南明离火

移动应用检测平台

ANDROID 静态分析报告

PROLOGIS

安博 • v1.0.0

本报告由南明离火移动安全分析平台生成

分析日期: 2025-08-01 12:03:49

应用概览

文件名称:	base.apk
文件大小:	42.97MB
应用名称:	安博
软件包名:	ftijbs.kcxjyl.kuujan.kaymow
主活动:	io.dcloud.PandoraEntry
版本号:	1.0.0
最小SDK:	19
目标SDK:	28
加固信息:	未加壳
开发框架:	DCloud, Weex
应用程序安全分数:	46/100 (中风险)
杀软检测:	AI评估：可能有安全隐患
MD5:	948c987d46dee4d9ca76ba1f9ba3798a
SHA1:	453ff90956e454a99b9[illegible]c8b94052529966fb7a63
SHA256:	2cc7b8b7ca6148[illegible]490f6db9ff464a8d0[illegible]f8c10fc78843c4fcdc1055339c

分析结果严重性分布

高危	中危	信息	安全	关注
4	9	1	2	1

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：[illegible]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

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=United States, ST=NOMJiiJ, L=kpUq, O=WJHEFba, OU=WJHEFba, CN=WJHEFba
签名算法: rsassa_pkcs1v15
有效期自: 2025-05-17 00:42:23+00:00
有效期至: 2125-04-23 00:42:23+00:00
发行人: C=United States, ST=NOMJiiJ, L=kpUq, O=WJHEFba, OU=WJHEFba, CN=WJHEFba
序列号: 0x6f9b9bc7
哈希算法: sha512
证书MD5: 46987b65ded04c3cc352b8c5354d15b9
证书SHA1: 0a3fa80ff8cc8dbeae104896d3ded89de0ddeab5
证书SHA256: ae0b30d97e781fc13078ec53eda77b5391cb475bd461c75bc3ef3631aafe822f
证书SHA512:
439be6e4397bbf101f9a6cf2782bd7f08c60477e60ebdcc59a63bfb7f8c5e651a8fc3f79c8499a842f4ae6d4ec0407a9c5fdf3d85ee25d7fd0caab464a15942c

公钥算法: rsa
密钥长度: 2048
指纹: 0a02f73d9de6f64739c2ad99ce54f6daa488dafc230d30bbe1b7ec5f7f5d0e80
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.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。
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_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。

ftijbs.kcxjyl.kuujan.kaymow_com.huawei.android.launcher.permission.CHANGE_BADGE	未知	未知权限	来自 android 引用的未知权限。
ftijbs.kcxjyl.kuujan.kaymow_com.vivo.notification.permission.BADGE_ICON	未知	未知权限	来自 android 引用的未知权限。
ftijbs.kcxjyl.kuujan.kaymow_com.asus.msa.SupplementaryDID.ACCESS	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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.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.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。

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: **3** | 警告: **1** | 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	Activity (io.dcloud.PandoraEntry) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。
3	Activity (io.dcloud.PandoraEntryActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。
4	Activity (io.dcloud.WebAppActivity) 的启动模式非 standard	高危	Activity 启动模式设置为 "singleTask" 或 "singleInstance" 时，可能成为根 Activity，导致其他应用可读取调用 Intent 内容。涉及敏感信息时应使用 "standard" 启动模式。

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	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
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	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
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	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
9	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
10	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

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，以便在缓冲区溢出覆盖返回地址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
00036	从 res/raw 目录获取资源文件	反射	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
00013	读取文件并将其放入流中	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
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
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
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
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
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
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
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
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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	7/30	android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.VIBRATE android.permission.CAMERA android.permission.GET_ACCOUNTS android.permission.WAKE_LOCK android.permission.WRITE_SETTINGS
其它常用权限	10/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FLASHLIGHT

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.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
er.dcloud.io	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://api.ipify.org • http://116.193.170.154 • http://feross.org • http://139.196.175.43:6061/api/route/log • https://service.dcloud.net.cn/uniapp/feedback.html • http://139.196.175.43:6061/api/route • https://feross.org/opensource	自研引擎-A
• https://er.dcloud.net.cn/rv • https://er.dcloud.io/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.
爱加密	北京智游网安科技有限公司	针对目前移动应用普遍存在的破解、篡改、劫持、盗版、数据窃取、钓鱼欺诈等各类安全风险，通过行业领先的第六代加固技术，爱加密为用户提供全面的移动应用加固加密技术和攻击防范服务。
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。

敏感凭证泄露检测

可能的密钥
"dcloud_permissions_reauthorization" : "reauthorize"
YHx8eHsyJydvaXs5JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
5rPjudJDczZ5L...[illegible]...Wbr6jIGaA05lJJ428hXa...gkb92nDYCi7GietE6VgZMY
YHx8eHsyJydqrDkmbGtkZ31sJmZtfCZrZidgfHx4J2tpaQ==
YHx8eHsyJydpazkmbGtkZ31sJmZtfCZrZidpeHgnfGBhemxLZ2ZuYW8=
YHx8eHsyJydqaXs5JmxrZGd9bCZmbXwma2YnYHx8eCdraWk=
YHx8eHsyJydvaXs5JmxrZGd9bCZmbXwma2YnaXh4JW8nams=
YHx8eHsyJydvaXs6JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
YHx8eHsyJydvaXo6JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J3p7eA==

YHx8eHsyJydpejkmbGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnent4
YHx8eHsyJydvaXo5JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnent4
amwtZ2BvbHZnLWBsbm5sbS1gcC1HTyo2YTNkODhmYS00YmEwLTQ3OWYtOTQyMi1lNWFhYmUxNTg5N2I2Nw==
YHx8eHsyJydqb2lrJmxrZGd9bCZmbXwma2YnaXh4J2lrew==
YHx8eHsyJydvaXo5JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J3p7eA==
YHx8eHsyJydvaWs5JmxrZGd9bCZmbXwma2YnaXh4J2lrew==
5rPjudJDczZ5DrTBECwfWfzp1lNiDJ3F7lPgTGKXbv/Ahar5ZZo+heD2Ylvu1Q1k
2BGSU2QqUAXYXuDA9OkD2SztJLGWMXqJb5xjvxk4w6dV7K0u
05af9cd4c463e01c4c38ed4a6cbbab2bd
YHx8eHsyJydpazombGtkZ31sJmZtfCZrZidpeHgnfGBhemxLZ2ZuYW8=
YHx8eHsyJydqb2l6JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnent4
p2WH3ao/DPQajXDOBOngAQRJy7HFI6I+rNVrL72Tvjg=
YHx8eHsyJyd8OiZsa2RnfWwmZm18JmtmJ2tnZGRta3wneGR9e2l4eCdpa3xhZ2Y=
YHx8eHsyJydqb2l7JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
YHx8eHsyJyd8OSZsa2RnfWwmZm18JmtmJ2tnZGRta3wneGR9e2l4eCdpa3xhZ2Y=
YHx8eHsyJydvaXo6JmxrZGd9bCZhZydrZ2RkbWt8J3hkfXtpeHgnent4
YHx8eHsyJydqaWs5JmxrZGd9bCZmbXwma2YnYHx8eCdpaWs=
YHx8eHsyJydvaXs5JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J2lrfGFnZg==
evs6OIME2yLCyUChqtQTGtxDh4/6wcspdRw8lh8NGkyLXZQtZ1a7YDehilU2yXH5
YHx8eHsyJydqaWs5JmxrZGd9bCZmbXwma2YnYHx8eCdpaXs=
YHx8eHsyJydpezkmbGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
UWV/BnpHVVhMaH30EU1XA15hAEFOAWIGYHBrcgIuSF0HFhlQZx15Yhhjb3xCHgRfWxV+cQhPS1ICFxRzdkUfeyo2YTNkODhmYS00YmEwLTQ3OWYtOTQyMj1lNWFhYmUxNTg5N2IxMjQ=
CEroA9kVTgd5YW85GtDBLrVZfsAsdrOdkBRjB/Uh1+E=
amwtZ2BvbHZnLWVmYnd2dWYtYGUtYEVmYnd2cWZKbnNvKjZhM2Q4OGZhLTRiYTAtNDc5Zi05NDIyLWU1YWFiZTE1ODk3YjY3
5rPjudJDczZ5DrTBECwfWX3lXIQFlIC/UMsP+phhn+hM5LDHPI8rrfGoWmO4XXwm
YHx8eHsyJydqb2l7JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J2lrfGFnZg==
YHx8eHsyJydqaXo6JmxrZGd9bCZmbXwma2YnYHx8eCdraXo=
YHx8eHsyJydpazombGtkZ31sJmZtfCZrZidpeHgnaWt7

YHx8eHsyJydqb2l6JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J3p7eA==
YHx8eHsyJydvaWs6JmxrZGd9bCZmbXwma2YnaXh4J2lrew==
YHx8eHsyJydpezombGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnaWt8YWdm
YHx8eHsyJydvaXs6JmxrZGd9bCZmbXwma2Yna2dkZG1rfCd4ZH17aXh4J2lrfGFnZg==
5rPjudJDczZ5DrTBECwfWer9fxhAWnoxI7Hr0jS/XKKlD9cg1eZLP+WDaj1U0IQ9
YHx8eHsyJydpazkmbGtkZ31sJmZtfCZrZidpeHgnaWt7
W3v2HgaLzgcTXlUiOoZ7E6RDsIpMd2Glz1MxJdRxdis
YHx8eHsyJydpejombGtkZ31sJmZtfCZrZidrZ2RkbWt8J3hkfXtpeHgnent4

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或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。