MoGua

防洪排涝 1.1.3.APK 分析报告

APP名称:	防洪排涝

包名:	uni.UNI8B3CE13
域名线索:	6条
URL线索:	17条
邮箱线索:	0条
分析日期:	2025年6月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: fhpl_v1.4.apk
文件大小: 20.55MB
MD5值: 66828a68abbe7e624653af593774f3fc
SHA1值: e6c442a0fde1987d9580557b6bd72f3666a5d794
SHA256值: e7172b6dbb4b0bd2b1c366206b43fdcfa20f3e95294c8da232942a2dcd29d5b8

APP 信息

App名称: 防洪排涝
包名: uni.UNI8B3CE13
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.1.3
安卓版本: 1

域名线索

域名	服务器信息
m3w.cn	**IP**: 221.204.14.81 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
er.dcloud.io	没有服务器地理信息.
schemas.android.com	没有服务器地理信息.
ask.dcloud.net.cn	**IP**: 123.12.235.54 **所属国家**: China **地区**: Henan **城市**: Hebi **纬度**: 35.899170

	经度: 114.192497
er.dcloud.net.cn	IP: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
ns.adobe.com	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/35627	b/a.java
https://ask.dcloud.net.cn/article/35877	b/a.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://ask.dcloud.net.cn/article/283	io/dcloud/feature/utsplugin/ProxyModule.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java

https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://er.dcloud.io/rv	d/c.java
https://er.dcloud.net.cn/rv	d/c.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
https://ask.dcloud.net.cn/article/283	j/b.java

邮箱线索

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

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=, L=, O=Android, OU=Android, CN=wvzbHtrSQIYPfeXf6tmfiaJanVC6FK92ThAk8mPEtwhYHRT0U%2BMMmY3NBkRfqPG9QBUO9amoMDzBoeWYx283dg%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2025-05-23 07:21:13+00:00
有效期至: 2125-04-29 07:21:13+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=wvzbHtrSQIYPfeXf6tmfiaJanVC6FK92ThAk8mPEtwhYHRT0U%2BMMmY3NBkRfqPG9QBUO9amoMDzBoeWYx283dg%3D%3D
序列号: 0x66acf9a5
哈希算法: sha256
md5值: aeeebdabcf50df3d32cd164f106817ec
sha1值: 34b7b31066c82c1ae37b6a42fe552c67c15cc5ae
sha256值: 3fae22bbeb7920b87523ae32b1c4e2147236479e9677f08b742095cadd95807c
sha512值: 39ce45db233ba9c5bcba17a5806e566ffbb13dd57d8e055e794db0528f56ff444e753cce149096c52a282142540defe1085570bcb5dffe51af74cb4f118c6343
公钥算法: rsa
密钥长度: 2048
指纹: 0a02555e93b13ea28c520f1e3437c0e19386c3f561d65c79d968a582fafd734e

硬编码敏感信息

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.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.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_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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
com.asus.msa.SupplementaryDID.ACCESS	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_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。

com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.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.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
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
			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

android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	用程序可以使用它来确定您的大致位置
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

应用内通信
