



MoGua

神州智电 1.0.2.APK 分析报告



APP名称:

神州智电

包名:	plus.H569E8560
域名线索:	7条
URL线索:	6条
邮箱线索:	1条
分析日期:	2025年8月2日
分析平台:	摸瓜APK反编译平台

文件名: 神州智电(1)[1].apk

文件大小: 17.44MB

MD5值: 9e5db800af95488e998132e555d21754

SHA1值: 4e4fb0d00f090d5486263834bc05a2c3a378327c

SHA256值: 8893b686b1a8dca4bb42ed24214b1bf43e44c5c7b7245e3bed297b2ee93ad1d3

i APP 信息

App名称: 神州智电

包名: plus.H569E8560

主活动Activity: io.dcloud.PandoraEntry

安卓版本名称: 1.0.2

安卓版本: 100

🔍 域名线索

域名	服务器信息
bit.ly	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
img01.yzcdn.cn	IP: 221.15.70.53 所属国家: China 地区: Henan 城市: Luoyang 纬度: 34.683289 经度: 112.453911
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California

	城市: San Francisco 纬度: 37.775700 经度: -122.395203
ns.adobe.com	没有服务器地理信息.
schemas.android.com	没有服务器地理信息.
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
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

URL线索

URL信息	Url所在文件
http://ns.adobe.com/xap/1.0\u0000	io/dcloud/common/util/ExifInterface.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java

https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://img01.yzcdn.cn/upload_files/2020/06/24/FmKWDg0bN9rMcTp9ne8MXiQWGtLn.png	摸瓜V2引擎
https://bit.ly/2Zqjzkp	摸瓜V2引擎
https://img01.yzcdn.cn/vant/empty-image-	摸瓜V2引擎
https://img01.yzcdn.cn/vant/coupon-empty.png	摸瓜V2引擎
https://github.com/zloirock/core-js/blob/v3.41.0/LICENSE	摸瓜V2引擎
https://github.com/zloirock/core-js	摸瓜V2引擎
https://img01.yzcdn.cn/vant/share-sheet-	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
jhruby.web@gmail.com	摸瓜V2引擎

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=Country Code, ST=State, L=City, O=Organization, OU=Organizational Unit, CN=Company Name

签名算法: rsassa_pkcs1v15

有效期自: 2025-04-22 11:18:05+00:00

有效期至: 2035-04-20 11:18:05+00:00

发行人: C=Country Code, ST=State, L=City, O=Organization, OU=Organizational Unit, CN=Company Name

序列号: 0x2180ea20b071fb2c

哈希算法: sha256

md5值: dbc89e210ff20bb4a62652596f509cad

sha1值: 5f4e3fc56004e207b29ac688f0b284063c89a307

sha256值: 470a08aca6332ada07a28d955161fdb9660136ee4e9987f3e9fff02ccd40f159

sha512值: 2454a5452667e550602e56b4a23c8c439c74b2423a3d8edd92b3bc9bd40cebe00d0441d23cbd28088c6a60172f443105e0715f5d6ff0b42202a9daccd2552d4b

公钥算法: rsa

密钥长度: 2048

指纹: 63d7549182151d25eae843f0cd03f98daae59c62bbda51b35c96fb293deed400

硬编码敏感信息

可能的敏感信息
"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"

"dcloud_tips_certificate" : "certificate"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"
"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"
"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"
"dcloud_tips_certificate" : "证书"

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_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
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_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
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。
		Unknown	

com.vivo.notification.permission.BADGE_ICON	未知	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_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
com.asus.msa.SupplementaryDID.ACCESS	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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: h569e8560://,

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。