Evaluation Warning: The document was created with Spire.Doc for Python.

**USB OTG Camera（ 1.0.42版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | USB OTG Camera |
| 版本 | 1.0.42 |
| 包名 | com.aplus.otgcamera |
| 域名线索 | 24条 |
| URL线索 | 35条 |
| APP图标 |  |
| 分析日期 | 2025年8月2日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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  |
| service.weibo.com | IP: 49.7.40.137 所属国家: China 地区: Beijing 城市: Beijing  |
| open.weibo.cn | IP: 49.7.37.118 所属国家: China 地区: Beijing 城市: Beijing  |
| www.sina.com | IP: 49.7.37.60 所属国家: China 地区: Beijing 城市: Beijing  |
| appsupport.qq.com | IP: 175.27.9.43 所属国家: China 地区: Beijing 城市: Beijing  |
| ug.edm.weibo.cn | IP: 49.7.37.77 所属国家: China 地区: Beijing 城市: Beijing  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| www.microdvrcamera.com | IP: 50.87.237.60 所属国家: United States of America 地区: Utah 城市: Provo  |
| long.open.weixin.qq.com | IP: 109.244.216.15 所属国家: China 地区: Beijing 城市: Beijing  |
| play.google.com | IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig  |
| login.imgcache.qq.com | IP: 182.254.59.164 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| fusion.qq.com | IP: 175.27.9.125 所属国家: China 地区: Beijing 城市: Beijing  |
| xz.3g-gifts.com | IP: 98.143.158.89 所属国家: United States of America 地区: California 城市: Los Angeles  |
| huatuocode.huatuo.qq.com | 没有服务器地理信息.  |
| api.weibo.cn | IP: 49.7.40.136 所属国家: China 地区: Beijing 城市: Beijing  |
| libusb.info | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| api.weibo.com | IP: 49.7.37.118 所属国家: China 地区: Beijing 城市: Beijing  |
| www.microdvrcamera.cn | IP: 47.107.78.61 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mta.oa.com | IP: 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| 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: -  |
| open.weixin.qq.com | IP: 175.24.209.30 所属国家: China 地区: Beijing 城市: Beijing  |
| pingma.qq.com | IP: 119.45.78.184 所属国家: China 地区: Beijing 城市: Beijing  |
| openmobile.qq.com | IP: 175.27.9.14 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 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/refreshtoken  | 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/SocialApiIml.java  |
| http://login.imgcache.qq.com/open/mobile/invite/sdk\_invite.html?  | com/tencent/open/SocialApiIml.java  |
| http://login.imgcache.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html?  | com/tencent/open/SocialApiIml.java  |
| http://login.imgcache.qq.com  | com/tencent/open/SocialApiIml.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&timestamp=%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  |

### **4.3 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  |

### **4.4 手机号线索**

## **5. 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: 16798de0e0427a2e27ef0bcbc214c082 sha1值: c3ecfe37ce64340cc2e4944c7330e587c55dc69a sha256值: 89b5e7b3909078d8e99ed03f446168fa73ccf94e4499e44b888a0cbd8a6dfa4a sha512值: 5516534271047d3aa0dc55c5de209e8588f21251bbe5ced4fbbbf2b67f41798ac74f62f9a41877a1b2417ae70de99e3c85d7ce164e0ba0a702486ac45c744886 公钥算法: rsa 密钥长度: 4096 指纹: 1a0d1b4f0b3607cbc63e0ec329cf8ff8e128086d7e725708eeb2f3062742ca7a**

## **6. 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 <b>facebook.com/device</b> and enter the code shown above."  |
| "com\_facebook\_device\_auth\_instructions" : "请访问<b>facebook.com/device</b>并输入以上验证码。"  |
| "com\_facebook\_device\_auth\_instructions" : "前往<b>facebook.com/device</b&gt，並輸入上方顯示的代碼。"  |
| "com\_facebook\_device\_auth\_instructions" : "Gå til <b>facebook.com/device</b> og indtast koden, som er vist ovenfor."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>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" : "<b>facebook.com/device</b> 'ਤੇ ਵਿਜਿਟ ਕਰੋ ਅਤੇ ਉੱਪਰ ਦਿੱਤੇ ਕੋਡ ਨੂੰ ਦਾਖ਼ਲ ਕਰੋ।"  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> ஐப் பார்வையிட்டு, மேலே காட்டப்பட்ட குறியீட்டை உள்ளிடவும்."  |
| "com\_facebook\_device\_auth\_instructions" : "[Visit <b>facebook.com/device</b> and enter the code shown above.#f385b026d401b4f2ebba4fa58eb02bd1:1]"  |
| "com\_facebook\_device\_auth\_instructions" : "Gå til <b>facebook.com/device</b> og skriv inn koden som vises over."  |
| "com\_facebook\_device\_auth\_instructions" : "Kunjungi <b>facebook.com/device</b> dan masukkan kode yang ditampilkan di atas."  |
| "com\_facebook\_device\_auth\_instructions" : "Gehe zu <b>facebook.com/device</b> und gib den oben angezeigten Code ein."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>ని సందర్శించి ఎగువన చూపిన కోడ్‌ను నమోదు చేయండి."  |
| "com\_facebook\_device\_auth\_instructions" : "Besoek <b>facebook.com/device</b> en voer die kode wat hierbo gewys word, in."  |
| "com\_facebook\_device\_auth\_instructions" : "ไปที่ <b>facebook.com/device</b> แล้วป้อนรหัสที่ปรากฏด้านล่าง"  |
| "cancel\_auth" : "授权取消"  |
| "com\_facebook\_device\_auth\_instructions" : "Siirry osoitteeseen <b>facebook.com/device</b> ja anna oheinen koodi."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> पर विज़िट करें और ऊपर दिखाया गया कोड डालें."  |
| "com\_facebook\_device\_auth\_instructions" : "Truy cập <b>facebook.com/device</b> và nhập mã được hiển thị bên trên."  |
| "com\_facebook\_device\_auth\_instructions" : "Navštívte stránku <b>facebook.com/device</b> a zadajte kód zobrazený vyššie."  |
| "com\_facebook\_device\_auth\_instructions" : "Πηγαίνετε στη διεύθυνση <b>facebook.com/device</b> και εισαγάγετε τον παραπάνω κωδικό."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> സന്ദർശിച്ച് മുകളിൽ കാണിച്ചിരിക്കുന്ന കോഡ് നൽകുക."  |
| "com\_facebook\_device\_auth\_instructions" : "Ga naar <b>facebook.com/device</b> en voer de bovenstaande code in."  |
| "com\_facebook\_device\_auth\_instructions" : "Odwiedź stronę <b>facebook.com/device</b> i wprowadź powyższy kod."  |
| "com\_facebook\_device\_auth\_instructions" : "Puntahan ang <b>facebook.com/device</b> at ilagay ang code na ipinapakita sa itaas."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> দেখুন এবং উপরে দেখানো কোডটিকে প্রবেশ করান৷"  |
| "cancel\_auth" : "Authorization cancelled"  |
| "com\_facebook\_device\_auth\_instructions" : "Kunjungi <b>facebook.com/device</b> dan masukkan kode yang ditampilkan di bawah ini."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> ಗೆ ಭೇಟಿ ನೀಡಿ ಮತ್ತು ಮೇಲೆ ತೋರಿಸಿದ ಕೋಡ್ ಅನ್ನು ನಮೂದಿಸಿ."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b>에 방문하여 위 코드를 입력하세요."  |
| "com\_facebook\_device\_auth\_instructions" : "Vizitează <b>facebook.com/device</b> şi introdu codul de mai sus."  |
| "com\_facebook\_device\_auth\_instructions" : "تفضل بزيارة <b>facebook.com/device</b> وإدخال الرمز الموضح أعلاه."  |
| "com\_facebook\_device\_auth\_instructions" : "Consultez <b>facebook.com/device</b> et entrez le code affiché ci-dessus."  |
| "com\_facebook\_device\_auth\_instructions" : "Posjetitw <b>facebook.com/device</b> i unesite gore prikazani kôd."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> भेट द्या आणि वरील कोड प्रविष्ट करा."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b> adresine git ve yukarıda gösterilen kodu gir."  |
| "com\_facebook\_device\_auth\_instructions" : "Přejděte na <b>facebook.com/device</b> a zadejte nahoře uvedený kód."  |
| "com\_facebook\_device\_auth\_instructions" : "Ve a <b>facebook.com/device</b> e ingresa el código que se muestra arriba."  |
| "com\_facebook\_device\_auth\_instructions" : "Lawati <b>facebook.com/device</b> dan masukkan kod yang ditunjukkan di atas."  |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e inserisci il codice mostrato qui sotto."  |
| "com\_facebook\_device\_auth\_instructions" : "Acesse <b>facebook.com/device</b> e insira o código mostrado acima."  |
| "com\_facebook\_device\_auth\_instructions" : "<b>facebook.com/device</b&gt ની મુલકાત લો; અને ઉપર આપેલો કોડ દાખલ કરો."  |
| "com\_facebook\_device\_auth\_instructions" : "Keresd fel a <b>facebook.com/device</b> címet, és írd be a fent megjelenített kódot."  |
| "com\_facebook\_device\_auth\_instructions" : "Откройте <b>facebook.com/device</b> и введите код, показанный выше."  |
| "com\_facebook\_device\_auth\_instructions" : "Gå till <b>facebook.com/device</b> och skriv in koden som visas ovan."  |
| "com\_facebook\_device\_auth\_instructions" : "יש לבקר בכתובת facebook.com/device</b&gt ולהזין את הקוד המוצג למעלה"  |
| "com\_facebook\_device\_auth\_instructions" : "Accédez à <b>facebook.com/device</b> et entrez le code affiché ci-dessus."  |
| "com\_facebook\_device\_auth\_instructions" : "前往<b>facebook.com/device</b&gt，並輸入上方顯示的代碼。"  |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e introduce el código que se muestra más arriba."  |
| "com\_facebook\_device\_auth\_instructions" : "Visita <b>facebook.com/device</b> e insere o código apresentado abaixo."  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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\_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 |

## **10. 应用内通信**

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

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