南明离火
移动应用检测平台

# ANDROID 静态分析报告


得卡 • v1.4.4

分析日期: 2024-06-04 07:38:07

# 应用概览

| | |
|---|---|
| 文件名称: | com.yokm.dcard_1.4.4.apk |
| 文件大小: | 48.05MB |
| 应用名称: | 得卡 |
| 软件包名: | com.yokm.dcard |
| 主活动: | io.dcloud.PandoraEntry |
| 版本号: | 1.4.4 |
| 最小SDK: | 21 |
| 目标SDK: | 30 |
| 加固信息: | 360加固 加固 |
| 应用程序安全分数: | 51/100 (中风险) |
| 跟踪器检测: | 1/432 |
| 杀软检测: | AI评估：可能有安全隐患 |
| MD5: | e3e5fb618448b5dddf81f9e06a1c4347 |
| SHA1: | 8e640c7e518f997a272be3da3d6[illegible]d7a240d320 |
| SHA256: | 73ab30b222b928b2ded5e65c37[illegible]df0546f2724bdf9f2514c050f218e04f04 |

# 分析结果严重性分布

| 高危 | 警告 | 信息 | 安全 | 关注 |
|---|---|---|---|---|
| 2 | 2 | 1 | 2 | 3 |

# 四大组件导出状态统计

| |
|---|
| Activity组件：38个，其中export的有：8个 |
| Service组件：6个，其中export的有：1个 |
| Receiver组件：3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: False
v4 签名: False
主题: CN=dcard, OU=cd, O=cd, L=cd, ST=sc, C=cn
签名算法: rsassa_pkcs1v15
有效期自: 2023-06-26 03:51:03+00:00
有效期至: 2048-06-19 03:51:03+00:00
发行人: CN=dcard, OU=cd, O=cd, L=cd, ST=sc, C=cn
序列号: 0x1
哈希算法: sha256
证书MD5: d50787d0f04cd9d4b125ed3818c0beac
证书SHA1: 26906aca369ebd406f7f3e47be7ebb1d57331da5
证书SHA256: 9905a7534f8c91b722629eb2ffc108c03a76aa75b03328f767a45f73e8bdc8ee
证书SHA512:
5500d0b1778593e15e97407a79a9d178279845bc8c567ae2e2b7d80173bcf56c3d272d8ad54c58fdb07af9289eb84e42631b87c149ebd5d03a351de186864558

公钥算法: rsa
密钥长度: 2048
指纹: d583457b76782d0803d74b172855d73fc1c6100a86c8c49e265e5c3c136d69a0
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.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.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.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.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.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.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.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.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.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.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.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.yokm.dcard | 未知 | 未知权限 | 来自 android 引用的未知权限。 |
| 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.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。 |
| com.yokm.dcard.permission.GYRECEIVER | 未知 | 未知权限 | 来自 android 引用的未知权限。 |
| 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。 |
| 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。 |
| 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。 |

## 可浏览 Activity 组件分析

| ACTIVITY | INTENT |
|---|---|
| io.dcloud.PandoraEntryActivity | Schemes: r76pfz://, |

## 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 |

## Manifest 配置安全分析

高危: **0** | 警告: **12** | 信息: **0** | 屏蔽: **0**

| 序号 | 问题 | 严重程度 | 描述信息 |
|---|---|---|---|


本报告由南明离火移动安全分析平台生成

| | | | |
|---|---|---|---|
| 1 | 应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.0-5.0.2, [minSdk=21] | 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 | 应用程序数据可以被备份 [android:allowBackup=true] | 警告 | 这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。 |
| 4 | Activity (io.dcloud.PandoraEntryActivity) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.miui.securitycenter.permission.AppPermissionsEditor [android:exported=true] | 警告 | 发现一个 Activity被共享给了设备上的其他应用程序，因此它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。 |
| 5 | Activity (com.yokm.dcard.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。 |
| 6 | Activity (com.yokm.dcard.wxapi.WXPayEntryActivity) 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。 |
| 7 | Activity设置了TaskAffinity属性 (com.igexin.sdk.GActivity) | 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 |
| 8 | Activity (com.igexin.sdk.GActivity) 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 | Service (com.igexin.sdk.GService) 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。 |
| 10 | Activity (com.igexin.sdk.GetuiActivity) 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。 |
| 11 | Activity (com.lianlian.securepay.token.activity.WechatPayActivity) 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。 |
| 12 | Activity (com.alipay.sdk.app.PayResultActivity) 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。 |
| 13 | Activity (com.alipay.sdk.app.AlipayResultActivity) 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。 |


本报告由南明离火移动安全分析平台生成

## 代码安全漏洞检测

高危: **2** | 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<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | 升级会员：解锁高级权限 |
| 2 | 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<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | 升级会员：解锁高级权限 |
| 3 | 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<br>OWASP MASVS: MSTG-STORAGE-3 | 升级会员：解锁高级权限 |
| 4 | 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<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | 升级会员：解锁高级权限 |
| 5 | 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<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | 升级会员：解锁高级权限 |
| 6 | 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<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14 | 升级会员：解锁高级权限 |
| 7 | 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<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | 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<br>OWASP Top 10: M5: Insufficient Cryptography<br>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<br>OWASP MASVS: MSTG-CODE-2 | 升级会员：解锁高级权限 |

| | | | | |
|---|---|---|---|---|
| 10 | 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 |
| 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 | 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<br>OWASP Top 10: M5: Insufficient Cryptography<br>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/libaliyunaf.so | True<br>info<br>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<br>info<br>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<br>info<br>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<br>info<br>二进制文件没有设置运行时搜索路径或 RPATH | None<br>info<br>二进制文件没有设置 RUNPATH | True<br>info<br>二进制文件有以下加固函数: ['__memcpy_chk', '__vsprintf_chk', '__memset_chk'] | False<br>warning<br>符号可用 |
| 2 | arm64-v8a/libAPSE_7.0.1.so | True<br>info<br>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<br>info<br>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<br>info<br>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<br>info<br>二进制文件没有设置运行时搜索路径或 RPATH | None<br>info<br>二进制文件没有设置 RUNPATH | True<br>info<br>二进制文件有以下加固函数: ['__FD_ISSET_chk', '__FD_SET_chk'] | False<br>warning<br>符号可用 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 3 | arm64-v8a/libAPSE_J.so | True<br>info<br>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。 | | False<br>high<br>这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI | Full RELRO<br>info<br>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<br>info<br>二进制文件没有设置运行时搜索路径或 RPATH | None<br>info<br>二进制文件没有设置 RUNPATH | False<br>warning<br>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<br>warning<br>符号可用 |
| 4 | arm64-v8a/libEncryptorP.so | True<br>info<br>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<br>info<br>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<br>info<br>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<br>info<br>二进制文件没有设置运行时搜索路径或 RPATH | None<br>info<br>二进制文件没有设置 RUNPATH | False<br>warning<br>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<br>warning<br>符号可用 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 5 | arm64-v8a/libsecuritydevice.so | True<br>info<br>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<br>info<br>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<br>info<br>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<br>info<br>二进制文件没有设置运行时搜索路径或 RPATH | None<br>info<br>二进制文件没有设置 RUNPATH | True<br>info<br>二进制文件有以下加固函数: ['__memmove_chk', '__memset_chk', '__memcpy_chk', '__vsnprintf_chk', '__strlen_chk'] | False<br>warning<br>符号可用 |
| 6 | arm64-v8a/libtoyger.so | True<br>info<br>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<br>info<br>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<br>info<br>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<br>info<br>二进制文件没有设置运行时搜索路径或 RPATH | None<br>info<br>二进制文件没有设置 RUNPATH | False<br>warning<br>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<br>warning<br>符号可用 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 7 | arm64-v8a/libzkfv_fj.so | True<br>info<br>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。 | | False<br>high<br>这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI | Full RELRO<br>info<br>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<br>info<br>二进制文件没有设置运行时搜索路径或 RPATH | None<br>info<br>二进制文件没有设置 RUNPATH | False<br>warning<br>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<br>warning<br>符号可用 |
| 8 | arm64-v8a/libzkfv_tj.so | True<br>info<br>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。 | | False<br>high<br>这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI | Full RELRO<br>info<br>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<br>info<br>二进制文件没有设置运行时搜索路径或 RPATH | None<br>info<br>二进制文件没有设置 RUNPATH | False<br>warning<br>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<br>warning<br>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 | 8/30 | android.permission.READ_PHONE_STATE<br>android.permission.ACCESS_COARSE_LOCATION<br>android.permission.MODIFY_AUDIO_SETTINGS<br>android.permission.CAMERA<br>android.permission.REQUEST_INSTALL_PACKAGES<br>android.permission.VIBRATE<br>android.permission.GET_TASKS<br>android.permission.WRITE_SETTINGS |

| | | |
|---|---|---|
| 其它常用权限 | 8/46 | android.permission.INTERNET<br>android.permission.ACCESS_NETWORK_STATE<br>android.permission.ACCESS_WIFI_STATE<br>android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.READ_MEDIA_IMAGES<br>android.permission.CHANGE_NETWORK_STATE<br>android.permission.READ_MEDIA_VIDEO<br>android.permission.READ_EXTERNAL_STORAGE |

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 |
|---|---|---|---|
| static.lianlianpay.com | 安全 | 是 | **IP地址:** 115.238.30.76<br>**国家:** 中国<br>**地区:** 浙江<br>**城市:** 杭州<br>**纬度:** 30.293650<br>**经度:** 120.161583<br>**查看:** 高德地图 |
| wap.lianlianpay.com | 安全 | 是 | **IP地址:** 115.238.30.69<br>**国家:** 中国<br>**地区:** 浙江<br>**城市:** 杭州<br>**纬度:** 30.293650<br>**经度:** 120.161583<br>**查看:** 高德地图 |
| haip-fy.lianlianpay.com | 安全 | 是 | **IP地址:** 115.238.30.69<br>**国家:** 中国<br>**地区:** 浙江<br>**城市:** 杭州<br>**纬度:** 30.293650<br>**经度:** 120.161583<br>**查看:** 高德地图 |

## URL 链接安全分析

| URL信息 | 源码文件 |
|---|---|
| • https://registry.npmjs.org/ajv/-/ajv-6.9.1.tgz<br>• https://registry.npmjs.org/<br>• https://registry.npmjs.org/json-stringify-safe/-/json-stringify-safe-5.0.1.tgz<br>• https://feross.org/support<br>• https://registry.npmjs.org/is-stream/-/is-stream-2.0.1.tgz<br>• https://registry.npmjs.org/bson/-/bson-4.6.5.tgz<br>• https://registry.npmjs.org/source-map/-/source-map-0.6.1.tgz<br>• https://registry.npmjs.org/form-data/-/form-data-2.3.3.tgz<br>• https://github.com/sponsors/sindresorhus<br>• https://registry.npmjs.org/lodash.isstring/-/lodash.isstring-4.0.1.tgz<br>• https://registry.npmjs.org/tweetnacl/-/tweetnacl-0.14.5.tgz<br>• https://registry.npmjs.org/core-util-is/-/core-util-is-1.0.2.tgz<br>• https://registry.npmjs.org/long/-/long-4.0.0.tgz<br>• https://registry.npmjs.org/tslib/-/tslib-1.14.1.tgz<br>• https://registry.npmjs.org/lodash.isplainobject/-/lodash.isplainobject-4.0.6.tgz | |


本报告由南明离火移动安全分析平台生成

- https://registry.npmjs.org/jsbn/-/jsbn-0.1.1.tgz
- https://registry.npmjs.org/wx-server-sdk/-/wx-server-sdk-2.6.3.tgz
- https://registry.npmjs.org/base64-js/-/base64-js-1.5.1.tgz
- https://registry.npmjs.org/querystring/-/querystring-0.2.0.tgz
- https://registry.npmjs.org/jsprim/-/jsprim-1.4.2.tgz
- https://registry.npmjs.org/lodash.isnumber/-/lodash.isnumber-3.0.3.tgz
- https://registry.npmjs.org/typescript/-/typescript-4.7.4.tgz
- https://registry.npmjs.org/semver/-/semver-5.7.1.tgz
- https://registry.npmjs.org/request-promise/-/request-promise-4.2.6.tgz
- https://registry.npmjs.org/performance-now/-/performance-now-2.1.0.tgz
- https://registry.npmjs.org/lodash.clonedeep/-/lodash.clonedeep-4.5.0.tgz
- https://registry.npmjs.org/asynckit/-/asynckit-0.4.0.tgz
- https://registry.npmjs.org/has-symbols/-/has-symbols-1.0.3.tgz
- https://registry.npmjs.org/extend/-/extend-3.0.2.tgz
- https://registry.npmjs.org/sax/-/sax-1.2.4.tgz
- https://registry.npmjs.org/has-tostringtag/-/has-tostringtag-1.0.0.tgz
- https://registry.npmjs.org/oauth-sign/-/oauth-sign-0.9.0.tgz
- https://registry.npmjs.org/request/-/request-2.88.2.tgz
- https://registry.npmjs.org/arg/-/arg-4.1.3.tgz
- https://registry.npmjs.org/tcb-admin-node/-/tcb-admin-node-1.23.0.tgz
- https://registry.npmjs.org/jwa/-/jwa-1.4.1.tgz
- https://registry.npmjs.org/agentkeepalive/-/agentkeepalive-4.2.1.tgz
- https://registry.npmjs.org/has/-/has-1.0.3.tgz
- https://github.com/sponsors/RubenVerborgh
- https://registry.npmjs.org/lodash.unset/-/lodash.unset-4.5.2.tgz
- https://registry.npmjs.org/mime-types/-/mime-types-2.1.35.tgz
- https://registry.npmjs.org/yn/-/yn-3.1.1.tgz
- https://registry.npmjs.org/delayed-stream/-/delayed-stream-1.0.0.tgz
- https://registry.npmjs.org/ecdsa-sig-formatter/-/ecdsa-sig-formatter-1.0.11.tgz
- https://registry.npmjs.org/tough-cookie/-/tough-cookie-2.5.0.tgz
- https://registry.npmjs.org/har-validator/-/har-validator-5.1.5.tgz
- https://registry.npmjs.org/jws/-/jws-3.2.2.tgz
- https://registry.npmjs.org/clone/-/clone-2.1.2.tgz
- https://www.patreon.com/feross
- https://registry.npmjs.org/psl/-/psl-1.9.0.tgz
- https://registry.npmjs.org/lodash.merge/-/lodash.merge-4.6.2.tgz
- https://registry.npmjs.org/safe-buffer/-/safe-buffer-5.2.1.tgz
- https://registry.npmjs.org/call-bind/-/call-bind-1.0.2.tgz
- https://registry.npmjs.org/dashdash/-/dashdash-1.14.1.tgz
- https://registry.npmjs.org/buffer-from/-/buffer-from-1.1.2.tgz
- https://registry.npmjs.org/aws4/-/aws4-1.11.0.tgz
- https://registry.npmjs.org/make-error/-/make-error-1.3.6.tgz
- https://registry.npmjs.org/request-promise-core/-/request-promise-core-1.1.4.tgz
- https://registry.npmjs.org/forever-agent/-/forever-agent-0.6.1.tgz
- https://registry.npmjs.org/function-bind/-/function-bind-1.1.1.tgz
- https://registry.npmjs.org/depd/-/depd-1.1.2.tgz
- https://registry.npmjs.org/is-typedarray/-/is-typedarray-1.0.0.tgz
- https://registry.npmjs.org/follow-redirects/-/follow-redirects-1.15.1.tgz
- https://registry.npmjs.org/getpass/-/getpass-0.1.7.tgz
- https://registry.npmjs.org/ecc-jsbn/-/ecc-jsbn-0.1.2.tgz
- https://resource.dekapop.com/privacy/deka/ysxy_wx_dk.html
- https://resource.dekapop.com/privacy/deka/yhxy_wx_dk.html
- https://registry.npmjs.org/is-regex/-/is-regex-1.1.4.tgz
- https://registry.npmjs.org/bignumber.js/-/bignumber.js-9.0.2.tgz
- https://registry.npmjs.org/assert-plus/-/assert-plus-1.0.0.tgz
- https://registry.npmjs.org/fast-deep-equal/-/fast-deep-equal-3.1.3.tgz
- https://registry.npmjs.org/ts-node/-/ts-node-8.10.2.tgz
- https://registry.npmjs.org/source-map-support/-/source-map-support-0.5.21.tgz
- https://registry.npmjs.org/tunnel-agent/-/tunnel-agent-0.6.0.tgz
- https://registry.npmjs.org/verror/-/verror-1.10.0.tgz
- https://registry.npmjs.org/fast-json-stable-stringify/-/fast-json-stable-stringify-2.1.0.tgz
- https://registry.npmjs.org/bluebird/-/bluebird-3.7.2.tgz
- https://github.com/sponsors/epoberezkin
- https://registry.npmjs.org/axios/-/axios-0.21.4.tgz
- https://registry.npmjs.org/get-intrinsic/-/get-intrinsic-1.1.2.tgz
- https://registry.npmjs.org/caseless/-/caseless-0.12.0.tgz

自研引擎-A

| | |
|---|---|
| • https://registry.npmjs.org/lodash.isinteger/-/lodash.isinteger-4.0.4.tgz<br>• https://registry.npmjs.org/lodash/-/lodash-4.17.21.tgz<br>• https://github.com/sponsors/feross<br>• https://registry.npmjs.org/uri-js/-/uri-js-4.4.1.tgz<br>• https://registry.npmjs.org/aws-sign2/-/aws-sign2-0.7.0.tgz<br>• https://registry.npmjs.org/http-signature/-/http-signature-1.2.0.tgz<br>• https://registry.npmjs.org/qs/-/qs-6.5.3.tgz<br>• https://github.com/request/request/issues/3142<br>• https://registry.npmjs.org/diff/-/diff-4.0.2.tgz<br>• https://registry.npmjs.org/lodash.isboolean/-/lodash.isboolean-3.0.3.tgz<br>• https://registry.npmjs.org/buffer-equal-constant-time/-/buffer-equal-constant-time-1.0.1.tgz<br>• https://registry.npmjs.org/uuid/-/uuid-3.4.0.tgz<br>• https://registry.npmjs.org/har-schema/-/har-schema-2.0.0.tgz<br>• https://registry.npmjs.org/safer-buffer/-/safer-buffer-2.1.2.tgz<br>• https://registry.npmjs.org/retry/-/retry-0.12.0.tgz<br>• https://registry.npmjs.org/lodash.includes/-/lodash.includes-4.3.0.tgz<br>• https://registry.npmjs.org/extsprintf/-/extsprintf-1.3.0.tgz<br>• https://registry.npmjs.org/json-bigint/-/json-bigint-1.0.0.tgz<br>• https://registry.npmjs.org/sshpk/-/sshpk-1.17.0.tgz<br>• https://registry.npmjs.org/ieee754/-/ieee754-1.2.1.tgz<br>• https://registry.npmjs.org/stealthy-require/-/stealthy-require-1.1.1.tgz<br>• https://registry.npmjs.org/xml2js/-/xml2js-0.4.23.tgz<br>• https://registry.npmjs.org/ms/-/ms-2.1.2.tgz<br>• https://registry.npmjs.org/xmlbuilder/-/xmlbuilder-11.0.1.tgz<br>• https://registry.npmjs.org/protobufjs/-/protobufjs-6.11.3.tgz<br>• https://registry.npmjs.org/buffer/-/buffer-5.7.1.tgz<br>• https://github.com/sponsors/ljharb<br>• https://registry.npmjs.org/isstream/-/isstream-0.1.2.tgz<br>• https://registry.npmjs.org/bcrypt-pbkdf/-/bcrypt-pbkdf-1.0.2.tgz<br>• https://service.dcloud.net.cn/uniapp/feedback.html<br>• https://v8.dev/blog/math-random<br>• https://registry.npmjs.org/combined-stream/-/combined-stream-1.0.8.tgz<br>• https://registry.npmjs.org/json-schema/-/json-schema-0.4.0.tgz<br>• https://registry.npmjs.org/mime-db/-/mime-db-1.52.0.tgz<br>• https://registry.npmjs.org/debug/-/debug-4.3.4.tgz<br>• https://registry.npmjs.org/humanize-ms/-/humanize-ms-1.2.1.tgz<br>• https://registry.npmjs.org/punycode/-/punycode-1.3.2.tgz<br>• https://registry.npmjs.org/json-schema-traverse/-/json-schema-traverse-0.4.1.tgz<br>• https://registry.npmjs.org/asn1/-/asn1-0.2.6.tgz<br>• https://registry.npmjs.org/lodash.set/-/lodash.set-4.3.2.tgz<br>• https://registry.npmjs.org/lodash.once/-/lodash.once-4.1.1.tgz<br>• https://registry.npmjs.org/url/-/url-0.11.0.tgz<br>• https://registry.npmjs.org/punycode/-/punycode-2.1.1.tgz<br>• https://registry.npmjs.org/jsonwebtoken/-/jsonwebtoken-8.5.1.tgz | |
| • https://gator.volces.com | 自研引擎-M |
| • https://static.lianlianpay.com/privacy.html | com/lianlian/securepay/token/b/b.java |
| • https://haip-ly.lianlianpay.com | com/lianlian/base/iprouter/IPRouterHelper.java |
| • https://static.lianlianpay.com/agreement/installment_agreement.html<br>• https://static.lianlianpay.com/agreement/agreement.html<br>• https://static.lianlianpay.com/agreement/agreement_vp.html | com/lianlian/securepay/token/activity/ProtocolActivity.java |
| • https://wap.lianlianpay.com/bank_list_notitle.html?pro_id=10&oid_partener=<br>• https://wap.lianlianpay.com/more.html?pro_id=10&oid_partener= | com/lianlian/securepay/token/activity/MoreActivity.java |
| • https://render.alipay.com/p/yuyan/180020010001208736/aliyunfacewelcome.html | 自研引擎-S |

## 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。 |
| 金融级实人认证 SDK | Alibaba | 金融级实人认证服务搭载真人检测和人脸比对等生物识别技术，配合权威数据源验证，可快速校验自然人的真实身份。 |
| 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。 |
| 极光认证 SDK | 极光 | 极光认证整合了三大运营商的网关认证能力，为开发者提供了一键登录和号码认证功能，优化用户注册/登录、号码验证的体验，提高安全性。 |
| 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. |
| IJKPlayer | Bilibili | IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。 |
| 360 加固 | 360 | 360 加固保是基于 360 核心加密技术，给安卓应用进行深度加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包、内存抓取等威胁。 |
| 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。 |
| DataFinder | Volcengine | 快速灵活高效的分析模型，发现用户行为数据的价值，进而转化为促进增长的行动。 |
| 移动号码认证 | 中国移动 | 号码认证能力提供一键登录、本机号码校验服务。 |
| 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。 |
| Jetpack Media | Google | 与其他应用共享媒体内容和控件。已被 media2 取代。 |

## 第三方追踪器检测

| 名称 | 类别 | 网址 |
| --- | --- | --- |
| Pangle | Advertisement | https://reports.exodus-privacy.eu.org/trackers/363 |

## 敏感凭证泄露检测

| 可能的密钥 |
| --- |
| 个推-推送服务的=> "GETUI_APPID" : "FYOe1JWaN8AFNgpCLeSoL5" |
| 微信分享的=> "WX_SECRET" : "4443974962260082b70fc719e675fed4" |

| |
|---|
| 卓信ID-SDK的=> "ZX_CHANNEL_ID" : "C01-GEztJH0JLdBC" |
| 个推–推送服务的=> "GY_APP_ID" : "FYOe1JWaN8AFNgpCLeSoL5" |
| 凭证信息=> "RangersAppLogUniPlugin_appid" : "20001693" |
| openinstall统计的=> "com.openinstall.APP_KEY" : "r76pfz" |
| 微信分享的=> "WX_APPID" : "wx9429de9838bee143" |
| 卓信ID-SDK的=> "ZX_APPID_GETUI" : "913e6a50-c3b6-4989-8ac6-1ecb53649be3" |
| DCloud（数字天堂）的=> "dcloud_appkey" : "bd3fdf8392c007403a4878db35f195ae" |
| "dcloud_permissions_reauthorization" : "reauthorize" |
| "umcsdk_oauth_version_name" : "v1.4.1" |
| "dcloud_feature_oauth_weixin_plugin_description" : "wechat" |
| 9f89c84a559f573636a47ff8daed0d33 |
| aHR0cDovL3Rlc3QueWludG9uZy5jb20uY24vZm91cmVsZW1lbnRhcGkvdjEv |
| cd9e459ea708a948d5c2f5a6ca8838cf |
| 1991ad762ee340299f65f1b9c2dea366 |
| 924b250d973d47f7936ee7ae9cac6f03 |
| aHR0cDovL3Rlc3QueWludG9uZy5jb20uY24vZm91cmVsZW1lbnRhcGkvdjEvYXkv |
| aHR0cDovL3Rlc3QueWludG9uZy5jb20uY24vZm91cmVsZW1lbnRhcGkv |
| aHR0cHM6Ly9wYXlzZXJ2ZXJzZGsubGlhbmxpYW5wYXkuY29tL3YxLw== |
| aHR0cHM6Ly9wYXlzZXJ2ZXJzZGsubGlhbmxpYW5wYXkuY29tL3JlcGF5L3YxLw== |

## 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，不得用于非法用途。请遵守《中华人民共和国网络安全法》及相关法律法规。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。