# MoGua

# 闪电应急 4.1.0.APK 分析报告


| | |
|---|---|
| APP名称: | 闪电应急 |

| | |
|---|---|
| 包名: | com.udcdxz.dzjaetri |
| 域名线索: | 17条 |
| URL线索: | 14条 |
| 邮箱线索: | 0条 |
| 分析日期: | 2025年1月15日 |
| 分析平台: | 摸瓜APK反编译平台 |

## 文件信息

**文件名**: sdyj.apk
**文件大小**: 16.11MB
**MD5值**: 0f1bcf64917615d6ae22b59025ec8756
**SHA1值**: fdbdf4ce0f940655684f494db87b35762ab0bd9d
**SHA256值**: 0ef5e58e350bb228198ea50ae1d94809e3d6c1984e9f29cf534f410fa157d714

# APP 信息

**App名称**: 闪电应急
**包名**: com.udcdxz.dzjaetri
**主活动Activity**: com.sdhay.ui.activitys.JDXF0ACT
**安卓版本名称**: 4.1.0
**安卓版本**: 51

# 域名线索

| 域名 | 服务器信息 |
| --- | --- |
| pop.yuncloudauth.com | **IP**: 106.11.232.147<br>**所属国家**: China<br>**地区**: Zhejiang<br>**城市**: Hangzhou<br>**纬度**: 30.293650<br>**经度**: 120.161583 |
| kjalsdfnanzasdf.s3.ap-southeast-1.amazonaws.com | **IP**: 52.219.125.75<br>**所属国家**: Singapore<br>**地区**: Singapore<br>**城市**: Singapore<br>**纬度**: 1.289987<br>**经度**: 103.850281 |
| www.beizhuabao.com | 没有服务器地理信息. |
| schemas.android.com | 没有服务器地理信息. |

| | |
|---|---|
| axzcvfeq-1324028813.cos.ap-guangzhou.myqcloud.com | **IP**: 36.248.13.149<br>**所属国家**: China<br>**地区**: Fujian<br>**城市**: Fuzhou<br>**纬度**: 26.061390<br>**经度**: 119.306107 |
| cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com | **IP**: 139.227.226.214<br>**所属国家**: China<br>**地区**: Shanghai<br>**城市**: Shanghai<br>**纬度**: 31.224333<br>**经度**: 121.468948 |
| render.alipay.com | **IP**: 182.40.59.241<br>**所属国家**: China<br>**地区**: Shandong<br>**城市**: Qingdao<br>**纬度**: 36.098610<br>**经度**: 120.371941 |
| auth.yunverify.com | **IP**: 106.11.232.147<br>**所属国家**: China<br>**地区**: Zhejiang<br>**城市**: Hangzhou<br>**纬度**: 30.293650<br>**经度**: 120.161583 |
| cloudauth.cn-beijing.aliyuncs.com | **IP**: 39.97.154.134<br>**所属国家**: China<br>**地区**: Zhejiang<br>**城市**: Hangzhou<br>**纬度**: 30.293650<br>**经度**: 120.161583 |
| tianshu.alicdn.com | **IP**: 117.163.61.250<br>**所属国家**: China<br>**地区**: Jiangxi<br>**城市**: Nanchang |

| | |
|---|---|
| | **纬度**: 28.683331<br>**经度**: 115.883331 |
| cloudauth-dualstack.aliyuncs.com | **IP**: 140.205.61.35<br>**所属国家**: China<br>**地区**: Zhejiang<br>**城市**: Hangzhou<br>**纬度**: 30.293650<br>**经度**: 120.161583 |
| cloudauth-dualstack.cn-beijing.aliyuncs.com | **IP**: 8.141.244.37<br>**所属国家**: China<br>**地区**: Zhejiang<br>**城市**: Hangzhou<br>**纬度**: 30.293650<br>**经度**: 120.161583 |
| nice800.com | **IP**: 194.41.36.6<br>**所属国家**: Hong Kong<br>**地区**: Hong Kong<br>**城市**: Hong Kong<br>**纬度**: 22.285521<br>**经度**: 114.157692 |
| mgw.mpaas.cn-hangzhou.aliyuncs.com | **IP**: 47.118.173.135<br>**所属国家**: China<br>**地区**: Zhejiang<br>**城市**: Hangzhou<br>**纬度**: 30.293650<br>**经度**: 120.161583 |
| cloudauth.aliyuncs.com | **IP**: 106.11.232.147<br>**所属国家**: China<br>**地区**: Zhejiang<br>**城市**: Hangzhou<br>**纬度**: 30.293650<br>**经度**: 120.161583 |
| | **IP**: 112.80.252.187 |

| | |
|---|---|
| ljkxcvzsdf-1326613936.cos.ap-nanjing.myqcloud.com | **所属国家**: China<br>**地区**: Jiangsu<br>**城市**: Nanjing<br>**纬度**: 32.061668<br>**经度**: 118.777992 |
| android-donwload.oss-cn-hangzhou.aliyuncs.com | **IP**: 47.110.23.115<br>**所属国家**: China<br>**地区**: Zhejiang<br>**城市**: Hangzhou<br>**纬度**: 30.293650<br>**经度**: 120.161583 |

## URL线索

| URL**信息** | Url**所在文件** |
|---|---|
| http://schemas.android.com/apk/res/android | a/h/e/d/g.java |
| https://cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com/model/toyger.face.dat | c/f/a/n/k.java |
| https://tianshu.alicdn.com/7504f3f0-aca8-4636-b486-e396559d3efb.png | c/f/a/n/k.java |
| http://schemas.android.com/apk/res-auto | c/g/a/a/v/a.java |
| https://android-donwload.oss-cn-hangzhou.aliyuncs.com/domai0dsfnName/5100sdfh0635.text/ | c/j/b/d/a/d.java |
| https://ljkxcvzsdf-1326613936.cos.ap-nanjing.myqcloud.com | c/j/b/d/a/e.java |
| https://axzcvfeq-1324028813.cos.ap-guangzhou.myqcloud.com | c/j/b/d/a/e.java |
| https://kjalsdfnanzasdf.s3.ap-southeast-1.amazonaws.com | c/j/b/d/a/e.java |
| http://www.beizhuabao.com | c/j/b/d/a/a.java |

| | |
|---|---|
| http://www.beizhuabao.com | c/j/b/d/a/b.java |
| https://mgw.mpaas.cn-hangzhou.aliyuncs.com | com/alipay/alipaysecuritysdk/common/config/Configuration.java |
| https://cloudauth-dualstack.aliyuncs.com | com/dtf/face/api/DTFacadeExt.java |
| https://cloudauth.aliyuncs.com | com/dtf/face/api/DTFacadeExt.java |
| https://cloudauth-dualstack.cn-beijing.aliyuncs.com | com/dtf/face/api/DTFacadeExt.java |
| https://cloudauth.cn-beijing.aliyuncs.com | com/dtf/face/api/DTFacadeExt.java |
| https://auth.yunverify.com | com/dtf/face/api/DTFacadeExt.java |
| https://pop.yuncloudauth.com | com/dtf/face/api/DTFacadeExt.java |
| https://render.alipay.com/p/f/fd-j8l9yjja/index.html | com/dtf/face/config/NavigatePage.java |
| https://nice800.com | com/sdhay/ui/activitys/MT7ACT.java |
| https://nice800.com/ | com/sdhay/ui/activitys/MT10ACT.java |
| https://render.alipay.com/p/yuyan/180020010001208736/aliyunFacewelcome.html | 摸瓜V1引擎 |

## 邮箱线索

## 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=nyTiTobH, ST=qxuYgyXz, L=rYHGEoAe, O=wivXoBnZ, OU=nzXIRLvy, CN=miwaoOQi
签名算法: rsassa_pkcs1v15
有效期自: 2024-08-05 09:03:09+00:00
有效期至: 2034-08-03 09:03:09+00:00
发行人: C=nyTiTobH, ST=qxuYgyXz, L=rYHGEoAe, O=wivXoBnZ, OU=nzXIRLvy, CN=miwaoOQi
序列号: 0x3f4c2e8b95933a67
哈希算法: sha256
md5值: c03586bff4cc23dffedb4b21c4f18e78
sha1值: 1c79389b7410ec31a1397e748bd79e57b463dd5c
sha256值: a5c9ebd1ea6c215e478a70ad5fc39a4366a178ce0fc48ae4ff6a93c038f49a41
sha512值: b9d83e4032b4f15f41b027b0e1cb967c6692efe61e3d76e79447232de225fde8023a1c9866e01fbc84e05aa1044b0e5581e07edcf39c3e09d7680ec4c718588c
公钥算法: rsa
密钥长度: 2048
指纹: 1c782d8794a2000de69695295138c34bb97fc91a222792e8b26fbd5b8130d354

# 🔑 硬编码敏感信息

| 可能的敏感信息 |
| --- |
| "agreee_user" : "请先同意并勾选用户协议" |
| "check_gesture_pwd" : "验证手势密码" |
| "check_login_pwd" : "验证登录密码" |
| "dear_user" : "尊敬的用户:" |
| "find_pwd" : "找回密码" |
| "gesture_pwd" : "手势密码" |

| |
|---|
| "has_authd" : "已授权" |
| "info_auth_fee" : "信息认证费： " |
| "info_auth_fee2" : "信息认证费" |
| "input_orgin_pwd" : "请输入原密码" |
| "input_pwd" : "请输入验证码" |
| "input_pwd_number" : "请输入新密码(6-16位数字字母组合)" |
| "modify_pwd" : "修改密码" |
| "ple_agree_auth_agreement" : "请先同意授权及借款协议" |
| "ple_input_service_pwd" : "请输入服务密码" |
| "real_auth" : "实名认证" |
| "reset_service_pwd" : "重置服务密码" |
| "service_pwd" : "服务密码:" |
| "to_authorize" : "去授权" |
| "user" : "用户" |

# 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.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.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_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.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.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.READ_CALL_LOG | 危险 | | 允许应用程序读取用户的通话日志 |
| 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.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.RECORD_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.READ_MEDIA_VISUAL_USER_SELECTED | 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_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |

# 应用内通信

---