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

**极简桌面（ 3.1.29.20220903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 | 极简桌面 |
| 版本 | 3.1.29.20220903 |
| 包名 | com.jeejen.family |
| 域名线索 | 67条 |
| URL线索 | 113条 |
| APP图标 |  |
| 分析日期 | 2025年6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 | com.jeejen.family\_3.1.29.20220903.apk |
| 文件大小 | 25.86MB |
| MD5值 | ac7606a74610e488a93091e82dfd3494 |
| SHA1值 | a08cefe69b5c4d9f37d4cf39458ec4af80289ef0 |
| SHA256值 | b53e43853f78d3c5676fd1cd9c97e5277350cc018549b1c1f4d15a17dcb27121 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 极简桌面 |
| 包名 | com.jeejen.family |
| 主活动Activity | com.jeejen.home.launcher.Launcher |
| 安卓版本名称 | 3.1.29.20220903 |
| 安卓版本 | 31029 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| family.jeejen.com | IP: 47.94.233.242 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| voicecloud.cn | 没有服务器地理信息.  |
| unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| shop.jeejen.com | IP: 47.94.233.242 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| weather.jeejen.com | IP: 47.94.233.242 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dev.voicecloud.cn | IP: 114.118.65.97 所属国家: China 地区: Beijing 城市: Beijing  |
| maps.google.com | IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| health.jeejen.com | IP: 47.94.233.242 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.map.baidu.com | IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing  |
| gallery.demo.jeejen.com | IP: 146.56.248.213 所属国家: China 地区: Beijing 城市: Beijing  |
| itsdata.map.baidu.com | IP: 111.206.209.180 所属国家: China 地区: Beijing 城市: Beijing  |
| apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| sdk.open.talk.igexin.com | IP: 124.160.124.156 所属国家: China 地区: Zhejiang 城市: Wenzhou  |
| social.msdn.microsoft.com | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| plugin.jeejen.com.w.kunlunca.com | IP: 61.48.83.229 所属国家: China 地区: Beijing 城市: Beijing  |
| www.xunfei.cn | IP: 123.125.46.38 所属国家: China 地区: Beijing 城市: Beijing  |
| s.sz.gt.igexin.com | IP: 124.160.155.61 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| cgicol.amap.com | IP: 110.253.188.148 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| www.google.com | IP: 199.16.158.182 所属国家: United States of America 地区: California 城市: San Francisco  |
| openapi.openspeech.cn | IP: 125.254.169.47 所属国家: China 地区: Beijing 城市: Beijing  |
| sdkconfig.ad.intl.xiaomi.com | IP: 47.236.194.71 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.iana.org | IP: 192.0.33.8 所属国家: United States of America 地区: California 城市: El Segundo  |
| sdk.open.talk.gepush.com | IP: 124.160.146.190 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| astore.demo.jeejen.com | IP: 146.56.248.213 所属国家: China 地区: Beijing 城市: Beijing  |
| 4f1ce6750872d196da07ad1f1ad42079.iflysec.com | IP: 103.8.33.178 所属国家: China 地区: Anhui 城市: Hefei  |
| restapi.amap.com | IP: 106.11.43.113 所属国家: China 地区: Beijing 城市: Beijing  |
| sdk.open.lbs.igexin.com | IP: 121.52.255.89 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.ad.xiaomi.com | IP: 221.194.175.244 所属国家: China 地区: Hebei 城市: Langfang  |
| sd.cname3.getui.com | IP: 124.160.146.190 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| daup.map.baidu.com | IP: 110.242.74.236 所属国家: China 地区: Hebei 城市: Baoding  |
| wke.openspeech.cn | 没有服务器地理信息.  |
| astore.jeejen.com | IP: 47.94.233.242 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| help.m.jeejen.com | IP: 47.94.233.242 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| logconf.iflytek.com | IP: 103.8.33.178 所属国家: China 地区: Anhui 城市: Hefei  |
| www.jeejen.com | IP: 39.107.117.235 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| pingma.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| sdk.open.phone.igexin.com | IP: 124.160.155.42 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| plugin.demo.jeejen.com | IP: 146.56.248.213 所属国家: China 地区: Beijing 城市: Beijing  |
| gallery.jeejen.com | IP: 47.94.233.242 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| sdkconfig.ad.xiaomi.com | IP: 111.206.174.238 所属国家: China 地区: Beijing 城市: Beijing  |
| push.jeejen.com | IP: 47.94.233.242 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| d.gt.igexin.com | 没有服务器地理信息.  |
| jsperf.com | IP: 104.16.227.18 所属国家: United States of America 地区: California 城市: San Francisco  |
| plugin.jeejen.com | IP: 61.48.83.229 所属国家: China 地区: Beijing 城市: Beijing  |
| ali-008.jeejen.com | IP: 47.94.233.242 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| co.jeejen.com | IP: 0.0.0.0 所属国家: - 地区: - 城市: -  |
| sdk.open.amp.igexin.com | IP: 124.160.124.197 所属国家: China 地区: Zhejiang 城市: Wenzhou  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| health.jeejen.coms | 没有服务器地理信息.  |
| log.iflytek.com | IP: 103.8.33.178 所属国家: China 地区: Anhui 城市: Hefei  |
| sdk.open.inc2.igexin.com | 没有服务器地理信息.  |
| mta.oa.com | IP: 141.144.196.217 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| conf.jeejen.com | IP: 39.106.24.111 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| shop.demo.jeejen.com | IP: 146.56.248.213 所属国家: China 地区: Beijing 城市: Beijing  |
| dev.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| sdk.open.talk.getui.net | IP: 124.160.124.156 所属国家: China 地区: Zhejiang 城市: Wenzhou  |
| bugs.sun.com | IP: 23.218.26.231 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| android.health.jeejen.com | IP: 47.94.233.242 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| c.sz.gt.igexin.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: -  |
| loc.map.baidu.com | IP: 111.206.209.174 所属国家: China 地区: Beijing 城市: Beijing  |
| www.anttna.com | IP: 58.221.60.89 所属国家: China 地区: Jiangsu 城市: Nantong  |
| test.ad.xiaomi.com | IP: 111.206.174.192 所属国家: China 地区: Beijing 城市: Beijing  |
| ofloc.map.baidu.com | IP: 110.242.70.118 所属国家: China 地区: Hebei 城市: Baoding  |
| iss.openspeech.cn | IP: 42.62.43.145 所属国家: China 地区: Beijing 城市: Beijing  |
| www.slf4j.org | IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://api.map.baidu.com/sdkcs/verify  | com/baidu/lbsapi/auth/LBSAuthManager.java  |
| https://loc.map.baidu.com/cc.php  | com/baidu/location/b/g.java  |
| https://ofloc.map.baidu.com/locnu  | com/baidu/location/b/v.java  |
| https://itsdata.map.baidu.com/long-conn-gps/sdk.php  | com/baidu/location/b/i.java  |
| https://loc.map.baidu.com/cfgs/loc/commcfgs  | com/baidu/location/b/a.java  |
| http://loc.map.baidu.com/sdk.php  | com/baidu/location/e/j.java  |
| http://loc.map.baidu.com/user\_err.php  | com/baidu/location/e/j.java  |
| http://loc.map.baidu.com/oqur.php  | com/baidu/location/e/j.java  |
| https://loc.map.baidu.com/tcu.php  | com/baidu/location/e/j.java  |
| http://loc.map.baidu.com/rtbu.php  | com/baidu/location/e/j.java  |
| http://loc.map.baidu.com/iofd.php  | com/baidu/location/e/j.java  |
| http://loc.map.baidu.com/wloc  | com/baidu/location/e/j.java  |
| https://loc.map.baidu.com/sdk\_ep.php  | com/baidu/location/e/j.java  |
| https://loc.map.baidu.com/sdk.php  | com/baidu/location/e/j.java  |
| https://daup.map.baidu.com/cltr/rcvr  | com/baidu/location/e/j.java  |
| http://apilocate.amap.com/mobile/binary  | com/aps/t.java  |
| http://apilocate.amap.com/mobile/binary  | com/aps/l.java  |
| http://cgicol.amap.com/collection/writedata?ver=v1.0\_ali&  | com/aps/l.java  |
| http://restapi.amap.com/v3/weather/weatherInfo?  | com/amap/api/location/b.java  |
| http://restapi.amap.com/log/init  | com/amap/api/location/core/a.java  |
| http://dev.voicecloud.cn/msc/help.html\  | com/iflytek/cloud/resource/b.java  |
| http://dev.voicecloud.cn/msc/help.html  | com/iflytek/cloud/resource/b.java  |
| http://dev.voicecloud.cn/msc/help.html\  | com/iflytek/cloud/resource/c.java  |
| http://dev.voicecloud.cn/msc/help.html  | com/iflytek/cloud/resource/c.java  |
| http://dev.voicecloud.cn/msc/help.html\  | com/iflytek/cloud/resource/a.java  |
| http://dev.voicecloud.cn/msc/help.html  | com/iflytek/cloud/resource/a.java  |
| http://www.xunfei.cn/?appid=  | com/iflytek/cloud/ui/a.java  |
| http://wke.openspeech.cn/wakeup/  | com/iflytek/cloud/a/d/d.java  |
| http://openapi.openspeech.cn/webapi/wfr.do  | com/iflytek/cloud/c/a/b.java  |
| http://iss.openspeech.cn/v?  | com/iflytek/speech/UtilityConfig.java  |
| https://logconf.iflytek.com/hotupdate  | com/iflytek/idata/extension/a.java  |
| https://log.iflytek.com/log  | com/iflytek/idata/extension/c.java  |
| http://sdk.open.inc2.igexin.com/api.php  | com/igexin/getuiext/data/Consts.java  |
| http://sdk.open.phone.igexin.com/api.php  | com/igexin/getuiext/data/Consts.java  |
| http://sdk.open.phone.igexin.com/api.php?format=json&t=1  | com/igexin/getuiext/service/i.java  |
| http://c.sz.gt.igexin.com/api.php  | com/igexin/push/config/SDKUrlConfig.java  |
| http://s.sz.gt.igexin.com/api.php  | com/igexin/push/config/SDKUrlConfig.java  |
| http://d.gt.igexin.com/api.htm  | com/igexin/push/config/SDKUrlConfig.java  |
| http://sdk.open.amp.igexin.com/api.htm  | com/igexin/push/config/SDKUrlConfig.java  |
| http://sdk.open.lbs.igexin.com/api.htm  | com/igexin/push/config/SDKUrlConfig.java  |
| http://bi.  | com/igexin/push/config/o.java  |
| http://config.  | com/igexin/push/config/o.java  |
| http://stat.  | com/igexin/push/config/o.java  |
| http://log.  | com/igexin/push/config/o.java  |
| http://amp.  | com/igexin/push/config/o.java  |
| http://lbs.  | com/igexin/push/config/o.java  |
| http://inc.  | com/igexin/push/config/o.java  |
| http://conf.jeejen.com/family/app/  | com/jeejen/common/updater/FcocUpdateEngine.java  |
| https://www.jeejen.com/user-agreement.html  | com/jeejen/home/launcher/Launcher.java  |
| https://www.jeejen.com/privacy-notice.html  | com/jeejen/home/launcher/Launcher.java  |
| https://www.jeejen.com/privacy-notice.html  | com/jeejen/home/launcher/SettingsActivity.java  |
| https://www.jeejen.com/user-agreement.html  | com/jeejen/home/launcher/SettingsActivity.java  |
| http://co.jeejen.com/crash  | com/jeejen/gallery/biz/Consts.java  |
| http://co.jeejen.com/log  | com/jeejen/gallery/biz/Consts.java  |
| http://plugin.jeejen.com/repo/gpl.r.%s.json  | com/jeejen/lam/model/LamConst.java  |
| http://plugin.jeejen.com/repo/gpl.d.%s.json  | com/jeejen/lam/model/LamConst.java  |
| http://plugin.demo.jeejen.com:8181/repo/gpl.r.%s.json  | com/jeejen/lam/model/LamConst.java  |
| http://plugin.demo.jeejen.com:8181/repo/gpl.d.%s.json  | com/jeejen/lam/model/LamConst.java  |
| http://push.jeejen.com  | com/jeejen/push/util/HttpUtil.java  |
| http://gallery.jeejen.com  | com/jeejen/pushcenter/PushCenterApplication.java  |
| http://gallery.demo.jeejen.com:8181  | com/jeejen/pushcenter/PushCenterApplication.java  |
| http://weather.jeejen.com/ip\_loc/ip\_loc  | com/jeejen/weather/model/WeatherNet.java  |
| http://weather.jeejen.com/realtimeByJSON  | com/jeejen/weather/model/WeatherNet.java  |
| http://weather.jeejen.com/realtime/%s  | com/jeejen/weather/model/WeatherNet.java  |
| http://weather.jeejen.com/forecast/%s  | com/jeejen/weather/model/WeatherNet.java  |
| http://test.ad.xiaomi.com/  | com/miui/zeus/mimo/sdk/server/d.java  |
| http://api.ad.xiaomi.com/  | com/miui/zeus/mimo/sdk/server/d.java  |
| http://test.ad.xiaomi.com/union/fetchAds  | com/miui/zeus/mimo/sdk/server/d.java  |
| http://api.ad.xiaomi.com/union/fetchAds  | com/miui/zeus/mimo/sdk/server/d.java  |
| http://www.google.com/loc/json  | com/miui/voicerecognizer/common/location/GoogleGetLocation.java  |
| http://www.anttna.com/cell2gps/cell2gps3.php?type=%d&mcc=%d&mnc=%d&lac=%d&cellid=%d  | com/miui/voicerecognizer/common/location/AnttnaGetLocation.java  |
| http://www.anttna.com/cell2gps/cell2gps3.php?type=%d&mcc=%d&mnc=%d&sid=%d&nid=%d&bid=%d  | com/miui/voicerecognizer/common/location/AnttnaGetLocation.java  |
| http://maps.google.com/maps/api/geocode/  | com/miui/voicerecognizer/common/location/GeocodeLocation.java  |
| http://maps.google.com/maps/api/geocode/json?sensor=true&language=zh&latlng=%f,%f  | com/miui/voicerecognizer/common/location/GeocodeLocation.java  |
| http://voicecloud.cn/opv1/food.aspx  | com/miui/voicerecognizer/common/net/NetConfig.java  |
| http://www.google.com  | com/ning/http/client/providers/grizzly/GrizzlyAsyncHttpProvider.java  |
| http://bugs.sun.com/view\_bug.do?bug\_id=5103988.  | com/ning/http/multipart/MultipartBody.java  |
| http://mta.qq.com/  | com/tencent/wxop/stat/e.java  |
| http://mta.oa.com/  | com/tencent/wxop/stat/e.java  |
| http://pingma.qq.com:80/mstat/report  | com/tencent/wxop/stat/c.java  |
| https://sdkconfig.ad.xiaomi.com/api/checkupdate/lastusefulversion2?  | com/xiaomi/analytics/a/d.java  |
| https://sdkconfig.ad.intl.xiaomi.com/api/checkupdate/lastusefulversion2?  | com/xiaomi/analytics/a/d.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/MDC.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/LoggerFactory.java  |
| http://co.jeejen.com/update1  | 摸瓜V1引擎  |
| http://co.jeejen.com/crash  | 摸瓜V1引擎  |
| http://health.jeejen.com%s  | 摸瓜V1引擎  |
| http://co.jeejen.com/log  | 摸瓜V1引擎  |
| http://help.m.jeejen.com/gen/cn/cache.txt  | 摸瓜V1引擎  |
| http://help.m.jeejen.com/gen/cn/help.html  | 摸瓜V1引擎  |
| http://health.jeejen.com/downLoad/getPeriodicaJson/%s  | 摸瓜V1引擎  |
| http://family.jeejen.com/promo/get\_current\_flag  | 摸瓜V1引擎  |
| http://shop.jeejen.com/store/download/after  | 摸瓜V1引擎  |
| http://shop.jeejen.com/store/download/before  | 摸瓜V1引擎  |
| http://shop.jeejen.com/store/app  | 摸瓜V1引擎  |
| http://astore.jeejen.com/app\_info.html  | 摸瓜V1引擎  |
| http://shop.jeejen.com/store/install  | 摸瓜V1引擎  |
| http://shop.jeejen.com/store/upgrade  | 摸瓜V1引擎  |
| http://astore.jeejen.com/cache\_policy.txt  | 摸瓜V1引擎  |
| http://astore.jeejen.com/index.html  | 摸瓜V1引擎  |
| http://android.health.jeejen.com/article.html  | 摸瓜V1引擎  |
| http://android.health.jeejen.com  | 摸瓜V1引擎  |
| http://android.health.jeejen.com/cache\_policy.txt  | 摸瓜V1引擎  |
| http://android.health.jeejen.com/fav.html  | 摸瓜V1引擎  |
| http://android.health.jeejen.com/index.html  | 摸瓜V1引擎  |
| http://android.health.jeejen.com/list.html  | 摸瓜V1引擎  |
| http://android.health.jeejen.com/test.html  | 摸瓜V1引擎  |
| http://health.jeejen.com/downLoad/articleimg/  | 摸瓜V2引擎  |
| http://family.jeejen.com/care';  | 摸瓜V2引擎  |
| http://astore.jeejen.com/img  | 摸瓜V2引擎  |
| http://shop.jeejen.com/store/banner  | 摸瓜V2引擎  |
| http://shop.jeejen.com/store/hotapps  | 摸瓜V2引擎  |
| http://shop.jeejen.com/store/autosearch  | 摸瓜V2引擎  |
| http://shop.jeejen.com/store/search  | 摸瓜V2引擎  |
| http://shop.jeejen.com/store/cat  | 摸瓜V2引擎  |
| http://astore.demo.jeejen.com:8181/img  | 摸瓜V2引擎  |
| http://shop.demo.jeejen.com:8181/store/banner  | 摸瓜V2引擎  |
| http://shop.demo.jeejen.com:8181/store/hotapps  | 摸瓜V2引擎  |
| http://shop.demo.jeejen.com:8181/store/autosearch  | 摸瓜V2引擎  |
| http://shop.demo.jeejen.com:8181/store/search  | 摸瓜V2引擎  |
| http://shop.demo.jeejen.com:8181/store/cat  | 摸瓜V2引擎  |
| http://astore.jeejen.com/app\_info.html  | 摸瓜V2引擎  |
| http://astore.jeejen.com/img/icon\_loading.png  | 摸瓜V2引擎  |
| http://astore.jeejen.com/img/icon\_error.png  | 摸瓜V2引擎  |
| http://astore.jeejen.com/img/icon\_error\_small.png  | 摸瓜V2引擎  |
| http://astore.jeejen.com/img/icon\_upgrade.png  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://jsperf.com/b64tests  | 摸瓜V2引擎  |
| http://server/myapp/index.html  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://social.msdn.microsoft.com/Forums/windowsapps/en-US/a327cf3c-f033-4a54-8b7f-03c56ba3203f/windows-foundation-uri-security-problem  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.iana.org/assignments/character-sets)  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://unicode.org/reports/tr35/tr35-4.html  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| logconf.iflytek.com  | 摸瓜V3引擎  |
| family.jeejen.com  | 摸瓜V3引擎  |
| sdk.open.talk.gepush.com  | 摸瓜V3引擎  |
| sdk.open.talk.getui.net  | 摸瓜V3引擎  |
| 4f1ce6750872d196da07ad1f1ad42079.iflysec.com  | 摸瓜V3引擎  |
| sd.cname3.getui.com  | 摸瓜V3引擎  |
| plugin.jeejen.com  | 摸瓜V3引擎  |
| ali-008.jeejen.com  | 摸瓜V3引擎  |
| sdk.open.talk.igexin.com  | 摸瓜V3引擎  |
| plugin.jeejen.com.w.kunlunca.com  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13065869616  | com/xiaomi/analytics/a/a/e.java  |
| 18438544409  | 摸瓜V2引擎  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=cn, ST=beijing, L=beijing, O=tiao.net, OU=tiao.net, CN=jeejen tiao 签名算法: rsassa\_pkcs1v15 有效期自: 2012-07-13 12:08:03+00:00 有效期至: 2122-01-18 12:08:03+00:00 发行人: C=cn, ST=beijing, L=beijing, O=tiao.net, OU=tiao.net, CN=jeejen tiao 序列号: 0x50000fa3 哈希算法: sha1 md5值: e93d7ab91649b86177ca1cc52603be41 sha1值: 81b245be2a142f92ac311a97f98caa26f6078335 sha256值: 771e08494fd33157d46be7cec338fdc528146902649fdad34f85d93ab6c642e1 sha512值: 9ac08128bd195d66a361ad1369aaa2059ffc18138b3f4957a25de0c4076deeeb784ac742398eb87e6793dcb324af0bcbc3e0b712798e11ba96fc8de86ff065f6 公钥算法: rsa 密钥长度: 1024 指纹: 9dd50400fc8002745644c5ff27414c04861b90027b9f8a4fac135f7f00bc0cd8**

## **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.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\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| android.permission.WRITE\_SMS | 危险 | 编辑短信或彩信 | 允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息 |
| android.permission.SEND\_SMS | 危险 | 发送短信 | 允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价 |
| android.permission.RECEIVE\_SMS | 危险 | 接收短信 | 允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示 |
| 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.Manifest.permission.MODIFY\_PHONE\_STATE | 系统需要 | 修改电话状态 | 允许应用程序控制设备的电话功能。具有此权限的应用程序可以切换网络,打开和关闭电话收音机等,而无需通知您 |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠  | 允许应用程序防止手机进入睡眠状态 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.READ\_CALL\_LOG | 危险 |  | 允许应用程序读取用户的通话日志 |
| android.permission.WRITE\_CALL\_LOG | 危险 |  | 允许应用程序写入（但不读取）用户号召日志数据。 |
| 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.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.RESTART\_PACKAGES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.RECEIVE\_WAP\_PUSH | 危险 | 接收WAP | 允许应用程序接收和处理 WAP 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示 |
| android.permission.RECEIVE\_MMS | 危险 | 接收短信 | 允许应用程序接收和处理彩信。恶意应用程序可能会监视您的消息或将其删除而不向您显示 |
| 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.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.EXPAND\_STATUS\_BAR | 正常 | 展开/折叠状态栏 | 允许应用程序展开或折叠状态栏 |
| android.permission.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| 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.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.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.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| 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.DOWNLOAD\_WITHOUT\_NOTIFICATION | 未知 | Unknown permission | Unknown permission from android reference |
| com.jeejen.client.collector.Collect | 未知 | Unknown permission | Unknown permission from android reference |
| com.jeejen.permission.MIUI\_CONTAINER | 未知 | Unknown permission | Unknown permission from android reference |
| com.jeejen.freecall.permission.FREECALL | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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 |
| getui.permission.GetuiService.com.jeejen.family | 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.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| android.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.jeejen.mms.ui.MmsNewSmsActivity | **Schemes**: sms://, smsto://, mms://, mmsto://, **Mime Types:** vnd.android.cursor.dir/mms, vnd.android-dir/mms-sms, text/\*,  |
| com.jeejen.phone.ui.DialActivity | **Schemes**: voicemail://, tel://, **Mime Types:** vnd.android.cursor.item/phone, vnd.android.cursor.item/person,  |
| com.jeejen.gallery.ui.VideoPortalActivity | **Schemes**: http://, https://, content://, file://, **Mime Types:** video/mpeg4, video/mp4, video/3gp, video/3gpp, video/3gpp2, application/sdp, video/\*, vnd.android.cursor.dir/video,  |
| com.jeejen.gallery.ui.AlbumActivity | **Schemes**: http://, https://, content://, file://, **Mime Types:** vnd.android.cursor.dir/image, image/\*, image/bmp, image/jpeg, image/gif, image/png, image/x-ms-bmp, image/vnd.wap.wbmp,  |
| com.jeejen.gallery.ui.VideoActivity | **Schemes**: rtsp://, http://, https://, content://, file://, **Mime Types:** video/mpeg4, video/mpeg, video/mp4, video/3gp, video/3gpp, video/3gpp2, video/webm, video/avi, video/x-msvideo, application/sdp, audio/x-mpegurl, audio/mpegurl, application/vnd.apple.mpegurl, application/x-mpegurl,  |

**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。**