南明离火
移动应用检测平台

ANDROID 静态分析报告

巡田 • v3.1.2

分析日期: 2024-03-11 15:55:40

应用概览

文件名称:	zhgb.apk
文件大小:	43.22MB
应用名称:	巡田
软件包名:	uni.UNI57EC75F
主活动:	io.dcloud.PandoraEntry
版本号:	3.1.2
最小SDK:	19
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	38/100 (高风险)
跟踪器检测:	1/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	d39e819231793bd8b660328b4463e87e
SHA1:	9fed5637f652c65cfe0615f2b48a6f95b4af833
SHA256:	53a0834c4caf92fb9d377105ece7c14c2c2a6f35af29cb7bc10f669249670b91

分析结果严重性分布

高危	中危	信息	安全	关注
8	11	1	2	18

四大组件导出状态统计

Activity组件：10个，其中export的有： 0个
Service组件：3个，其中export的有： 0个
Receiver组件：1个，其中export的有： 0个
Provider组件：2个，其中export的有： 0个

应用签名证书信息

二进制文件已签名

v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=CN, ST=, L=, O=Android, OU=Android,
CN=2wxScNW3YJdgAnEfZWZ6rR3kHUYfijRWK5jejP8SGG63w%2FedqvrF03TZjAqbzV%2FAvcAnZ0p70rnFxz22%2Fsz6%2BQ%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2023-08-02 08:31:06+00:00
有效期至: 2123-07-09 08:31:06+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android,
CN=2wxScNW3YJdgAnEfZWZ6rR3kHUYfijRWK5jejP8SGG63w%2FedqvrF03TZjAqbzV%2FAvcAnZ0p70rnFxz22%2Fsz6%2BQ%3D%3D
序列号: 0x5ce3f8c6
哈希算法: sha256
证书MD5: a44830945582fbff579aa72897c453fa
证书SHA1: 43df13dc7f1c6d5e987d9ee74117bd1ba4acd1aa
证书SHA256: 8e143e8a33f77d498abf8d9a99f16a365d307425c31344f9ad540304d7742983
证书SHA512:
e052c9e2977c24ec52259de833c59e5f441c623b1ac062e65a0a7ddca55b47f63ee5fafdaee7a991d632cc208bda6d42[illegible]47a4fb438641c6f91c5c3dcc7915c

公钥算法: rsa
密钥长度: 2048
指纹: 6d1dad943d8d50e26c3f728b4ad6cc86041785a19282aff59f40192fab08d390
找到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
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.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.ACCESS_WIFI_STATE	普通	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	签名(系统)	请求安装APP	允许应用程序安装全新的或更新的 Android 包。恶意应用程序可能会借此添加其具有任意权限的新应用程序。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
android.permission.ACCESS_MOCK_LOCATION	危险	获取模拟定位信息	获取模拟定位信息，一般用于帮助开发者调试应用。恶意程序可以用它来覆盖真实位置信息源。
android.permission.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。

android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.CONTROL_LOCATION_UPDATES	签名(系统)	控制定位更新	允许获得移动网络定位信息改变。普通应用程序不能使用此权限。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
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置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	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	普通	桌面图标角标	vivo平台桌面图标角标，接入vivo平台后需要用户手动开启，开启完成后收到新消息时，在已安装的应用桌面图标右上角显示“数字角标”。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	警告	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: **3** | 警告: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 4.4-4.4.4, [minSdk=19]	警告	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
3	Activity (io.dcloud.PandoraEntry) is vulnerable to StrandHogg 2.0	高危	已发现活动容易受 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
4	Activity (io.dcloud.PandoraEntryActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
5	Activity (io.dcloud.WebAppActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。

代码安全漏洞检测

高危: **5** | 警告: **7** | 信息: **1** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息，不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	使用SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

3	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
4	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
5	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
6	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
7	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
8	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
9	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
10	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限

11	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
12	该文件是World Writable。任何应用程序都可以写入文件	高危	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
13	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
14	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
15	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)

1	armeabi-v7a/libAMapSDK_MAP_v9_5_0.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用
2	armeabi-v7a/libbreakpad-core.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__memcpy_chk']	False warning 符号可用

3	armeabi-v7a/libdcblur.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用
4	armeabi-v7a/liblamemp3.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限

恶意软件常用权限	10/30	android.permission.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CALL_PHONE android.permission.CAMERA android.permission.GET_ACCOUNTS android.permission.READ_PHONE_STATE android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.WRITE_SETTINGS
其它常用权限	12/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.ACCESS_MOCK_LOCATION android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FLASHLIGHT android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

恶意域名威胁检测

域名	状态	中国境内	位置信息
wap.amap.com	安全	是	**IP地址:** 101.226.26.145 **国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.224333 **经度:** 121.469139 **查看:** 高德地图
er.dcloud.net.cn	安全	是	**IP地址:** 118.89.168.191 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
dualstack-a.apilocate.amap.com	安全	是	**IP地址:** 59.82.9.131 **国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看:** 高德地图
wprd0d.is.autonavi.com	安全	否	No Geolocation information available.

mpsapi.amap.com	安全	是	**IP地址:** 59.82.43.198 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
ask.dcloud.net.cn	安全	否	**IP地址:** 43.132.84.11 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.774929 **经度:** -122.419416 **查看:** Google 地图
mps.amap.com	安全	是	**IP地址:** 59.82.43.198 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
dualstack-arestapi.amap.com	安全	是	**IP地址:** 59.82.29.60 **国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看:** 高德地图
yuntuapi.amap.com	安全	否	No Geolocation information available.
www.android.com	安全	否	**IP地址:** 142.250.176.14 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
restsdk.amap.com	安全	是	**IP地址:** 59.82.34.102 **国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.224333 **经度:** 121.469139 **查看:** 高德地图
maps.testing.amap.com	安全	是	**IP地址:** 140.205.69.9 **国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看:** 高德地图

m3w.cn	安全	是	**IP地址:** 124.166.238.85 **国家:** China **地区:** Shanxi **城市:** Taiyuan **纬度:** 37.869438 **经度:** 112.560280 **查看:** 高德地图
lbs.amap.com	安全	是	**IP地址:** 59.82.29.231 **国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.16142 **查看:** 高德地图
lame.sf.net	安全	否	**IP地址:** 72.64.153.102 **国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.783058 **经度:** -96.806671 **查看:** Google 地图
apilocate.amap.com	安全	是	**IP地址:** 59.82.14.113 **国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看:** 高德地图
wb.amap.com	安全	是	**IP地址:** 59.82.34.118 **国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.224333 **经度:** 121.469139 **查看:** 高德地图
cgicol.amap.com	安全	是	**IP地址:** 180.97.165.104 **国家:** China **地区:** Jiangsu **城市:** Suzhou **纬度:** 31.311390 **经度:** 120.618057 **查看:** 高德地图
adiu.amap.com	安全	是	**IP地址:** 59.82.29.231 **国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看:** 高德地图

m5.amap.com	安全	是	**IP地址:** 59.82.44.177 **国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看:** 高德地图
mst01.is.autonavi.com	安全	是	**IP地址:** 59.82.33.237 **国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.224333 **经度:** 121.46913 **查看:** 高德地图
er.dcloud.io	安全	否	No Geolocation information available.
apiinit.amap.com	安全	是	**IP地址:** 59.82.34.102 **国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.224333 **经度:** 121.469139 **查看:** 高德地图
abroad.apilocate.amap.com	安全	是	**IP地址:** 203.209.230.18 **国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• data:image	com/bumptech/glide/load/model/DataUrlLoader.java
• data:text/html, • javascript:var • javascript:(function(){var	io/dcloud/common/adapter/ui/AdaWebview.java
• file:///	io/dcloud/common/adapter/ui/webview/WebJsEvent.java
• javascript:(function(){var • javascript:setTimeout(function(){location.__page__load__over__ • data:text/html,chromewebdata • file:///	io/dcloud/common/adapter/ui/webview/WebLoadEvent.java
• 4.5.4.1 • 4.5.4.2	io/dcloud/common/adapter/util/MobilePhoneModel.java

• javascript:(function(){if(!((window.__html5plus__&&__html5plus__.isReady)?__html5plus__:(navigator.plus&&navigator.plus.isReady)?navigator.plus:window.plus)){window.__load__plus__&&window.__load__plus__();}var • javascript:!function(){(window.__html5plus__&&__html5plus__.isReady?__html5plus__:navigator.plus&&navigator.plus.isReady?navigator.plus:window.plus)	io/dcloud/common/constant/AbsoluteConst.java
• https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
• javascript:(function(){if(!((window.__html5plus__&&__html5plus__.isReady)?__html5plus__:(navigator.plus&&navigator.plus.isReady)?navigator.plus:window.plus)){window.__load__plus__&&window.__load__plus__();}var	io/dcloud/common/core/ui/DCKeyboardManager.java
• javascript:window.__needNotifyNative__=true;	io/dcloud/common/core/ui/g.java
• http://ns.adobe.com/xap/1.0/	io/dcloud/common/util/ExifInterface.java
• data:image • http://localhost • https://localhost	io/dcloud/common/util/PdrUtil.java
• https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
• https://ask.dcloud.net.cn/article/35627 • https://ask.dcloud.net.cn/article/35877	io/dcloud/e/b/a.java
• http://localhost • file:///	io/dcloud/e/b/e.java
• https://er.dcloud.io/rv • https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/b.java
• https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
• https://er.dcloud.io/sc • https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
• data:image/	io/dcloud/feature/nativeObj/NativeBitmap.java
• file://%s',	io/dcloud/feature/nativeObj/NativeBitmapMgr.java
•	io/dcloud/feature/nativeObj/TitleNView.java
• file:///android_asset	io/dcloud/feature/nativeObj/photoview/PhotoActivity.java
• file:///	io/dcloud/feature/nativeObj/photoview/subscaleview/ImageSource.java
• file:///	io/dcloud/feature/nativeObj/photoview/subscaleview/SubsamplingScaleImageView.java
• file://%s	io/dcloud/feature/pdr/a.java
• http://localhost	io/dcloud/feature/weex/adapter/DefaultWebSocketAdapter.java

• file:///	io/dcloud/feature/weex/adapter/PlusUriAdapter.java
• javascript:(function • file:///	io/dcloud/feature/weex/adapter/webview/DCWXWebView.java
• javascript:(function(){	io/dcloud/feature/weex/adapter/webview/WXDCWeb.java
• javascript:!function(){(window.__html5plus__&&__html5plus__.isReady?__html5plus__:navigator.plus&&navigator.plus.isReady?navigator.plus:window.plus)	io/dcloud/feature/weex/extend/PlusModule.java
• https://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java
• data:%s;base64,%s	io/dcloud/is/file/FileFeatureImpl.java
• http://lbs.amap.com/api/android-sdk/guide/error/	io/dcloud/is/map/amap/adapter/AMapLink.java
• https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java

- http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0
- http://restsdk.amap.com/v5
- http://restsdk.amap.com/v3/config/district?
- http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0
- javascript:!function(){(window.__html5plus__&&__html5plus__.isReady?__html5plus__:navigator.plus&&navigator.plus.isReady?navigator.plus:window.plus)
- http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明
- javascript:(function(){if(!((window.__html5plus__&&__html5plus__.isReady)?__html5plus__:(navigator.plus&&navigator.plus.isReady)?navigator.plus:window.plus)){window.__load__plus__&&window.__load__plus__();}var
- https://restsdk.amap.com/v3/iasdkauth
- https://restsdk.amap.com/v5
- https://restsdk.amap.com/rest/me/cpoint
- http://yuntuapi.amap.com
- https://restsdk.amap.com/v3
- http://restsdk.amap.com/sdk/compliance/params
- http://abroad.apilocate.amap.com/mobile/binary
- http://restsdk.amap.com/v3
- javascript:(function(){var
- http://dualstack-a.apilocate.amap.com/mobile/binary
- http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0
- javascript:(function
- data:image
- http://apilocate.amap.com/mobile/binary
- http://apiinit.amap.com/v3/log/init
- https://localhost
- http://dualstack-arestapi.amap.com/v3/geocode/regeo
- http://restsdk.amap.com/v4/grasproad/driving?
- http://wprd0%d.is.autonavi.com/appmaptile?
- javascript:var
- http://restsdk.amap.com/v4/gridmap?
- http://restsdk.amap.com/rest/me/cpoint
- 4.5.4.1
- https://er.dcloud.io/sc
- http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&
- http://restsdk.amap.com/v3/geocode/regeo
- http://mst01.is.autonavi.com/appmaptile?z=%d&x=%d&y=%d&lang=zh_cn&size=1&scale=1&style=6
- https://ask.dcloud.net.cn/article/36199
- http://restsdk.amap.com/rest/lbs/demData?z=%d&x=%d&y=%d&type=2
- http://mpsapi.amap.com/
- http://m5.amap.com/
- http://www.android.com/
- https://restsdk.amap.com/v4
- http://m5.amap.com/ws/mapapi/shortaddress/transform
- http://localhost
- http://restsdk.amap.com/v3/place/around?
- http://mpsapi.amap.com/ws/mps/lyrdata/utc/
- http://restsdk.amap.com/v4
- http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0
- javascript:window.postMessage
- https://n3w.cn/s/
- https://er.dcloud.net.cn/sc
- https://adiu.amap.com/ws/device/adius
- https://m5.amap.com/ws/mapapi/shortaddress/transform
- https://dualstack-arestapi.amap.com/v3/iasdkauth
- http://restsdk.amap.com/v3/place/text?
- 4.5.4.2
- http://www.amap.com/
- http://restsdk.amap.com
- https://restsdk.amap.com/sdk/compliance/params
- https://yuntuapi.amap.com
- data:text/html,

自研引擎分析结果

• • data:text/plain;base64, • 4.3.4.3 • http://m5.amap.com/ws/transfer/auth/map/indoor_maps • data:application/octet-stream;base64, • http://mpsapi.amap.com/ws/mps/rtt/ • 4.3.4.4 • http://mpsapi.amap.com/ws/mps/vmap/ • http://mpsapi.amap.com/ws/mps/lyrdata/ugc/ • http://m5.amap.com • 4.3.4.2 • • • 11.15.81.89 • http://mpsapi.amap.com/ws/mps/smap • https://mps.amap.com/ws/mps/rtt • https://mps.amap.com/ws/mps/vmap • https://maps.testing.amap.com/ws/transfer/auth/map/indoor_maps • https://mps.amap.com/ws/mps/smap • https://mps.amap.com/ws/mps/spot • https://mps.amap.com/ws/mps/hot • 11.15.81.67 • • http://mpsapi.amap.com/ • data:application/gltf-buffer;base64, • 9.5.0.206	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so
• http://lame.sf.net	lib/armeabi-v7a/liblamemp3.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
MSA SDK	移动安全联盟	移动智能终端补充设备标识体系统一调用 SDK 由中国信息通信研究院泰尔终端实验室、移动安全联盟整合提供，知识产权归中国信息通信研究院所有。
Fresco	Facebook	Fresco 是一个用于管理图像及其使用的内存的 Android 库。
C++ 共享库	Android	在 Android 应用中运行原生代码。
GIFLIB	GIFLIB	The GIFLIB project maintains the giflib service library, which has been pulling images out of GIFs since 1989. It is deployed everywhere you can think of and some places you probably can't: graphics applications and web browsers on multiple operating systems, game consoles, smartphones, and likely your ATM too.
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
Weex	Alibaba	Weex 致力于使开发者能基于通用跨平台的 Web 开发语言和开发经验，来构建 Android、iOS 和 Web 应用。简单来说，在集成了 WeexSDK 之后，你可以使用 JavaScript 语言和前端开发经验来开发移动应用。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。

第三方追踪器检测

名称	类别	网址

AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361

敏感凭证泄露检测

可能的密钥
"dcloud_permissions_reauthorization" : "重新授权"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"
"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"
"dcloud_io_without_authorization" : "没有获得授权"
YHx8eHsyJydvaWs6JmxrZGd9bCZmbXwma2YnaXh4J2lrew==
evs6OIME2yLCyUChqtQTGtxDh4/6wcSpdRw8lh8NGkyLXZQtZ1A7NDeHIlL2yXH5
YHx8eHsyJydpezkmbGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnGWt8YWdm
YHx8eHsyJydvaXs6JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZU17aXh4J2lrfGFnZg==
YHx8eHsyJydqfDkmbGtkZ31sJmZtfCZrZidgfHx4J2tpaQ==
YHx8eHsyJydpazombGtkZ31sJmZtfCZrZidpeHgnaWk7
YHx8eHsyJydvaXo5JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZU17aXl43p7eA==
YHx8eHsyJydrOSZsa2RnfWwmZm18JmtmJ2tnZGRta3wneGR9e2l4eCdraWw=
YHx8eHsyJydpazkmbGtkZ31sJmZtfCZrZidpeHgnaWk=
UWV/BnpHVVhMakD0EU1XA15hAEFOAWlGVH3kxgluSF0HFhlQZx15Yhhjb3xCHgRfWxV+cQhPS1ICFxRzdkUfeyo2YTNkODhmYS00YmEwLTQ3OWYtOTQyMi1lNWFhYmUxNTg5N2IxMjQ=
YHx8eHsyJyd7OiZsa2RnfWwmZm18JmtmJ2tnZGRta3wneGR9e2l4eCd7fGl6fH14J346
YHx8eHsyJydpazombGtkZ31sJmZtfCZrZidpeHgnfGBhemxLZ2ZuYW8=
YHx8eHsyJyd7OSZsa2RnfWwmZm18JmtmJ2tnZGRta3wneGR9e2l4eCd7fGl6fH14J346
W3v2HgaLzgcYUOeZ7E6RDsIpMd2Glz1MxJdRxdis
YHx8eHsyJydaWs5JmxrZGd9bCZmbXwma2YnYHx8eCdpaXs=
YHx8eHsyJydvaXo5JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnent4
YHx8eHsyJyd8OiZsa2RnfWwmZm18JmtmJ2tnZGRta3wneGR9e2l4eCdpa3xhZ2Y=

eG5/SmdnZHxNYmduSmhobnh4TXlkZk1iZ25eWUd4KjZhM2Q4OGZhLTRiYTAtNDc5Zi05NDIyLWU1YWFiZTE1ODk3Yjc1
amwtZ2BvbHZnLWBsbm5sbS1gcC1HTyo2YTNkODhmYS00YmEwLTQ3OWYtOTQyMi1lNWFhYmUxNTg5N2I2Nw==
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
YHx8eHsyJydvazkmbGtkZ31sJmFnJ2tnZGRta3wneGR9e2l4eCdraWw=
5rPjudJDczZ5DrTBECwfWer9fxhAWnoxI7Hr0jS/XKKlD9cg1eZLP+WDaj1U0IQ9
YHx8eHsyJydvaXs5JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J2lrfGFnZg==
YHx8eHsyJydvazkmbGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgna2ls
YHx8eHsyJydpezombGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
YHx8eHsyJydvaXs5JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
p2WH3ao/DPQajXDOBOngAQRJy7HFl6I+rNVrL72Tvjg=
CEroA9kVcgb5YW85GtDBLrVZfsAsUrOdkBRjB/Uh1+E=
9F89C84A559F573636A47FF8DAED0D33
YHx8eHsyJydvaXo6JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J3p7eA==
YHx8eHsyJydpejombGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnent4
f2l4TWBgY3tKZWBpTW9vaX9/KjZhM2Q4OGZhLTRiYTAtNDc5Zi05NDIyLWU1YWFiZTE1ODk3Yjc2
YHx8eHsyJydvaWs5JmxrZGd9bCZmbXwma2YnaXh4J2lrew==
YHx8eHsyJydvaXs6JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
YHx8eHsyJydqezkmbGtkZ31sJmZtfCZrZidgfHx4J2tpeWw+Og==
YHx8eHsyJydqaWs5JmxrZGd9bCZmbXwma2YnYHx8eCdpaWs=
E3F5536A141811DB40EFD6400F1D0A4E
YHx8eHsyJydqb2l7JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
aHR0cHM6Ly9jci5kY2xvWOubnV0LmNuLw==
YHx8eHsyJyd8OSZsa3RnfWwmZm18JmtmI2thZGRta3wneGR9e2l4eCdpa3xhZ2Y=
Y29tLmFuZHJvaWQuaW50ZXJuYWwuUiRzdHlsZWFibGU=
2BGSU2QcUAXYXuDA9OkD2SrtLCWMXqJb5xjvxk4w6dV7K0u
YHx8eHsyJydqb2l7JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J2lrfGFnZg==
5rPjudJDczZ5DrTBECwfWXZlxIQFlIC/UMsP+phhn+hM5LDHPI8rrfGoWmO4XXwm
e218Qml+aYtrenF4fEtpZkd4bWZfYWZsZ397SX18Z2VpfGFraWRkcQ==
YHx8eHsyJydpazkmbGtkZ31sJmZtfCZrZidpeHgnfGBhemxLZ2ZuYW8=
5rPjudJDczZ5DrTBECwfWSjBF5HsOIb6t/fa0kExz2phP+SrGrN3+oS6bbF8z8n+

YHx8eHsyJydqb2l6JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J3p7eA==
NcnBDcMwCEDRXThXDJBtSKAWiQErjtVWVXcvB0f60j+8L1wrLLCF4UWxUszBA3aesKsXDi9IraFRrYmNb30PN0ls6jwiS+XPxN6RnM9QxlE2pJeYpB/9dtMqWPRpdMgJvz8=
YHx8eHsyJydqb2l6JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnent4
YHx8eHsyJydqaXs5JmxrZGd9bCZmbXwma2YnYHx8eCdraWk=
YHx8eHsyJydvaXo6JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnent4
YHx8eHsyJydqb2lrJmxrZGd9bCZmbXwma2YnaXh4J2lrew==
amwtZ2BvbHZnLWVmYnd2cWYtYGUtYEVmYnd2cWZKbnNvKjZhM2Q4OGZhLTRiYTAtNDc5Zi05NDIyLWU1YWFiZTE1ODk1YjY=
5rPjudJDczZ5DrTBECwfWbr6jIGaA05lJJ4z8lfXa1gko92nDYCi7GietE6VgZMY
eW9+S2ZmZX1fZGN8b3h5a2ZLaWlveXlMeGVnTGNmb19YRnkqNmEzZDg4ZmEtNGJhMC00NzlmLTk0MjItZTVhYWJlMTU4OTdiNzQ=
YHx8eHsyJydpejkmbGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnent4
YHx8eHsyJydqaXo6JmxrZGd9bCZmbXwma2YnYHx8eCdraXo=

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架，它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。