南明离火
移动应用检测平台

ANDROID 静态分析报告

广发金选 • v2.8

本报告由南明离火移动安全分析平台生成

分析日期: 2025-07-06 00:28:48

应用概览

文件名称:	alc.xt0pru1qwmjc0.mzzkn.apk
文件大小:	42.75MB
应用名称:	广发金选
软件包名:	alc.xt0pru1qwmjc0.mzzkn
主活动:	io.dcloud.NewPandoraEntry
版本号:	2.0
最小SDK:	24
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:	55/100 (中风险)
跟踪器检测:	3/432
杀软检测:	AI评估：非常危险，建议联系安全专家人工研判
MD5:	be2c7c07b70f2731a8a90ecef76bfd06
SHA1:	9c1f84709602499efec91ae35cf308ffa62940cb
SHA256:	235fb8e1bc0a91a7f82d089908b6be4975e6ba30324e6bb86d115fc6e98b32

分析结果严重性分布

高危	中危	信息	安全	关注
1	15	1	2	4

四大组件导出状态统计

Activity组件：18个，其中export的有： 4个
Service组件：5个，其中export的有： 2个
Receiver组件：1个，其中export的有： 0个
Provider组件：3个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=CN, ST=Beijing, L=Beijing, O=VckHsYVH, OU=jcWKklsc, CN=ZPGNErCd
签名算法: dsa
有效期自: 2025-06-17 02:57:04+00:00
有效期至: 2031-08-28 02:57:04+00:00
发行人: C=CN, ST=Beijing, L=Beijing, O=VckHsYVH, OU=jcWKklsc, CN=ZPGNErCd
序列号: 0x77569885
哈希算法: sha256
证书MD5: ecbba3f39df129bc1e63d59232a21367
证书SHA1: 891205d94b234cef9fe57fc519fe710bc24472c6
证书SHA256: 28ad3863fb384b2bee4c5ef00596f8cf2e7ca63011fd32fb70a43fb0018c2ce5
证书SHA512:
6eb0d30ed43d9ba89ee7b6b19ce852014b32e5ee1f2b8cb0ded2f7b24872738e9d5b0b5d724d892fd2257a38096280d5816665db3faea9b94ab380729dabb9ae

公钥算法: dsa
密钥长度: 2048
指纹: 3494d279b403bfb1f3c287b9d82dc5834abce064b97d1c6e2c2554d80568895b
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.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.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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
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.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.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_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.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.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.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.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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.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。
com.xiaomi.permission.AUTH_SERVICE	未知	未知权限	来自 android 引用的未知权限。
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.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.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
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.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入手机或 SIM 卡中存储的短信。恶意应用程序可借此删除您的信息。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
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。

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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
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。
freemme.permission.msa	未知	未知权限	来自 android 引用的未知权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
android.permission.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
getui.permission.GetuiService.com.example.app	未知	未知权限	来自 android 引用的未知权限。
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.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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
io.dcloud.PandoraEntryActivity	Schemes: ://,

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: 0 | 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: **8** | 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	应用数据存在泄露风险 未设置[android:allowBackup]标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。
3	Activity (io.dcloud.PandoraEntryActivity) 受权限保护，但应检查权限保护级别。 Permission: com.miui.securitycenter.permission.AppPermissionsEditor [android:exported=true]	警告	检测到 Activity 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 (com.alipay.sdk.app.PayResultActivity) 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 (com.alipay.sdk.app.AlipayResultActivity) 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	Service (com.igexin.sdk.GTIntentService) 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。
7	Service (com.igexin.sdk.GService) 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。
8	Activity (com.igexin.sdk.GetuiActivity) 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。

代码安全漏洞检测

高危: **1** | 警告: **5** | 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	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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

Native等安全加固检测

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，以便它会在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
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
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
00053	监视给定内容 URI 标识的数据更改（SMS、MMS 等）	短信	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
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
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
00082	获取当前WiFi MAC地址	信息收集 WiFi	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
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
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
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
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
00013	读取文件并将其放入流中	文件	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
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	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
00030	通过给定的 URL 连接到远程服务器	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
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
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
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00134	获取当前WiFi IP地址	WiFi 信息收集	升级会员：解锁高级权限
00015	将缓冲流（数据）放入 JSON 对象	文件	升级会员：解锁高级权限
00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 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

本报告由南明离火移动安全分析平台生成

恶意软件常用权限	16/30	android.permission.CAMERA android.permission.VIBRATE android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.WRITE_SETTINGS android.permission.READ_PHONE_STATE android.permission.MODIFY_AUDIO_SETTINGS android.permission.RECORD_AUDIO android.permission.RECEIVE_BOOT_COMPLETED android.permission.GET_TASKS android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.GET_ACCOUNTS android.permission.SEND_SMS android.permission.WRITE_SMS android.permission.READ_SMS
其它常用权限	15/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.FLASHLIGHT android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_MOCK_LOCATION android.permission.CHANGE_NETWORK_STATE android.permission.BLUETOOTH_ADMIN android.permission.BLUETOOTH android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_EXTERNAL_STORAGE com.google.android.gms.permission.AD_ID android.permission.ACCESS_BACKGROUND_LOCATION

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
aid.mobileservice.cn	安全	是	**IP地址:** 115.231.163.68 **国家:** 中国 **地区:** 浙江 **城市:** 嘉兴 **纬度:** 30.752199 **经度:** 120.750000 **查看:** 高德地图
er.dcloud.net.cn	安全	是	**IP地址:** 115.231.163.69 **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
er.dcloud.io	安全	否	No Geolocation information available.

nisportal.10010.com	安全	是	IP地址: 115.231.163.69 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
zxid-m.mobileservice.cn	安全	是	IP地址: 115.231.163.69 国家: 中国 地区: 浙江 城市: 嘉兴 纬度: 30.752199 经度: 120.750000 查看: 高德地图

URL 链接安全分析

URL信息	源码文件
• https://service.dcloud.net.cn/uniapp/feedback.html • https://f.m.suning.com/api/ct.do • https://github.com/ecomfe/zrender/blob/master/LICENSE.txt • https://matomo.ybmall.net • https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf • https://www.baidu.com • https://cdn.jsdelivr.net/npm/echarts-liquidfill • http://149.88.86.118:8083	自研引擎-A
• https://zxid-m.mobileservice.cn/sdk/uaid/reportauthtoken	com/zx/a/I8b7/v1.java
• https://zxid-m.mobileservice.cn/sdk/config/init	com/zx/a/I8b7/l.java
• https://zxid-m.mobileservice.cn/sdk/uaid/get	com/zx/a/I8b7/w1.java
• https://nisportal.10010.com:9001	com/zx/a/I8b7/f1.java
• https://zxid-m.mobileservice.cn/sdk/module/getcoremodule	com/zx/a/I8b7/f0.java
• https://aid.mobileservice.cn/	com/zx/a/I8b7/j3.java
• https://zxid-m.mobileservice.cn/sdk/ext/pconfig	com/zx/a/I8b7/f.java
• https://zxid-m.mobileservice.cn/sdk/extend/tag	com/zx/a/I8b7/b2.java
• https://ext.dcloud.io/rv • https://ext.dcloud.net.cn/rv	d/c.java
• https://zxid-m.mobileservice.cn/sdk/config/v2/init	com/zx/a/I8b7/n.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。
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。
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
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
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Analytics, Crash reporting	https://reports.exodus-privacy.eu.org/trackers/448

敏感凭证泄露检测

可能的密钥
卓信ID-SDK的=> "ZX_CHANNEL_ID" : "C01-GEztJH0jzDC"
卓信ID-SDK的=> "ZX_APPID_GETUI" : "913eCa30-25b6-4989-8ac6-1ecb53649be3"
个推-推送服务的=> "GETUI_APPID" : "uniPush的appid"
"dcloud_permissions_reauthorization" : "reauthorize"
YHx8eHsyJyd8OiZsa2RnfWwmZm18JmtmJ2tnZGRta3wneGR9e2l4eCdpa3xhZ2Y=
YHx8eHsyJydvaXo9JnxrZCd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnent4
YHx8eHsyJyd8OSZsa2RnfWwmZm18JmtmJ2tnZGRta3wneGR9e2l4eCdpa3xhZ2Y=
BXR/YZEsZkKgydkACAIi9ZIpwlaFcVU0svFCdqK+9k=
YHx8eHsyJydpazombGtkZ31sJmZtfCZrZidpeHgnaWt7

YHx8eHsyJydqfDkmbGtkZ31sJmZtfCZrZidgfHx4J2tpaQ==
YHx8eHsyJydvaXs6JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J2lrfGFnZg==
amwtZ2BvbHZnLWBsbm5sbS1gcC1HTyo2YTNkODhmYS00YmEwLTQ3OWYtOTQyMi1lNWFhYmUxNTg5N2I2Nw==
YHx8eHsyJydvaWs6JmxrZGd9bCZmbXwma2YnaXh4J2lrew==
YHx8eHsyJydqaWs5JmxrZGd9bCZmbXwma2YnYHx8eCdpaWs=
YHx8eHsyJydqb2l7JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
YHx8eHsyJydpezkmbGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
5rPjudJDczZ5DrTBECwfWX3lxIQFlIC/UMsP+phhn+hM5LDHPI8rrfGoWmO4XXwm
YHx8eHsyJydqb2l6JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J3p7eA==
Y29tLmFzdXMubXNhLlN1cHBsZW1lbnRhcnlESUQuSURpZEFpZGxJbnRlcmZhY2U=
YHx8eHsyJydpezombGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
5rPjudJDczZ5DrTBECwfWfzp1lNiDJ3F7lPgTGKXbv/Ahar5ZZo+heD2Ylvu1Q1k
Y29tLmFzdXMubXNhLmFjdGlvbi5BQ0NFU1NfRElE
YHx8eHsyJydpazkmbGtkZ31sJmZtfCZrZidpeHgnaWt7
amwtZ2BvbHZnLWVmYnd2cWYtYGUtYEVmYnd2cWZKbnNvKjZhM2Q4OGZ[illegible]TRiYTAtNDc5Zi05NDIyLWU1YWFiZTE1ODk3YjY3
YHx8eHsyJydpejkmbGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnaWt4
UWV/BnpHVVhMahB0EU1XA15hAEFOAWlGVHBkcgluSF0FFhQZx15Yhhjb3xCHgRfWxV+cQbFS1ICFxRzdkUfeyo2YTNkODhmYS00YmEwLTQ3OWYtOTQyMi1lNWFhYmUxNTg5N2IxMjQ=
W3v2HgaLzgcTXlUiOoZ7E6RDsIpMd2Glz1M[illegible]dis
YHx8eHsyJydqb2l7JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J2lrfGFnZg==
CEroA9kVcgb5YW85GtDBLrVZfsA[illegible]UrO[illegible]kBRjB/Uh1+E=
YHx8eHsyJydpazombGtkZ31sJmZtfCZrZidpeHgnfGBhemxLZ2ZuYW8=
p2WH3ao/DPQai[illegible]QBO[illegible]oAQRJy7HFI6I+rNV[illegible]2Tvjg=
YHx8eHsyJydvaXs5JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
evs6OIME[illegible]yCCyUChqtQTGtxDh4/6w[illegible]SpdRw8lh8NGkyLXZQtZ1A7NDehilU2yXH5
YHx8eHsyJydvaXo5JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J3p7eA==
5rPjudJDczZ5DrTBECwfWer9fxhAWnoxI7Hr0jS/XKKlD9cg1eZLP+WDaj1U0IQ9
YHx8eHsyJydvaXs6JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnent4
YHx8eHsyJydpazkmbGtkZ31sJmZtfCZrZidpeHgnfGBhemxLZ2ZuYW8=
Y29tLmFzdXMubXNhLlN1cHBsZW1lbnRhcnlESUQuU3VwcGxlbWVudGFyeURJRFNlcnZpY2U=

本报告由南明离火移动安全分析平台生成

YHx8eHsyJydqb2lrJmxrZGd9bCZmbXwma2YnaXh4J2lrew==
YHx8eHsyJydqaXs5JmxrZGd9bCZmbXwma2YnYHx8eCdraWk=
Y29tLmFzdXMubXNhLlN1cHBsZW1lbnRhcnlESUQ=
YHx8eHsyJydqaWs5JmxrZGd9bCZmbXwma2YnYHx8eCdpaXs=
YHx8eHsyJydqaXo6JmxrZGd9bCZmbXwma2YnYHx8eCdraXo=
YHx8eHsyJydvaWs5JmxrZGd9bCZmbXwma2YnaXh4JW8nams=
YHx8eHsyJydqb2l6JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnent4
YHx8eHsyJydvaXs5JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J2lrfGFnZg==
2BGSU2QqUAXYXuDA9OkD2SztJLGWMXqJb5xjvxk4w6dV7K0u
YHx8eHsyJydvaWs5JmxrZGd9bCZmbXwma2YnaXh4J2lrew==
YHx8eHsyJydpejombGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnent4
5rPjudJDczZ5DrTBECwfWbr6jIGaA05lJJ4z8IfXa1gko92nDYCi7GietE6VgZMY
YHx8eHsyJydvaXo6JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J3p7eA==
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。