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

**ProjectChat（ 2.02.03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 | ProjectChat |
| 版本 | 2.02.03 |
| 包名 | plus.H5ACE11EE |
| 域名线索 | 39条 |
| URL线索 | 29条 |
| APP图标 |  |
| 分析日期 | 2025年5月29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 | projectchat.apk |
| 文件大小 | 11.06MB |
| MD5值 | e75eb4527e603c16ee08c36315624bda |
| SHA1值 | 960f73f8ce775ce6f4033300829ca1314c33d14f |
| SHA256值 | 1d334a61aa7f89850c54f872bf3033c0bbb88d82d01c02bc441a9f6ac3423cfa |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | ProjectChat |
| 包名 | plus.H5ACE11EE |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 2.02.03 |
| 安卓版本 | 192 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| fontawesome.comthe | 没有服务器地理信息. |
| sdk.api.oaid.wocloud.cn | 没有服务器地理信息. |
| fontawesome.comhttps | 没有服务器地理信息. |
| ns.adobe.com | 没有服务器地理信息. |
| s1.dcloud.net.cn | IP: 150.158.3.107  所属国家: China  地区: Beijing  城市: Beijing |
| html.spec.whatwg.org | IP: 165.227.248.76  所属国家: United States of America  地区: New Jersey  城市: Clifton |
| edgedl.me.gvt1.com | IP: 34.104.35.123  所属国家: United States of America  地区: California  城市: Mountain View |
| zi.artx.cn | IP: 208.98.43.15  所属国家: United States of America  地区: Illinois  城市: Chicago |
| msdn.microsoft.com | IP: 13.107.246.73  所属国家: United States of America  地区: Washington  城市: Redmond |
| android.googlesource.com | IP: 142.250.107.82  所属国家: United States of America  地区: California  城市: Mountain View |
| perfectionkills.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| greensock.com | IP: 50.28.34.250  所属国家: United States of America  地区: Michigan  城市: Lansing |
| vuejs.org | IP: 15.197.167.90  所属国家: United States of America  地区: Washington  城市: Seattle |
| bugzilla.mozilla.org | IP: 34.110.178.183  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| sdk.api.oaid.wocloud.cn.local | 没有服务器地理信息. |
| app.visionsic.com | IP: 124.70.189.146  所属国家: China  地区: Shanghai  城市: Shanghai |
| gac2.dcloud.net.cn | IP: 124.222.75.101  所属国家: China  地区: Beijing  城市: Beijing |
| www.jsdelivr.com | IP: 172.67.208.113  所属国家: United States of America  地区: California  城市: San Francisco |
| www.dcloud.io | IP: 124.163.195.101  所属国家: China  地区: Shanxi  城市: Taiyuan |
| popper.js.org | IP: 172.67.73.64  所属国家: United States of America  地区: California  城市: San Francisco |
| cli.vuejs.org | IP: 15.197.167.90  所属国家: United States of America  地区: Washington  城市: Seattle |
| dev.dcloud.net.cn | IP: 119.188.180.230  所属国家: China  地区: Shandong  城市: Jinan |
| opencollective.com | IP: 104.26.13.145  所属国家: United States of America  地区: California  城市: San Francisco |
| cdn.bootcdn.net | IP: 121.22.232.162  所属国家: China  地区: Hebei  城市: Qinhuangdao |
| tidelift.com | IP: 54.144.237.174  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| m3w.cn | IP: 124.163.195.65  所属国家: China  地区: Shanxi  城市: Taiyuan |
| fontawesome.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| cdn.dcloud.net.cn | IP: 121.4.61.130  所属国家: China  地区: Beijing  城市: Beijing |
| getbootstrap.com | IP: 104.22.59.100  所属国家: United States of America  地区: California  城市: San Francisco |
| er.dcloud.io | 没有服务器地理信息. |
| registry.npmjs.org | IP: 104.16.29.34  所属国家: United States of America  地区: California  城市: San Francisco |
| schemas.android.com | 没有服务器地理信息. |
| bgac.dcloud.net.cn | IP: 170.106.67.149  所属国家: United States of America  地区: California  城市: San Francisco |
| er.dcloud.net.cn | IP: 43.142.57.168  所属国家: China  地区: Beijing  城市: Beijing |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| gac1.dcloud.net.cn | IP: 122.51.46.227  所属国家: China  地区: Beijing  城市: Beijing |
| www.webkaka.com | IP: 211.149.147.36  所属国家: China  地区: Sichuan  城市: Chengdu |
| ask.dcloud.net.cn | IP: 116.136.188.184  所属国家: China  地区: Nei Mongol  城市: Hohhot |

### **4.2 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://m3w.cn/s/ | io/dcloud/common/util/ShortCutUtil.java |
| https://ask.dcloud.net.cn/article/282 | io/dcloud/common/constant/DOMException.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/35058 | io/dcloud/feature/audio/AudioRecorderMgr.java |
| https://er.dcloud.io/rv | io/dcloud/e/c/h/c.java |
| https://er.dcloud.net.cn/rv | io/dcloud/e/c/h/c.java |
| https://ask.dcloud.net.cn/article/35627 | io/dcloud/e/b/a.java |
| https://ask.dcloud.net.cn/article/35877 | io/dcloud/e/b/a.java |
| https://ask.dcloud.net.cn/article/283 | io/dcloud/g/b.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 |
| 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/36199 | 摸瓜V1引擎 |
| https://registry.npmjs.org/@babel/parser/-/parser-7.23.6.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/@jridgewell/sourcemap-codec/-/sourcemap-codec-1.4.15.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/@vue/compiler-core/-/compiler-core-3.3.12.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/@vue/compiler-dom/-/compiler-dom-3.3.12.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/@vue/compiler-sfc/-/compiler-sfc-3.3.12.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/@vue/compiler-ssr/-/compiler-ssr-3.3.12.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/@vue/reactivity/-/reactivity-3.3.12.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/@vue/reactivity-transform/-/reactivity-transform-3.3.12.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/@vue/runtime-core/-/runtime-core-3.3.12.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/@vue/runtime-dom/-/runtime-dom-3.3.12.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/@vue/server-renderer/-/server-renderer-3.3.12.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/@vue/shared/-/shared-3.3.12.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/base64-arraybuffer/-/base64-arraybuffer-1.0.2.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/css-line-break/-/css-line-break-2.1.0.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/csstype/-/csstype-3.1.3.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/estree-walker/-/estree-walker-2.0.2.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/file-saver/-/file-saver-2.0.5.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/html2canvas/-/html2canvas-1.4.1.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/magic-string/-/magic-string-0.30.5.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/nanoid/-/nanoid-3.3.7.tgz | 摸瓜V2引擎 |
| https://github.com/sponsors/ai | 摸瓜V2引擎 |
| https://registry.npmjs.org/picocolors/-/picocolors-1.0.0.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/postcss/-/postcss-8.4.32.tgz | 摸瓜V2引擎 |
| https://opencollective.com/postcss/ | 摸瓜V2引擎 |
| https://tidelift.com/funding/github/npm/postcss | 摸瓜V2引擎 |
| https://registry.npmjs.org/source-map-js/-/source-map-js-1.0.2.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/text-segmentation/-/text-segmentation-1.0.3.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/utrie/-/utrie-1.0.2.tgz | 摸瓜V2引擎 |
| https://registry.npmjs.org/vue/-/vue-3.3.12.tgz | 摸瓜V2引擎 |
| http://www.dcloud.io/hellomui/ | 摸瓜V2引擎 |
| https://github.com/ftlabs/fastclick/issues/251 | 摸瓜V2引擎 |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=922896 | 摸瓜V2引擎 |
| http://msdn.microsoft.com/en-us/library/windows/apps/Hh767313.aspx | 摸瓜V2引擎 |
| https://github.com/highlightjs/highlight.js/issues/2277 | 摸瓜V2引擎 |
| https://github.com/highlightjs/highlight.js/issues/2886 | 摸瓜V2引擎 |
| http://dev.dcloud.net.cn/mui) | 摸瓜V2引擎 |
| http://ask.dcloud.net.cn/article/113'; | 摸瓜V2引擎 |
| http://perfectionkills.com/global-eval-what-are-the-options/ | 摸瓜V2引擎 |
| http://dev.dcloud.net.cn/mui) | 摸瓜V2引擎 |
| http://zi.artx.cn/zi/) | 摸瓜V2引擎 |
| http://www.dcloud.io/helloh5p/HelloH5.apk | 摸瓜V2引擎 |
| http://www.dcloud.io/helloh5/update.json | 摸瓜V2引擎 |
| https://vuejs.org/guide/essentials/computed.html | 摸瓜V2引擎 |
| https://github.com/vuejs/core | 摸瓜V2引擎 |
| https://cli.vuejs.org/guide/webpack.html | 摸瓜V2引擎 |
| https://github.com/vitejs/vite-plugin-vue/tree/main/packages/plugin-vue | 摸瓜V2引擎 |
| https://html.spec.whatwg.org/multipage/parsing.html | 摸瓜V2引擎 |
| https://www.jsdelivr.com/using-sri-with-dynamic-files | 摸瓜V2引擎 |
| https://github.com/vuejs/core | 摸瓜V2引擎 |
| https://cli.vuejs.org/guide/webpack.html | 摸瓜V2引擎 |
| https://github.com/vitejs/vite-plugin-vue/tree/main/packages/plugin-vue | 摸瓜V2引擎 |
| https://github.com/andreasgal/pdf.js | 摸瓜V2引擎 |
| http://greensock.com | 摸瓜V2引擎 |
| http://greensock.com/standard-license | 摸瓜V2引擎 |
| https://getbootstrap.com/) | 摸瓜V2引擎 |
| https://github.com/twbs/bootstrap/graphs/contributors) | 摸瓜V2引擎 |
| https://github.com/twbs/bootstrap/blob/main/LICENSE) | 摸瓜V2引擎 |
| https://popper.js.org) | 摸瓜V2引擎 |
| https://github.com/richtr/NoSleep.js/issues/15 | 摸瓜V2引擎 |
| https://registry.npmjs.org/magic-string/-/magic-string-0.30.5.tgz | 摸瓜V3引擎 |
| sdk.api.oaid.wocloud.cn | 摸瓜V3引擎 |
| https://registry.npmjs.org/estree-walker/-/estree-walker-2.0.2.tgz | 摸瓜V3引擎 |
| https://registry.npmjs.org/html2canvas/-/html2canvas-1.4.1.tgz | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm-project | 摸瓜V3引擎 |
| s1.dcloud.net.cn | 摸瓜V3引擎 |
| https://cdn.bootcdn.net/ajax/libs/vue/2.7.0-beta.5/vue.min.js | 摸瓜V3引擎 |
| https://cdn.bootcdn.net/ajax/libs/element-ui/2.15.9/index.js | 摸瓜V3引擎 |
| https://registry.npmjs.org/text-segmentation/-/text-segmentation-1.0.3.tgz | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| https://github.com/highlightjs/highlight.js/issues/2277 | 摸瓜V3引擎 |
| https://registry.npmjs.org/base64-arraybuffer/-/base64-arraybuffer-1.0.2.tgz | 摸瓜V3引擎 |
| edgedl.me.gvt1.com | 摸瓜V3引擎 |
| http://dev.dcloud.net.cn/mui | 摸瓜V3引擎 |
| https://cdn.bootcdn.net/ajax/libs/vue/3.3.4/vue.global.min.js | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/35058 | 摸瓜V3引擎 |
| https://registry.npmjs.org/postcss/-/postcss-8.4.32.tgz | 摸瓜V3引擎 |
| https://er.dcloud.io/rv | 摸瓜V3引擎 |
| https://fontawesome.com/license/free | 摸瓜V3引擎 |
| https://er.dcloud.net.cn/rv | 摸瓜V3引擎 |
| https://registry.npmjs.org/picocolors/-/picocolors-1.0.0.tgz | 摸瓜V3引擎 |
| https://github.com/sponsors/ai | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm | 摸瓜V3引擎 |
| gac2.dcloud.net.cn | 摸瓜V3引擎 |
| sdk.api.oaid.wocloud.cn.local | 摸瓜V3引擎 |
| https://github.com/highlightjs/highlight.js/issues/2886 | 摸瓜V3引擎 |
| app.visionsic.com | 摸瓜V3引擎 |
| https://registry.npmjs.org/nanoid/-/nanoid-3.3.7.tgz | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto((androidx.appcompat.widget.ActionMenuView | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| https://tidelift.com/funding/github/npm/postcss | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android00androidx.appcompat.widget.FitWindowsLinearLayout((androi | 摸瓜V3引擎 |
| https://registry.npmjs.org/file-saver/-/file-saver-2.0.5.tgz | 摸瓜V3引擎 |
| https://registry.npmjs.org/source-map-js/-/source-map-js-1.0.2.tgz | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/35877 | 摸瓜V3引擎 |
| https://fontawesome.comThe | 摸瓜V3引擎 |
| https://er.dcloud.io/sc | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto00androidx.appcompat.widget.ActionBarOverlayLayout | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/clang | 摸瓜V3引擎 |
| https://registry.npmjs.org/ | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/283 | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/282 | 摸瓜V3引擎 |
| https://fontawesome.comhttps://fontawesome.comFont | 摸瓜V3引擎 |
| https://m3w.cn/s/ | 摸瓜V3引擎 |
| https://registry.npmjs.org/utrie/-/utrie-1.0.2.tgz | 摸瓜V3引擎 |
| https://cdn.dcloud.net.cn/img/mui-shadow-grey.png); | 摸瓜V3引擎 |
| https://ask.dcloud.net.cn/article/35627 | 摸瓜V3引擎 |
| bgac.dcloud.net.cn | 摸瓜V3引擎 |
| https://fontawesome.com | 摸瓜V3引擎 |
| http://www.webkaka.com/tutorial/html/2023/0407372/ | 摸瓜V3引擎 |
| er.dcloud.net.cn | 摸瓜V3引擎 |
| https://opencollective.com/postcss/ | 摸瓜V3引擎 |
| https://registry.npmjs.org/css-line-break/-/css-line-break-2.1.0.tgz | 摸瓜V3引擎 |
| https://registry.npmjs.org/csstype/-/csstype-3.1.3.tgz | 摸瓜V3引擎 |
| gac1.dcloud.net.cn | 摸瓜V3引擎 |
| https://registry.npmjs.org/vue/-/vue-3.3.12.tgz | 摸瓜V3引擎 |
| https://er.dcloud.net.cn/sc | 摸瓜V3引擎 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 7wb1fnu@gꧪ6h.al | 摸瓜V2引擎 |
| admin@imuboy.cn | 摸瓜V2引擎 |
| houfeng@dcloud.io | 摸瓜V2引擎 |
| yanyilin@dcloud.io | 摸瓜V2引擎 |
| hilongjw@gmail.com | 摸瓜V2引擎 |
| gal@mozilla.com  cjones@mozilla.com  shaon.barman@gmail.com  21@vingtetun.org  justindarc@gmail.com | 摸瓜V2引擎 |
| jack@greensock.com | 摸瓜V2引擎 |
| h@p5w.ښii | 摸瓜V2引擎 |

### **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=CN, ST=shanghai, L=shanghai, O=null, OU=null, CN=fang 签名算法: rsassa\_pkcs1v15 有效期自: 2024-03-30 16:05:33+00:00 有效期至: 2124-03-06 16:05:33+00:00 发行人: C=CN, ST=shanghai, L=shanghai, O=null, OU=null, CN=fang 序列号: 0x26b70560 哈希算法: sha256 md5值: 8607b04846c0199763a6205ffc21b45b sha1值: d5ea81b41725b27ecb7508397a865a277fee86b4 sha256值: 3e4a83edbb6379bf54b4ed21da2a1053af627362e34a0cdaf7f6ce7a1f9cb5a5 sha512值: 00703fd009a0ff552f0dc3896b5a4bedb4315913df8f33c76174d4fae6f97b05cc51387efb0b4e3996443fc6225745c43f4a6208983951d5331e6a62df728643 公钥算法: rsa 密钥长度: 2048 指纹: b6174b698f2a795b1be6d6812d2faec43ce2f8de7b231650e2aca6c308ba16f5**

## **6. 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\_feature\_confusion\_exception\_no\_private\_key\_input" : "no private key input" |
| "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\_feature\_confusion\_exception\_no\_private\_key\_input" : "私钥数据为空" |
| "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" |

## **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**

## **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。**