUTPUT	正常		允许应用程序捕获视频输出
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.PROCESS_OUTGOING_CALLS	危险	拦截拨出电话	允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话
android.permission.READ_CALENDAR	危险	读取日历事件	允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.READ_LOGS	危	读取敏感日	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做

android.permission.READ_LOGS	危险	日志数据	什么的一般信息,可能包括个人或私人信息
android.permission.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
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定数据。恶意应用可能会损坏你的系统的配置。

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。