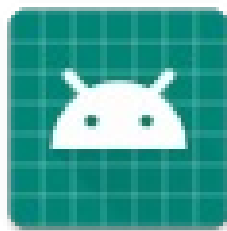




MoGua

USB OTG Camera 1.0.42.APK 分析报告



APP名称:

USB OTG Camera

包名:	com.aplus.otgcamera
域名线索:	24条
URL线索:	35条
邮箱线索:	2条
分析日期:	2025年8月2日
分析平台:	摸瓜APK反编译平台

文件名: USB OTG Camera_v1.0.42.apk
文件大小: 5.72MB
MD5值: 03ced48f72837077bac56a6a7e6e1c98
SHA1值: 63f79cdf8f591319ae79d230ae6c231a1c054fea
SHA256值: 56047d3f616c5518a9ee3d1efd14778648f35c901c867384584ddaef4f634d3d

i APP 信息

App名称: USB OTG Camera
包名: com.aplus.otgcamera
主活动Activity: com.aplus.otgcamera.activity.MainActivity
安卓版本名称: 1.0.42
安卓版本: 42

🔍 域名线索

域名	服务器信息
cgi.connect.qq.com	IP: 175.27.9.14 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
service.weibo.com	IP: 49.7.40.137 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
	IP: 49.7.37.118 所属国家: China 地区: Beijing

open.weibo.cn	城市: Beijing 纬度: 39.907501 经度: 116.397232
www.sina.com	IP: 49.7.37.60 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
appsupport.qq.com	IP: 175.27.9.43 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
ug.edm.weibo.cn	IP: 49.7.37.77 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
github.com	IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
www.microdvrcamera.com	IP: 50.87.237.60 所属国家: United States of America 地区: Utah 城市: Provo 纬度: 40.213909 经度: -111.634071

long.open.weixin.qq.com	IP: 109.244.216.15 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
play.google.com	IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig 纬度: 52.265942 经度: 10.526730
login.imgcache.qq.com	IP: 182.254.59.164 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298
fusion.qq.com	IP: 175.27.9.125 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
xz.3g-gifts.com	IP: 98.143.158.89 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
huatuocode.huatuo.qq.com	没有服务器地理信息.
	IP: 49.7.40.136 所属国家: China

api.weibo.cn	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
libusb.info	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
api.weibo.com	IP: 49.7.37.118 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
www.microdvrcamera.cn	IP: 47.107.78.61 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
mta.oa.com	IP: 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690
cgi.qplus.com	没有服务器地理信息.
mta.qq.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000

	经度: 0.000000
open.weixin.qq.com	IP: 175.24.209.30 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
pingma.qq.com	IP: 119.45.78.184 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
openmobile.qq.com	IP: 175.27.9.14 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

 URL线索

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java

https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
http://www.sina.com	com/aplus/updatelibrary/Constants.java
http://xz.3g-gifts.com	com/aplus/updatelibrary/BaseUrls.java
http://xz.3g-gifts.com/version.config.js	com/aplus/updatelibrary/BaseUrls.java
https://play.google.com/store/apps/details?id=	com/aplus/otgcamera/activity/MainActivity.java
http://www.microdvrcamera.cn	com/aplus/otgcamera/activity/MainActivity.java
http://www.microdvrcamera.com	com/aplus/otgcamera/activity/MainActivity.java
http://www.microdvrcamera.cn	com/aplus/otgcamera/activity/MainActivityBackup.java
http://www.microdvrcamera.com	com/aplus/otgcamera/activity/MainActivityBackup.java
https://api.weibo.com/2/proxy/sdk/statistic.json	com/sina/weibo/sdk/statistic/LogReport.java
https://api.weibo.com/oauth2/getaid.json	com/sina/weibo/sdk/utils/AidTask.java
http://service.weibo.com/share/mobilesdk.php	com/sina/weibo/sdk/web/param/ShareWebViewRequestParam.java
http://service.weibo.com/share/mobilesdk_uppic.php	com/sina/weibo/sdk/web/param/ShareWebViewRequestParam.java
https://ug.edm.weibo.cn/api/gettoken	com/sina/weibo/sdk/network/intercept/RequestTokenInterception.java
https://ug.edm.weibo.cn/api/refresh token	com/sina/weibo/sdk/network/intercept/RequestTokenInterception.java
https://api.weibo.cn/2/sdk/login	com/sina/weibo/sdk/network/intercept/CommonParamInterception.java

https://api.weibo.cn/2/sdk/login	com/sina/weibo/sdk/network/intercept/GuestParamInterception.java
http://api.weibo.cn/2/sdk/login	com/sina/weibo/sdk/network/intercept/GuestParamInterception.java
https://api.weibo.com/oauth2/access_token	com/sina/weibo/sdk/auth/AccessTokenKeeper.java
https://open.weibo.cn/oauth2/authorize?	com/sina/weibo/sdk/auth/BaseSsoHandler.java
https://openmobile.qq.com/oauth2.0/me	com/tencent/connect/UnionInfo.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1\$s&from=%2\$s&isOpenAppID=1	com/tencent/connect/share/QQShare.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1\$s&from=%2\$s&isOpenAppID=1	com/tencent/connect/share/QzoneShare.java
http://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/connect/common/BaseApi.java
http://login.imgcache.qq.com/ptlogin/static/qzsjump.html?	com/tencent/connect/common/BaseApi.java
https://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/user/user_login_statis	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/v3/user/get_info	com/tencent/connect/auth/AuthAgent.java
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	com/tencent/connect/auth/AuthAgent.java
http://login.imgcache.qq.com/ptlogin/static/qzsjump.html?	com/tencent/connect/auth/a.java
http://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java

http://login.imgcache.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApilml.java
http://login.imgcache.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/SocialApilml.java
http://login.imgcache.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/SocialApilml.java
http://login.imgcache.qq.com	com/tencent/open/SocialApilml.java
https://openmobile.qq.com/cgi-bin/qunopensdk/unbind	com/tencent/open/SocialOperation.java
https://openmobile.qq.com/cgi-bin/qunopensdk/check_group	com/tencent/open/SocialOperation.java
http://cgi.qplus.com/report/report	com/tencent/open/utils/k.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utils/f.java
https://huatuocode.huatuo.qq.com	com/tencent/open/a/d.java
http://open.weixin.qq.com/connect/sdk/qrconnect? appid=%s&noncestr=%s×tamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
http://libusb.info	lib/armeabi/libusb100.so

邮箱线索

邮箱地址	所在文件
t_saki@serenegiant.com	com/serenegiant/utils/CrashExceptionHandler.java
liwei31@staff.weibo	com/sina/weibo/sdk/network/intercept/RequestTokenInterception.java

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2020-10-19 08:35:43+00:00
有效期至: 2050-10-19 08:35:43+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x3c44ae3b565bf63baddafdeaf4e1f576005a4b73
哈希算法: sha256
md5值: 16798de0e0427a2e27ef0bcbcb214c082
sha1值: c3ecfe37ce64340cc2e4944c7330e587c55dc69a
sha256值: 89b5e7b3909078d8e99ed03f446168fa73ccf94e4499e44b888a0cbd8a6dfa4a
sha512值: 5516534271047d3aa0dc55c5de209e8588f21251bbe5ced4fbbbf2b67f41798ac74f62f9a41877a1b2417ae70de99e3c85d7ce164e0ba0a702486ac45c744886
公钥算法: rsa
密钥长度: 4096
指纹: 1a0d1b4f0b3607cbc63e0ec329cf8ff8e128086d7e725708eeb2f3062742ca7a

硬编码敏感信息

可能的敏感信息
"cancel_auth" : "授权取消"
"com_facebook_device_auth_instructions" : "Visit facebook.com/device and enter the code shown above."
"com_facebook_device_auth_instructions" : "请访问 facebook.com/device 并输入以上验证码。"

"com_facebook_device_auth_instructions" : "请访问facebook.com/device并输入以上验证码。"
"com_facebook_device_auth_instructions" : "前往facebook.com/device, 並輸入上方顯示的代碼。"
"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og indtast koden, som er vist ovenfor."
"com_facebook_device_auth_instructions" : "facebook.com/deviceにアクセスして、上のコードを入力してください。"
"com_facebook_device_auth_instructions" : "facebook.com/device 'ਤੇ ਵਿਜ਼ਿਟ ਕਰੋ ਅਤੇ ਉੱਪਰ ਦਿੱਤੇ ਕੋਡ ਨੂੰ ਦਾਖ਼ਲ ਕਰੋ।"
"com_facebook_device_auth_instructions" : "facebook.com/device ஐப் பார்வையிட்டு, மேலே காட்டப்பட்ட குறியீட்டை உள்ளிடவும்."
"com_facebook_device_auth_instructions" : "[Visit facebook.com/device and enter the code shown above.#f385b026d401b4f2ebba4fa58eb02bd1:1]"
"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og skriv inn koden som vises over."
"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di atas."
"com_facebook_device_auth_instructions" : "Gehe zu facebook.com/device und gib den oben angezeigten Code ein."
"com_facebook_device_auth_instructions" : "facebook.com/device సందర్శించి ఎగువన చూపిన కోడ్‌ను నమోదు చేయండి."
"com_facebook_device_auth_instructions" : "Besoek facebook.com/device en voer die kode wat hierbo gewys word, in."
"com_facebook_device_auth_instructions" : "ไปที่ facebook.com/device แล้วป้อนรหัสที่ปรากฏด้านล่าง"
"cancel_auth" : "授权取消"
"com_facebook_device_auth_instructions" : "Siirry osoitteeseen facebook.com/device ja anna oheinen koodi."
"com_facebook_device_auth_instructions" : "facebook.com/device पर विज़िट करें और ऊपर दिखाया गया कोड डालें."
"com_facebook_device_auth_instructions" : "Truy cập facebook.com/device và nhập mã được hiển thị bên trên."
"com_facebook_device_auth_instructions" : "Navštívte stránku facebook.com/device a zadajte kód zobrazený vyššie."

"com_facebook_device_auth_instructions" : "Πηγαίνετε στη διεύθυνση facebook.com/device και εισαγάγετε τον παραπάνω κωδικό."
"com_facebook_device_auth_instructions" : "facebook.com/device സന്ദർശിച്ച് മുകളിൽ കാണിച്ചിരിക്കുന്ന കോഡ് നൽകുക."
"com_facebook_device_auth_instructions" : "Ga naar facebook.com/device en voer de bovenstaande code in."
"com_facebook_device_auth_instructions" : "Odwiedź stronę facebook.com/device i wprowadź powyższy kod."
"com_facebook_device_auth_instructions" : "Puntahan ang facebook.com/device at ilagay ang code na ipinapakita sa itaas."
"com_facebook_device_auth_instructions" : "facebook.com/device দেখুন এবং উপরে দেখানো কোডটিকে প্রবেশ করান।"
"cancel_auth" : "Authorization cancelled"
"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di bawah ini."
"com_facebook_device_auth_instructions" : "facebook.com/device ಗೆ ಭೇಟಿ ನೀಡಿ ಮತ್ತು ಮೇಲೆ ತೋರಿಸಿದ ಕೋಡ್ ಅನ್ನು ನಮೂದಿಸಿ."
"com_facebook_device_auth_instructions" : "facebook.com/device에 방문하여 위 코드를 입력하세요."
"com_facebook_device_auth_instructions" : "Vizitează facebook.com/device și introdu codul de mai sus."
"com_facebook_device_auth_instructions" : "وإدخال الرمز الموضح أعلاه facebook.com/device تفضل بزيارة."
"com_facebook_device_auth_instructions" : "Consultez facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "Posjetitw facebook.com/device i unesite gore prikazani kôd."
"com_facebook_device_auth_instructions" : "facebook.com/device भेट द्या आणि वरील कोड प्रविष्ट करा."
"com_facebook_device_auth_instructions" : "facebook.com/device adresine git ve yukarıda gösterilen kodu gir."
"com_facebook_device_auth_instructions" : "Přejděte na facebook.com/device a zadejte nahoře uvedený kód."

"com_facebook_device_auth_instructions" : "Ve a facebook.com/device e ingresa el código que se muestra arriba."
"com_facebook_device_auth_instructions" : "Lawati facebook.com/device dan masukkan kod yang ditunjukkan di atas."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e inserisci il codice mostrato qui sotto."
"com_facebook_device_auth_instructions" : "Acesse facebook.com/device e insira o código mostrado acima."
"com_facebook_device_auth_instructions" : "facebook.com/devicegt ની મુલકાત લો; અને ઉપર આપેલો કોડ દાખલ કરો."
"com_facebook_device_auth_instructions" : "Keresd fel a facebook.com/device címet, és írd be a fent megjelenített kódot."
"com_facebook_device_auth_instructions" : "Откройте facebook.com/device и введите код, показанный выше."
"com_facebook_device_auth_instructions" : "Gå till facebook.com/device och skriv in koden som visas ovan."
"com_facebook_device_auth_instructions" : "ולהזין את הקוד המוצג למעלה facebook.com/devicegt יש לבקר בכתובת"
"com_facebook_device_auth_instructions" : "Accédez à facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "前往facebook.com/devicegt，並輸入上方顯示的代碼。"
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e introduce el código que se muestra más arriba."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e insere o código apresentado abaixo."

🔗 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

向手机申请的权限	是否危险	类型	详细情况
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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.READ_LOGS	危险	读取敏感日志数据	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什么的一般信息,可能包括个人或私人信息
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.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

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: \ 1110220112://,