



ANDROID 静态分析报告



智管家 • v2.1.41

分析日期: 2024-07-28 06:41:49

i应用概览

文件名称:	zgjv2.1.44.apk
文件大小:	16.52MB
应用名称:	智管家
软件包名:	com.g1150613283.znz
主活动:	com.uzmap.pkg.LauncherUI
版本号:	2.1.41
最小SDK:	16
目标SDK:	26
加固信息:	未加壳
应用程序安全分数:	35/100 (高风险)
跟踪器检测:	4/432
杀软检测:	AI评估: 很危险, 请谨慎安装
MD5:	caf017d4e1ad4365673de6b00206573f
SHA1:	e1a5a2d3b2ea349f6753306b2626a841264e48d6
SHA256:	7f2e196fcb03050d7057ec903404a9066af5785402036b98412520a47cda5d0b

📊分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✅ 安全	🔍 关注
10	19	1	1	2

📦四大组件导出状态统计

Activity组件: 10个, 其中export的有: 5个
Service组件: 6个, 其中export的有: 2个
Receiver组件: 5个, 其中export的有: 1个
Provider组件: 5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: False
v4 签名: False
主题: C=(zh), ST=(Beijing), L=(Beijing), O=(1150613283@qq.com), OU=(1150613283@qq.com), CN=(r1150613283)
签名算法: rsassa_pkcs1v15
有效期自: 2018-12-21 02:15:00+00:00
有效期至: 2118-11-27 02:15:00+00:00
发行人: C=(zh), ST=(Beijing), L=(Beijing), O=(1150613283@qq.com), OU=(1150613283@qq.com), CN=(r1150613283)
序列号: 0x3f42381a
哈希算法: sha256
证书MD5: a45eca24d3dd3b5d1613326707b4f690
证书SHA1: 5c0e84f6df48be3995d6f0942b21321d57017e82
证书SHA256: dfd3574cf547f251a231436b562d837b76db6beb13a303260c6887c9762c0b9d
证书SHA512:
8475df8737f37126907aa98f347dc3a69f430fac9b7148bcb6143ec168870760d075ce2db747316a4b31181578f9bac2d571371b1dd5424f4b25e31f0e8c6a2e

公钥算法: rsa
密钥长度: 1024
指纹: ed6bb58d289c43530455e3454f366d4645fef739f3c0e14c0541021ac9803207
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。
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。
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_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_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.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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。

android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
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.RECEIVE_USER_PRESENT	普通	允许程序唤醒机器	允许应用可以接收点亮屏幕或解锁广播。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
com.g1150613283.znz.permission.JPUSH_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
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.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.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。

🔒 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:

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

🔍 Manifest 配置安全分析

高危: 6 | 警告: 10 | 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 4.1-4.1.2, [minSdk=16]	信息	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 (com.uzmap.pkg.EntranceActivity) 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。
4	Activity (com.uzmap.pkg.EntranceActivity) 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。这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”或设置空 taskAffinity (taskAffinity= "") 属性来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 28 或更高版本以在平台级别修复此问题。
5	Activity (cn.jp.push.android.ui.PushActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
6	Activity设置了TaskAffinity属性 (cn.jp.push.android.service.JNotifyActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
7	Activity (cn.jp.push.android.service.JNotifyActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 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 (26) 更新到 29 或更高版本以在平台级别修复此问题。
8	Activity (cn.jp.push.android.service.JNotifyActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
9	Activity设置了TaskAffinity属性 (com.g1150613283.znz.wxapi.WXEntryActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
10	Activity (com.g1150613283.znz.wxapi.WXEntryActivity) 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。
11	Activity (com.g1150613283.znz.wxapi.WXEntryActivity) 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。这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”或设置空 taskAffinity (taskAffinity= "") 属性来修复此漏洞。您还可以将应用的目标 SDK 版本 (26) 更新到 28 或更高版本以在平台级别修复此问题。
12	Activity (com.g1150613283.znz.wxapi.WXEntryActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 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 (26) 更新到 29 或更高版本以在平台级别修复此问题。
13	Activity (com.g1150613283.znz.wxapi.WXEntryActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

14	Service (cn.jpush.android.service.DaemonService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
15	Service (com.open.apicloud.jpush.PushService) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Service是显式导出的。
16	Broadcast Receiver (com.open.apicloud.jpush.PushMessageReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
17	高优先级的Intent (1000) [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

</> 代码安全漏洞检测

高危: 4 | 警告: 7 | 信息: 1 | 安全: 1 | 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	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: 证书验证失败 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员: 解锁高级权限
3	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
4	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
5	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

6	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
7	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
8	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。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
9	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
10	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
11	应用程序创建临时文件。敏感信息永远不应该被写入临时文件	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
12	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
13	该文件是World Readable。任何应用程序都可以读取文件	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	P I E	STACK CANARY (栈保护)	RELRO	RP AT H (指定 SO 搜索路径)	R UN P AT H (指定 S O 搜索路径)	FORTIFY(常用函数加强检查)	S Y M B O L S T R I P P E D(裁剪符号表)
1	armeabi/libsec.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。	No ne inf o 二进制文件没有设置运行时搜索路径或 RPA TH	N o n e i n f o 二进制文件没有设置 R U N P AT H	False warning 二进制文件没有任何加固函数。加固函数提供了针对 libc 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 symbol table stripped 符号可用

2	armeabi/libwebpbackport.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。	No ne info 二进制文件没有设置运行时搜索路径	No ne 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 libc 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/FIutter 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	11/30	android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.RECEIVE_BOOT_COMPLETED android.permission.REQUEST_INSTALL_PACKAGES android.permission.SYSTEM_ALERT_WINDOW android.permission.MODIFY_AUDIO_SETTINGS 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.FLASHLIGHT android.permission.BLUETOOTH_ADMIN android.permission.BLUETOOTH android.permission.FOREGROUND_SERVICE android.permission.CHANGE_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS

常用: 已知恶意软件经常滥用的权限。

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
p.app3c.cn	安全	否	No Geolocation information available.
s.apicloud.com	安全	否	No Geolocation information available.
mta.oa.com	安全	否	IP地址: 141.144.196.217 国家: 荷兰 (王国) 地区: 北荷兰省 城市: 阿姆斯特丹 纬度: 52.378502 经度: 4.899980 查看: Google 地图
www.ccil.org	安全	否	IP地址: 142.251.40.51 国家: 美利坚合众国 地区: 纽约 城市: 纽约市 纬度: 40.713192 经度: -74.006065 查看: Google 地图
d.app3c.cn	安全	否	No Geolocation information available.
as.apicloud.com	安全	否	No Geolocation information available.
r.app3c.cn	安全	是	IP地址: 47.93.90.46 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图
a.app3c.cn	安全	是	IP地址: 47.93.90.46 国家: 中国 地区: 北京 城市: 北京 纬度: 39.907501 经度: 116.397102 查看: 高德地图

🌐 URL 链接安全分析

URL 信息	源码文件
--------	------

• http://www.aucss.com • https://html.spec.whatwg.org/multipage/infrastructure.html • http://aerolab.github.io/midnight.js/ • https://html.spec.whatwg.org/ • http://file02.16sucai.com/d/file/2014/0829/372edfeb74c3119b666237bd4af92be5.jpg • http://www.google.com • https://github.com/eslint/eslint/issues/6125 • https://jsperf.com/getall-vs-sizzle/2 • http://phpjs.org/functions/base64_encode • http://www.mescroll.com • https://github.com/axios/axios/issues/201 • https://github.com/cubiq/iscrollForIOS/issues/1029 • http://www.mescroll.com/qa.html • http://url.spec.whatwg.org/ • https://ib.cnooc.com.cn/app/ • http://unixpapa.com/js/mouse.html • https://sizzlejs.com/ • http://willow-systems.com • https://github.com/davidchambers/Base64.js • http://aerolab.github.io/midnight.js/LICENSE.txt • https://html.spec.whatwg.org/multipage/forms.html • http://kukawski.pl • https://github.com/mescroll/mescroll/releases • https://html.spec.whatwg.org/multipage/syntax.html • http://www.cnooc.com.cn/ • http://feross.org • https://github.com/mescroll/mescroll/issues • https://bugzilla.mozilla.org/show_bug.cgi?id=687787 • https://github.com/eslint/eslint/issues/3229 • https://web.archive.org/web/20141116233347/http • https://connect.microsoft.com/IE/feedback/details/1736512/ • http://kevin.vanzonneveld.net • http://rumkin.com • https://github.com/jrburke/requirejs/wiki/Updating-existing-libraries • https://trial.mobiscroll.com/ • https://html.spec.whatwg.org/multipage/scripting.html • https://bugzilla.mozilla.org/show_bug.cgi?id=922606 • http://blog.alexmaccau.com/css-transitions • https://github.com/ftlabs/fastclick/issues/251 • https://m.cnooc.com.cn/web/cas/detail?casId=32 • http://www.unbolt.net • https://web.archive.org/web/20100524014747/http • https://ibtest.cnooc.com.cn/app/ • https://jsperf.com/thor-indexof-vs-for/5 • https://promisesaplus.com/ • http://cityselect.ydtv.org • https://github.com/dcodeIO/bcrypt.js	自研引擎-A
---	--------

- https://s.apicloud.com - https://a.app3c.cn - https://d.app3c.cn - https://p.app3c.cn - https://r.app3c.cn - https://as.apicloud.com	compile/Properties.java
http://lbslife.baidu.com/shopmall/guide/getarbuilding	map/baidu/ar/http/client/ConstantHost.java
https://github.com/tootallnate/java-websocket/wiki/lost-connection-detection	com/deepe/c/k/a.java
http://www.ccil.org/~cowan/tagsoup/properties/schema	com/deepe/c/h/m.java
https://mapsv1.bdimg.com/scape/?qt=pdata&sid=	com/baidu/paliosdk/plugin/indoor/view/IndoorAlbumView.java
- https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code - https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=%s&grant_type=refresh_token&refresh_token=%s	com/uzmap/pkg/uzmodules/uzWx/tasks/AccessTokenTask.java
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s&lang=%s	com/uzmap/pkg/uzmodules/uzWx/tasks/GetUserInfoTask.java

• http://cp01-lbs-api01.cp01.baidu.com:8108/lbs_navsdk_mini/tripshare/v1/trip/search • http://pingma.qq.com:80/mstat/report • 123.126.121.167 • 117.135.169.101 • 180.153.8.53 • https://s.apicloud.com • https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=%s&grant_type=refresh_token&refresh_token=%s • 10.0.0.200 • https://mapsv1.bdimg.com/scape/?qt=pdata&sid= • 123.196.118.23 • http://mta.oa.com/ • https://github.com/tootallnate/java-websocket/wiki/lost-connection-detection • https://p.app3c.cn • https://a.app3c.cn • https://dusee.baidu.com • 117.121.49.100 • http://lbslife.baidu.com/shopmall/guide/getarbuilding • http://mta.qq.com/ • https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code • 123.151.152.111 • http://182.92.20.189:9099/ • http://www.ccil.org/~cowan/tagsoup/properties/schema • 14.17.43.18 • 113.142.45.79 • https://as.apicloud.com • https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s&lang=%s • http://bbs.lbsyun.baidu.com/forum.php?mod=viewthread&tid=106461 • 140.207.54.125 • http://app.navi.baidu.com/mobile/#navi/naiving/ • 103.7.30.94 • 10.0.0.172 • 111.30.131.31 • 123.138.162.90 • 103.229.215.60 • 120.198.203.175 • https://r.app3c.cn • 163.177.71.186 • https://d.app3c.cn	自研引擎-S
--	--------

第三方 SDK 组件分析

SDK名称	开发者	描述信息
百度 LBS	Baidu	百度地图 Android SDK 是一套基于 Android 4.0 及以上版本设备的应用程序接口。您可以使用该套 SDK 开发适用于 Android 系统移动设备的地图应用，通过调用地图 SDK 接口，您可以轻松访问百度地图服务和数据，构建功能丰富、交互性强的地图类应用程序。
WebP	Alexey Pelykh	WebP format support for Android < 4.0.
极光推送	极光	JPush 是经过考验的大规模 App 推送平台，每天推送消息数超过 5 亿条。开发者集成 SDK 后，可以通过调用 API 推送消息。同时，JPush 提供可视化的 web 端控制台发送通知，统计分析推送效果。JPush 全面支持 Android, iOS, Winphone 三大手机平台。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
developer@apicloud.com	com/uzmap/pkg/uzcore/b/d.java
developer@apicloud.com	自研引擎-S

第三方追踪器检测

名称	类别	网址
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Baidu Map		https://reports.exodus-privacy.eu.org/trackers/99
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/312
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116

🔑 敏感凭证泄露检测

可能的密钥
极光推送的=> "JPUSH_APPKEY": "b266db8acc6dda06b5b1cf19"
极光推送的=> "JPUSH_CHANNEL": "IBMP-CNOOC-TEST"
aHR0cHM6Ly93d3cuZ29vZ2xlLWFuYWx5dGJlcy5jb20vYmF0Y2g=
aHR0cHM6Ly93d3cuZ29vZ2xlLWFuYWx5dGJlcy5jb20vY29yb3VjZDk=
YW5kcm9pZC50ZWxlGhvbknkuU21zTWFuYWdlcg==
Y29tLnV6bWFwLnBrZy51em1vZHVzZXMuZm9udUxvY2F0aW9uLlV6QmF0Y29vYmB2NhdGlvbg==
258EAF5-E914-47DA-95CA-C5AB0D2C5B31
62587239-AD3C-8190-47B4-37DE080D7E9D
6X8Y4XdM2Vhvn0KfzcEhGnWanU=

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火-修真安全分析平台自动生成