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

**XS Group（ 3.1.1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 | XS Group |
| 版本 | 3.1.1 |
| 包名 | com.xjlolbwpixdd.app |
| 域名线索 | 13条 |
| URL线索 | 7条 |
| APP图标 |  |
| 分析日期 | 2024年10月18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 | base.apk |
| 文件大小 | 16.82MB |
| MD5值 | d9cde597b45843eb5a32e4e326be9c4e |
| SHA1值 | bf25a620471821846e1538cb32b358d6fdf09f77 |
| SHA256值 | c56716e98928b5e53313246ee2abc0588be319549c4a4491bd5e1222c6a21788 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | XS Group |
| 包名 | com.xjlolbwpixdd.app |
| 主活动Activity | com.jsjt2hk.app.MainActivity |
| 安卓版本名称 | 3.1.1 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| xiangyu-macau.oss-cn-hongkong.aliyuncs.com | IP: 47.79.65.158 所属国家: United States of America 地区: California 城市: San Mateo  |
| www.example.com | IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| hupun-pc.oss-cn-hangzhou.aliyuncs.com | IP: 47.110.178.113 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| store-order.oss-cn-shanghai.aliyuncs.com | IP: 106.14.228.189 所属国家: China 地区: Shanghai 城市: Shanghai  |
| whb-oss.oss-cn-shanghai.aliyuncs.com | IP: 106.14.228.116 所属国家: China 地区: Shanghai 城市: Shanghai  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| developer.android.com | IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.ibm.com | IP: 23.13.189.250 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| greatsea.oss-cn-beijing.aliyuncs.com | IP: 39.97.203.97 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| xsjt-hk-1323860845.cos.ap-hongkong.myqcloud.com | IP: 43.128.240.61 所属国家: Japan 地区: Tokyo 城市: Tokyo  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/g.java  |
| https://github.com/pichillilorenzo/flutter\_inappwebview  | com/pichillilorenzo/flutter\_inappwebview/in\_app\_webview/FlutterWebView.java  |
| https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects\n\n\n  | com/pichillilorenzo/flutter\_inappwebview/in\_app\_webview/FlutterWebView.java  |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |
| https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html  | lib/armeabi-v7a/libapp.so  |
| http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd  | lib/armeabi-v7a/libapp.so  |
| https://whb-oss.oss-cn-shanghai.aliyuncs.com/r/cms/jquery-1.10.2.min.js  | lib/armeabi-v7a/libapp.so  |
| https://greatsea.oss-cn-beijing.aliyuncs.com/assets/js/modernizr.js  | lib/armeabi-v7a/libapp.so  |
| https://hupun-pc.oss-cn-hangzhou.aliyuncs.com/js/aos.js  | lib/armeabi-v7a/libapp.so  |
| https://xiangyu-macau.oss-cn-hongkong.aliyuncs.com/amucsite/freePaper/pc/static/js/index.js  | lib/armeabi-v7a/libapp.so  |
| https://store-order.oss-cn-shanghai.aliyuncs.com/bootstrap.min.css  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| https://xsjt-hk-1323860845.cos.ap-hongkong.myqcloud.com/jquery.js  | lib/armeabi-v7a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/armeabi-v7a/libapp.so  |
| https://github.com/flutter/flutter/issues/new.  | lib/armeabi-v7a/libapp.so  |
| https://github.com/flutter/flutter/issues.  | lib/armeabi-v7a/libflutter.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |
| w@9lpbq.ec \_double@0150898.fromintege \_growablelist@0150898.\_literal \_casterror@0150898.\_create \_immutablelist@0150898.\_ak \_typeerror@0150898.\_create \_bytebuffer@7027147.\_new \_assertionerror@0150898.\_create  | lib/armeabi-v7a/libapp.so  |

### **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=KO, ST=IA, L=JD, O=QV, OU=HB, CN=AH 签名算法: rsassa\_pkcs1v15 有效期自: 2024-05-13 03:08:47+00:00 有效期至: 2051-09-29 03:08:47+00:00 发行人: C=KO, ST=IA, L=JD, O=QV, OU=HB, CN=AH 序列号: 0x72b839d8 哈希算法: sha256 md5值: 77f7e46bb95c57c29a8b1f9781e04ca7 sha1值: 869fe5f0d11bcf25842254b67a7dc8b7d1706186 sha256值: e72f155b12fa9ff3f6804c47a707499808cceb9f90adfaadbddde3d63f788c3d sha512值: 73b0be1e805bbc82dfbbcff4982d836f314e0589144d6636409998fdd60464db0a3ac2d49459e8763a36168def6abcb9f1a04e9619848f1886c83326ee431d4e 公钥算法: rsa 密钥长度: 2048 指纹: 4b3a29a3b8dcd9917865cce37f43a93d2ac6d919b316080592be7cc3f785e071**

## **6. 硬编码敏感信息**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.VIDEO\_CAPTURE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.AUDIO\_CAPTURE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| com.jsjt2hk.app.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**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。**