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

**闪电应急（ 4.1.0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 | 闪电应急 |
| 版本 | 4.1.0 |
| 包名 | com.udcdxz.dzjaetri |
| 域名线索 | 17条 |
| URL线索 | 14条 |
| APP图标 |  |
| 分析日期 | 2025年1月15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 | sdyj.apk |
| 文件大小 | 16.11MB |
| MD5值 | 0f1bcf64917615d6ae22b59025ec8756 |
| SHA1值 | fdbdf4ce0f940655684f494db87b35762ab0bd9d |
| SHA256值 | 0ef5e58e350bb228198ea50ae1d94809e3d6c1984e9f29cf534f410fa157d714 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| pop.yuncloudauth.com | IP: 106.11.232.147 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| kjalsdfnanzasdf.s3.ap-southeast-1.amazonaws.com | IP: 52.219.125.75 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| 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 所属国家: China 地区: Fujian 城市: Fuzhou  |
| cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com | IP: 139.227.226.214 所属国家: China 地区: Shanghai 城市: Shanghai  |
| render.alipay.com | IP: 182.40.59.241 所属国家: China 地区: Shandong 城市: Qingdao  |
| auth.yunverify.com | IP: 106.11.232.147 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cloudauth.cn-beijing.aliyuncs.com | IP: 39.97.154.134 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| tianshu.alicdn.com | IP: 117.163.61.250 所属国家: China 地区: Jiangxi 城市: Nanchang  |
| cloudauth-dualstack.aliyuncs.com | IP: 140.205.61.35 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cloudauth-dualstack.cn-beijing.aliyuncs.com | IP: 8.141.244.37 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| nice800.com | IP: 194.41.36.6 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| mgw.mpaas.cn-hangzhou.aliyuncs.com | IP: 47.118.173.135 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cloudauth.aliyuncs.com | IP: 106.11.232.147 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ljkxcvzsdf-1326613936.cos.ap-nanjing.myqcloud.com | IP: 112.80.252.187 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| android-donwload.oss-cn-hangzhou.aliyuncs.com | IP: 47.110.23.115 所属国家: China 地区: Zhejiang 城市: Hangzhou  |

### **4.2 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  |

### **4.3 邮箱线索**

### **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=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**

## **6. 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"  |

## **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.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 |

## **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。**