南明离火
移动应用检测平台

ANDROID 静态分析报告

光伏电站卫士 • v1.1.0

分析日期: 2025-08-03 21:54:40

应用概览

文件名称:	202502251521044q3ki.apk
文件大小:	39.56MB
应用名称:	光伏电站卫士
软件包名:	longi.dcs
主活动:	io.dcloud.PandoraEntry
版本号:	1.1.0
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
开发框架:	DCloud, Weex
应用程序安全分数:	50/100 (中风险)
跟踪器检测:	3/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	fbebdfd88e2270c1ec7c0ae02bcf1a89
SHA1:	18f564cffd3ebf5[illegible]1468169e7b9878394a
SHA256:	3c9d4174b[illegible]5e5d115376175c64fd0560cf4eb3b5c6a60b8591f4d07852f19

分析结果严重性分布

高危	中危	信息	安全	关注
1	27	1	1	1

四大组件导出状态统计

Activity组件：20个，其中export的有： 6个
Service组件：22个，其中export的有： 5个
Receiver组件：16个，其中export的有： 4个

Provider组件：8个，其中export的有： 1个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=CN, ST=shaanxi, L=xi'an, O=longi, OU=longi, CN=longi
签名算法: rsassa_pkcs1v15
有效期自: 2024-05-30 09:13:19+00:00
有效期至: 2124-05-06 09:13:19+00:00
发行人: C=CN, ST=shaanxi, L=xi'an, O=longi, OU=longi, CN=longi
序列号: 0x26ad2dec
哈希算法: sha256
证书MD5: e9ea040ce767ca76f8017d1a01adfa05
证书SHA1: d24faae0c59cbff3a8199922b4b38ced0c6e4c24
证书SHA256: df310ac558f3ca87d72d152372f4770f6c9227c4895ebb61a6be6c5aac9c5700
证书SHA512:
817bc6cb4b6ef5629b0189526c7116cc336934334806c5c9f5816e07a9782b79a409d3b96cd721f190d4df5c136c4ba4e6f71a060f66d5a6c7d9dbe1c06c66ce4

公钥算法: rsa
密钥长度: 2048
指纹: 90d8d3924c53e89d73724c5dbd5dd1e3ed4a7568040bb577a36ca0a879e1f4ff
共检测到 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.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.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.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.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
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。
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。

android.permission.READ_MEDIA_VISUAL_USER_SELECTED	危险	允许从外部存储读取用户选择的图像或视频文件	允许应用程序从用户通过权限提示照片选择器选择的外部存储中读取图像或视频文件。应用程序可以检查此权限以验证用户是否决定使用照片选择器，而不是授予对 READ_MEDIA_IMAGES 或 READ_MEDIA_VIDEO 的访问权限。它不会阻止应用程序手动访问标准照片选择器。应与 READ_MEDIA_IMAGES 和/或 READ_MEDIA_VIDEO 一起请求此权限，具体取决于所需的媒体类型。
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”。
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。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
com.skyui.launcher.permission.UPDATE_BADGE	未知	未知权限	来自 android 引用的未知权限。
longi.dcs.permission.JPUSH_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
com.hihonor.android.launcher.permission.CHANGE_BADGE	未知	未知权限	来自 android 引用的未知权限。
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.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粗略的经纬度信息，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_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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。
longi.dcs.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。

com.meizu.flyme.permission.PUSH	未知	未知权限	来自 android 引用的未知权限。
longi.dcs.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
longi.dcs.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
com.hihonor.push.permission.READ_PUSH_NOTIFICATION_INFO	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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.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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.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.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: 1

标题	严重程度	描述信息
已签名应用	信息	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **0** | 警告: **18** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	Broadcast Receiver (com.skyui.push.sdk.PushReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.skyui.permission.PUSH_RECEIVE [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
3	Service (com.vivo.push.sdk.service.CommandClientService) 受权限保护，但应检查权限保护级别。 Permission: com.push.permission.UPSTAGESERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
4	Activity (cn.jpush.android.ui.PopWinActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
5	Activity (cn.jpush.android.ui.PushActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
6	Activity (cn.jpush.android.service.JNotifyActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
7	Service (com.xiaomi.mipush.sdk.PushMessageHandler) 受权限保护，但应检查权限保护级别。 Permission: com.xiaomi.mipush.sdk.MIPUSH_RECEIVE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
8	Broadcast Receiver (cn.jpush.android.service.PluginXiaomiPlatformsReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。

9	Activity (com.xiaomi.mipush.sdk.NotificationClickedActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
10	Broadcast Receiver (cn.jpush.android.service.PluginMeizuPlatformsReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.meizu.flyme.permission.PUSH [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
11	Service (cn.jpush.android.service.PluginOppoPushService) 受权限保护，但应检查权限保护级别。 Permission: com.coloros.mcs.permission.SEND_MCS_MESSAGE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
12	Service (com.heytap.msp.push.service.DataMessageCallbackService) 受权限保护，但应检查权限保护级别。 Permission: com.heytap.mcs.permission.SEND_PUSH_MESSAGE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
13	Activity (cn.jiguang.uniplugin_jpush.OpenClickActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
14	Activity (cn.android.service.JTransitActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
15	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护。 Permission: longi.dds.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	检测到 Broadcast Receiver 已导出，但受权限保护。

本报告由南明离火移动安全分析平台生成

16	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护。 Permission: longi.dcs.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	检测到 Broadcast Receiver 已导出，但受权限保护。
17	Service (com.huawei.hms.support.api.push.service.HmsMsgService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
18	Content Provider (com.huawei.hms.support.api.push.PushProvider) 未受保护。 [android:exported=true]	警告	检测到 Content Provider 已导出，未受任何权限保护，任意应用均可访问。
19	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别：若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
20	高优先级 Intent（1000）- {1} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

高危: **1** | 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	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成

3	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
4	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
5	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
6	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
7	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
8	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
9	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
10	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	arm64-v8a/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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	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	True info 符号被剥离

2	arm64-v8a/libstatic-webp.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	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', '__strlen_chk', '__memcpy_chk', '__memmove_chk', '__vsprintf_chk']	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
00189	获取短信内容	短信	升级会员：解锁高级权限
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00066	查询ICCID号码	信息收集	升级会员：解锁高级权限
00067	查询IMSI号码	信息收集	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限

00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00131	获取当前GSM的位置并将其放入JSON中	信息收集 位置	升级会员：解锁高级权限
00099	获取当前GSM的位置并将其放入JSON中	信息收集 位置	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限

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.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.GET_TASKS android.permission.REQUEST_INSTALL_PACKAGES android.permission.CAMERA android.permission.GET_ACCOUNTS android.permission.WRITE_SETTINGS android.permission.CALL_PHONE
其它常用权限	13/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO com.google.android.c2dm.permission.RECEIVE android.permission.ACCESS_BACKGROUND_LOCATION android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FLASHLIGHT android.permission.ACCESS_LOCATION_EXTRA_COMMANDS

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
er.dcloud.io	安全	否	No Geolocation information available.
er.dcloud.net.cn	安全	是	**IP地址:** 43.142.57.168 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件

• https://lodash.com/license • https://itunes.apple.com/app/id1549643500 • https://rdcp.longi.com:6443/agreement_docs/app_service_zh.html • http://uri.amap.com/navigation?from • https://service.dcloud.net.cn/uniapp/feedback.html • https://rdcp.longi.com:6443/agreement_docs/third_party_sharing_checklist_zh.html • https://github.com/ecomfe/zrender/blob/master/LICENSE.txt • https://bit.ly/2ZqJzkp • https://rdcp.longi.com:6443 • http://developer.yahoo.com/yui/license.html • https://cdn.jsdelivr.net/npm/echarts-liquidfill • https://lodash.com • https://openjsf.org • https://rdcp.longi.com:6443/images/PhotovoltaicButler.apk • http://underscorejs.org/LICENSE • https://rdcp.longi.com:6443/agreement_docs/app_privacy_policy_zh.html	自研引擎-A
• https://er.dcloud.io/rv • https://er.dcloud.net.cn/rv	d/c.java

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以及使用的内存的 Android 库。
C++ 共享库	Android	在 Android 应用中运行原生代码。
DCloud	数字天堂	libdeflate is a library for fast, whole-buffer DEFLATE-based compression and decompression.
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。
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。

Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
HMS Core	Huawei	HMS Core 是华为终端云服务提供的端、云开放能力的合集，助您高效构建精品应用。
Huawei Push	Huawei	华为推送服务（HUAWEI Push Kit）是华为为开发者提供的消息推送平台，建立了从云端到终端的消息推送通道。开发者通过集成 HUAWEI Push Kit 可以实时推送消息到用户终端应用，构筑良好的用户关系，提升用户的感知度和活跃度。
vivo Push	vivo	vivo 推送是 Funtouch OS 上系统级消息推送平台，帮助开发者在 vivo 平台有效提升活跃和留存。通过和系统的深度结合，建立稳定可靠、安全可控、高性能的消息推送服务，帮助不同行业的开发者挖掘更多的运营价值。
MiPush	Xiaomi	小米消息推送服务在 MIUI 上为系统级通道，并且全平台通用，可以为开发者提供稳定、可靠、高效的推送服务。
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。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
AppGallery Connect	Huawei	为开发者提供移动应用全生命周期服务，覆盖全终端全场景，降低开发成本，提升运营效率，助力商业成功。
HMS Core AAID	Huawei	华为推送服务开放能力合集提供的匿名设备标识(AAID) 实体类与令牌实体类包。异步方式获取的 AAID 与令牌通过此包中对应的类承载返回。
Meizu Push	Meizu	魅族推送服务是由魅族公司为开发者提供的消息推送服务，开发者可以向集成了魅族 push SDK 的客户端实时地推送通知或者消息，与用户保持互动，提高活跃率。
OPPO Push	OPPO	OPPO PUSH 是 ColorOS 上的系统级通道，为开发者提供稳定，高效的消息推送服务。

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
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343

敏感凭证泄露检测

可能的密钥
极光推送的=> "JPUSH_APPKEY" : "799962082dc746dd1acc87cf"
DCLOUD的 "APPID" : "__UNI__380C303"
OPPO推送的=> "OPPO_APPID" : "OP-32722467"

华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "appid=113208283"
DCLOUD的 "ApplicationId" : "longi.dcs"
vivo推送的=> "com.vivo.push.app_id" : "105847880"
高德地图的=> "com.amap.api.v2.apikey" : "ee9533d255736c238f8c98b2fc41a5a6"
极光推送的=> "JPUSH_CHANNEL" : "android"
vivo推送的=> "com.vivo.push.api_key" : "52594b2dbb5ba6fb10111fbd5964a2a5"
小米推送的=> "XIAOMI_APPKEY" : "MI-5472038147869"
OPPO推送的=> "OPPO_APPSECRET" : "OP-ff1c9064793a477288afd40542a3cadb"
小米推送的=> "XIAOMI_APPID" : "MI-2882303761520381869"
DCLOUD的 "AD_ID" : "122118130310"
DCLOUD的 "DCLOUD_STREAMAPP_CHANNEL" : "longi.dcs|__UNI__380C303|1221181303|0|"
荣耀推送的=> "com.hihonor.push.app_id" : "104481042"
OPPO推送的=> "OPPO_APPKEY" : "OP-6df0da2d86904392b3ec2319f03d56e6"
vivo推送的=> "local_iv" : "MzMsMzQsMzUsMzYsMzcsMzgsMzksNDAsNDEsMzIsMzgsMzcsMzYsMzUsMzQsMzMsI0AzNCwzMiwzMywzNywzMywzNCwzMiwzMywzMywzMywzNCw0MSwzNSwzNSwzMiwzMiwiQDM2LDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDMyLDM4LDM3LDMzLDM1LDM0LDMzLCNAMzQsMzIsMzMsMzMsMzcsMzMsMzQsMzIsMzMsMzMsMzQsNDEsMzUsMzIsMzIsMzI"
"dcloud_permissions_reauthorization" : "reauthorize"
"security_public_key" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8hzUojzHX8jDL+97pqr7CaLiKSsZ0aOES7FUcX7vh9PoEDbCKNCTakRXdS5EiurPk3QpvsAGbfyIs7JWKm4py9KeldJSzBH90nknVeAVlU++jnrGFG2YFCb8iKzClN059gYeeJBs9mwi7RGU9tj0KHUG659v5sMBxv7zNse3fJQIDAQAB"
YHx8eHsyJydqb2l7JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J2lrfGFnZg==
UWV/BnpHVVhMahB0EU1XA15hAEFOAWlGVHBkcgluSF0HPhlQZx15Yhhjb3xCHgRfWxV+cQhPS1ICFxRzdkUfeyo2YTNkODhmYS00YmEwLTQ3OWYtOTQyMi1lNWFhYmUxNTgsM2IxMjQ=
YHx8eHsyJydpazkmbGdkZ31sJmZtfCZrZidpeHgnhGZheHxLZ2ZuYW8=
CEroA9kVcgb5YW85QtDBLrVZfsAsUrOdkERR3/Uh1+E=
YHx8eHsyJydvaXs5JmxrZGd9bCZmbXwma2RkbWt8J3hkfXtpeHgnaWt8YWdm
YHx8eHsyJydvaWs6JmxrZGd9bCZmbXwma2YnaXh4J2lrew==
1954544a0003cb001d315bffe671ca25c
YHx8eHsyJydpeGmbGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnent4
YHx8eHsyJydpbazombGtkZ31sJmZtfCZrZidpeHgnaWt7
YHx8eHsyJydvaXo6JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J3p7eA==

YHx8eHsyJydqaWs5JmxrZGd9bCZmbXwma2YnYHx8eCdpaXs=
W3v2HgaLzgcTXlUiOoZ7E6RDsIpMd2Glz1MxJdRxdis
p2WH3ao/DPQajXDOBOngAQRJy7HFI6I+rNVrL72Tvjg=
YHx8eHsyJydqb2l7JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
2BGSU2QqUAXYXuDA9OkD2SztJLGWMXqJb5xjvxk4w6dV7K0u
YHx8eHsyJydqb2lrJmxrZGd9bCZmbXwma2YnaXh4J2lrew==
amwtZ2BvbHZnLWBsbm5sbS1gcC1HTyo2YTNkODhmYS00YmEwLTQ3OWYtOTQyMi1lNWFhYmUxNTg5N2I2Nw==
YHx8eHsyJydqaXs5JmxrZGd9bCZmbXwma2YnYHx8eCdraWk=
5rPjudJDczZ5DrTBECwfWX3lxIQFlIC/UMsP+phhn+hM5LDHPI8rrfGoWmO4XXwm
YHx8eHsyJyd8OSZsa2RnfWwmZm18JmtmJ2tnZGRta3wneGR9e2l4eCdpa3xhZ2Y=
YHx8eHsyJyd8OiZsa2RnfWwmZm18JmtmJ2tnZGRta3wneGR9e2l4eCdpa3xhZ2Y=
YHx8eHsyJydvaWs5JmxrZGd9bCZmbXwma2YnaXh4J2lrew==
YHx8eHsyJydqb2l6JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnent4
YHx8eHsyJydvaXs6JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J2lrfGFnZg==
YHx8eHsyJydpezombGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
YHx8eHsyJydqaWs5JmxrZGd9bCZmbXwma2YnYHx8eCdpaWs=
amwtZ2BvbHZnLWVmYnd2cWYtYGUtYEVmYnd2cWZkanNvKjZhM2Q4OGZhLTRiYTAtNDc5Zi05NDIyLWU1YWFiZTE1ODk3YjY3
YHx8eHsyJydpejkmbGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnent4
5rPjudJDczZ5DrTBECwfWbr6jIGaA05jJ1zdfXa1gko92nDYCi7diet[illegible]ZMY
YHx8eHsyJydvaXo5JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnent4
YHx8eHsyJydpazkmbGtkZ31sJmZtfCZrZidpeHgnaWt8
evs6OIME2yLCwUChntQTGtxDh4/6wcSpdRw8hdNGkyLXZQtZ1A7NDehilU2yXH5
YHx8eHsyJydvaXs5JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J2lrfGFnZg==
YHx8eHsyJydqfDkmbGtkZ31sJmZtfCZrZidgfHx4J2tpaQ==
YHx8eHsyJydpazombGtkZ31sJmZtfCZrZidpeHgnfGBhemxLZ2ZuYW8=
YHx8eHsyJydvaXo5JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J3p7eA==
5rPjudJDczZ5DrTBECwfWer9fxhAWnoxI7Hr0jS/XKKlD9cg1eZLP+WDaj1U0IQ9
YHx8eHsyJydqaXo6JmxrZGd9bCZmbXwma2YnYHx8eCdraXo=
YHx8eHsyJydqb2l6JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J3p7eA==

YHx8eHsyJydvaWs5JmxrZGd9bCZmbXwma2YnaXh4JW8nams=
YHx8eHsyJydpezkmbGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
YHx8eHsyJydvaXo6JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnent4
5rPjudJDczZ5DrTBECwfWfzp1lNiDJ3F7lPgTGKXbv/Ahar5ZZo+heD2Ylvu1Q1k
YHx8eHsyJydvaXs6JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm

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。