南明离火
移动应用检测平台

ANDROID 静态分析报告

Online Loans • v421.2.42

分析日期: 2025-08-29 15:50:19

应用概览

文件名称:	ph_onlineloans_mobile_android_v421.2.42google.apk
文件大小:	10.48MB
应用名称:	Online Loans
软件包名:	ph.onlineloans.mobile.android
主活动:	ph.onlineloans.mobile.flutter.ph_mobile_flutter.MainActivity
版本号:	421.2.42
最小SDK:	23
目标SDK:	35
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	52/100 (中风险)
跟踪器检测:	4/432
杀软检测:	AI评估：安全
MD5:	e38a0c49612e7a1b18564a9b3aeb2312
SHA1:	250457fd6b5ef84ac62ba9fa6d22afdaa05f7715
SHA256:	e2641de744d2c55fac9e2e207d14116cc253b43474a2151cd7689b0b135c739d

分析结果严重性分布

高危	中危	信息	安全	关注
3	16	1	3	0

四大组件导出状态统计

Activity组件：14个，其中export的有： 0个
Service组件：14个，其中export的有： 0个
Receiver组件：9个，其中export的有： 3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: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2019-04-25 08:12:42+00:00
有效期至: 2049-04-25 08:12:42+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xac2a5279fabd7677789ea42ff7061ead970f1a1c
哈希算法: sha256
证书MD5: 312b5e85d6ca010818b5a80868522259
证书SHA1: 48c79e5792b19b4d4c098b2e8fc86b1ba2903c37
证书SHA256: b44c98ad4db5518020b9e5e65e29f104123d2ffda812b8a11212a1fa5ade11a2
证书SHA512:
7a495317ff0dacf7c86c60464b3ccf434ef1582d10b756a41f39d2f96828377a59c004305eabecb31a1cd39139373bff7e7e94a2e39237b01842ecf1ab058af

公钥算法: rsa
密钥长度: 4096
指纹: 534e3909dc6e279ed7de32f478899c89d3b4587f9b3e79874d214856a[illegible]33971
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.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.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.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.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_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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
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.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。

android.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
android.permission.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
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
com.google.android.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
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.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以测量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
ph.onlineloans.mobile.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.samsung.android.mapsagent.permission.READ_APP_INFO	未知	未知权限	来自 android 引用的未知权限。
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	未知权限	来自 android 引用的未知权限。
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.DETECT_SCREEN_RECORDING	普通	授予应用程序在进行音频或屏幕录制时接收通知的能力	允许应用程序在录制时收到通知。

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: **3** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) 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。
2	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。
3	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [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。

代码安全漏洞检测

高危: **3** | 警告: **11** | 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
2	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

3	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
4	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
5	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
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	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
8	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
9	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
10	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

11	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
12	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
13	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
14	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
15	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
16	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
17	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
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
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集 位置	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
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
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
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
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00034	查询当前数据网络类型	信息收集 网络	升级会员：解锁高级权限
00065	获取SIM卡提供商的国家代码	信息收集	升级会员：解锁高级权限
00079	隐藏当前应用程序的图标	规避	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
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	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
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
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

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
00147	获取当前位置的时间	信息收集 位置	升级会员：解锁高级权限
00175	获取通知管理器并取消通知	通知	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
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
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
00003	将压缩后的位图数据放入JSON对象中	相机	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 文件	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 控制	升级会员：解锁高级权限
00035	查询已安装的包列表	反射	升级会员：解锁高级权限
00043	计算WiFi信号强度	信息收集 WiFi	升级会员：解锁高级权限
00114	创建到代理地址的安全套接字连接	网络 命令	升级会员：解锁高级权限
00064	监控来电状态	控制	升级会员：解锁高级权限
00085	获取ISO国家代码并将其放入JSON中	信息收集 电话服务	升级会员：解锁高级权限
00132	查询ISO国家代码	电话服务 信息收集	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

00189	获取短信内容	短信	升级会员：解锁高级权限
00126	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
00188	获取短信地址	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
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
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	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
00209	从最新渲染图像中获取像素	信息收集	升级会员：解锁高级权限
00210	将最新渲染图像中的像素复制到位图中	信息收集	升级会员：解锁高级权限
00031	检查当前正在运行的应用程序列表	反射 信息收集	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	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
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	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	4/30	android.permission.CAMERA android.permission.WAKE_LOCK android.permission.ACCESS_COARSE_LOCATION android.permission.READ_PHONE_STATE

其它常用权限	8/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH com.google.android.gms.permission.AD_ID com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE 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
sgcdsdk.s	安全	否	No Geolocation information available.
app-measurement.com	安全	是	**IP地址:** 220.181.174.97 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
sdlsdk.s	安全	否	No Geolocation information available.
sars.s	安全	否	No Geolocation information available.
smonitorsdk.s	安全	否	No Geolocation information available.
sregister.s	安全	否	No Geolocation information available.
simpression.s	安全	否	No Geolocation information available.
portal.infobip.com	安全	否	**IP地址:** 3.33.219.3 **国家:** 德国 **地区:** 黑森 **城市:** 美因河畔法兰克福 **纬度:** 50.110882 **经度:** 8.681996 **查看:** Google 地图
goo.gl	安全	否	**IP地址:** 3.33.219.3 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.386051 **经度:** -122.083847 **查看:** Google 地图

api.bureau.id	安全	否	**IP地址:** 104.20.27.68 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
qw.idbur.com	安全	否	**IP地址:** 3.7.97.92 **国家:** 印度 **地区:** 马哈拉施特拉邦 **城市:** 孟买 **纬度:** 19.075973 **经度:** 72.877300 **查看:** Google 地图
svalidate.s	安全	否	No Geolocation information available.
privacy-sandbox.appsflyersdk.com	安全	否	**IP地址:** 18.155.202.44 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
ap.api.fpjs.io	安全	否	**IP地址:** 3.33.219.3 **国家:** 美国 **地区:** 华盛顿 **城市:** 西雅图 **纬度:** 47.604309 **经度:** -122.329842 **查看:** Google 地图
bfp.prd.bureau.id	安全	否	**IP地址:** 172.66.172.227 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
api.stg.bureau.id	安全	否	**IP地址:** 104.20.27.68 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
sconversions.s	安全	否	No Geolocation information available.
sattr.s	安全	否	No Geolocation information available.
sadrevenue.s	安全	否	No Geolocation information available.

score.juicyscore.com	安全	否	**IP地址:** 172.235.56.12 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
api.dev.bureau.id	安全	否	**IP地址:** 172.66.172.227 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
firebase-settings.crashlytics.com	安全	是	**IP地址:** 220.181.174.162 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
slaunches.s	安全	否	No Geolocation information available.
mobile.infobip.com	安全	否	**IP地址:** 3.123.188.246 **国家:** 德国 **地区:** 黑森 **城市:** 美因河畔法兰克福 **纬度:** 50.110882 **经度:** 8.681996 **查看:** Google 地图
docs.flutter.dev	安全	否	**IP地址:** 199.36.158.100 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.386051 **经度:** -122.083847 **查看:** Google 地图
scdn-ssettings.s	安全	否	No Geolocation information available.
sonelink.s	安全	否	No Geolocation information available.
sviap.s	安全	否	No Geolocation information available.
sinapps.s	安全	否	No Geolocation information available.
sapp.s	安全	否	No Geolocation information available.
scdn-stestsettings.s	安全	否	No Geolocation information available.
svalidate-and-log.s	安全	否	No Geolocation information available.

api.fpjs.io	安全	否	**IP地址:** 13.248.176.92 **国家:** 美国 **地区:** 华盛顿 **城市:** 西雅图 **纬度:** 47.604309 **经度:** -122.329842 **查看:** Google 地图
eu.api.fpjs.io	安全	否	**IP地址:** 13.248.176.92 **国家:** 美国 **地区:** 华盛顿 **城市:** 西雅图 **纬度:** 47.604309 **经度:** -122.329842 **查看:** Google 地图
pagead2.googlesyndication.com	安全	是	**IP地址:** 220.181.174.38 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://github.com/zloirock/core-js/blob/v3.32.0/LICENSE • https://kjur.github.io/jsrsasign/licensen • wss://127.0.0.1 • http://lapo.it/asn1js/n • https://spb01-static.juicyscore.com • https://ams01-static.juicyscore.com • https://score.juicyscore.com • https://github.com/zloirock/core-js • https://tools.ietf.org/html/rfc3447 • https://livechat.infobip.com/widget.js • https://kjur.github.io/jsrsasign/license	自研引擎-A
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	C3/C.java
• https://api.dev.bureau.id • https://api.stg.bureau.id • https://api.bureau.id	com/bureau/base/e.java
• https://firebase.google.com/support/guides/disable-analytics	M2/C2501q2.java
• 10.0.2.15	e6/C1619l.java
• 10.0.2.15	e6/l.java
• https://goo.gl/naoooi	M2/o7.java
• https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java

• https://%svalidate-and-log.%s/api/v1.0/android/validateandlog?app_id= • https://%sars.%s/api/v2/android/validate_subscription_v2?app_id= • https://%sonelink.%s/shortlink-sdk/v2 • https://%sars.%s/api/v2/android/validate_subscription?app_id= • https://%sviap.%s/api/v1/android/validate_purchase?app_id= • https://%sgcdsdk.%s/install_data/v5.0/ • https://%sviap.%s/api/v1/android/validate_purchase_v2?app_id=	com/appsflyer/internal/AFd1lSDK.java
• https://docs.flutter.dev/deployment/android#what-are-the-supported-target-architectures	X4/f.java
• https://app-measurement.com/s/d • https://app-measurement.com/a	M2/AbstractC2413f2.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	j1/b.java
• https://qw.idbur.com/topics/aws.msk.bureau.androiddeviceevents • https://bfp.prd.bureau.id/topics/aws.msk.bureau.androiddeviceevents	com/bureau/devicefingerprint/r.java
• https://github.com/infobip/mobile-messaging-sdk-android/wiki/android-manifest-components#push-notifications	org/infobip/mobile/messaging/ConfigurationException.java
• https://mobile.infobip.com/	org/infobip/mobile/messaging/MobileMessagingProperty.java
• https://portal.infobip.com/push/applications	org/infobip/mobile/messaging/MobileMessagingCore.java
• https://eu.api.fpjs.io • https://api.fpjs.io • https://ap.api.fpjs.io	N1/f.java
• https://app-measurement.com/s/d • https://app-measurement.com/a	M2/AbstractC1963f2.java
• https://mobile.infobip.com/	org/infobip/mobile/messaging/api/support/Generator.java
• https://%sapp.%s	com/appsflyer/internal/AFj1fSDK.java
• 127.0.0.1	juicylab/juicyscore/fvtiv.java
• 10.0.2.15	io/seon/androidsdk/service/M.java
• javascript:window.infobipmobilemessaging.readbodyheight	org/infobip/mobile/messaging/interactive/inapp/view/InAppWebViewDialog.java
• https://%scdn-%stestsettings.%s/android/v1/%s/settings • https://%scdn-%ssettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFe1ySDK.java
• https://%smonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFd1uSDK.java

• https://%sregister.%s/api/v • https://privacy-sandbox.appsflyersdk.com/api/trigger • https://%smonitorsdk.%s/api/remote-debug/v2.0?app_id= • https://%sdlsdk.%s/v1.0/android/ • https://%sinapps.%s/api/v • https://%sadrevenue.%s/api/v2/generic/v6.16.2/android?app_id= • https://%svalidate.%s/api/v • https://%sattr.%s/api/v • https://%slaunches.%s/api/v • https://%sconversions.%s/api/v	com/appsflyer/internal/AFj1kSDK.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	K3/g.java
• https://plus.google.com/	S1/n0.java
• 127.0.0.1 • 172.20.10.1 • 192.168.42.254 • 192.168.42.1	io/jsonandroidsdk/service/N3.java
• 8.8.8.8 • 127.0.0.1 • 1.1.1.1	juicylab/juicyscore/Ucgca.java
• https://score.juicyscore.com/internal_mb.html • https://score.juicyscore.com/static/mb.html	juicylab/juicyscore/Juicyscore.java
• https://%s/%s/%s	Y3/c.java

Firebase 配置安全检测

标题	严重程度	描述信息

Firebase远程配置已禁用	安全	Firebase远程配置URL（ https://firebaseremoteconfig.googleapis.com/v1/projects/742200262878/namespaces/firebase:fetch?key=AIzaSyBiDP6LVktbIgd0gm2PpTW9e9qK20MANwY ） 已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Play Services	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。

Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
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。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

第三方追踪器检测

名称	类别	网址
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

敏感凭证泄露检测

可能的密钥
"app_id" : "102461289"
"google_api_key" : "AIzaSyBnDP6LVktbIgd0gm2PpTW9e9qK20MANwY"
"google_app_id" : "1:742200262878:android:599daae9d1722cafa024f"
"google_crash_reporting_api_key" : "AIzaSyBnDP6LVktbIgd0gm2PpTW9e9qK20MANwY"
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
7ce180772162edad1efb2e3b20a732b7
VGhpcyBpcyB0aGUgcHJpbmI4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg
ab067ac0965a0d0bc22b2ac966036da3
3BAF59A2563C1C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkK

FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
470fa2b4ae81cd56ecbcda9735803434cec591fa
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEgyDuy2d0i9oygI9czIibKoJiU0RDEvCfxItNTQAjbynZ6bC1ygeeiX/Ymn9XY3jYR5iu2IGjkr8ZtRJ3wrhZ5A==

Google Play 应用市场信息

标题: Online Loans Pilipinas

评分: 4.503912 **安装:** 5,000,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** ph.onlineloans.mobile.android

开发者信息: ONLINE LOANS PILIPINAS FINANCING INC., ONLINE+LOANS+PILIPINAS+FINANCING+INC., None, https://onlineloanspilipinas.ph, help@olp.ph,

发布日期: 2019年4月28日 **隐私政策:** Privacy link

关于此应用:

菲律宾0%利息在线快速比索现金贷款应用程序。 在进行贷款交易之前，请研究披露声明中的条款和条件。 新客户特别优惠：低至 0% 利息，且无其他费用抵免。对于新的和有价值的重复借款人：贷款金额为 1,000 比索至 30,000 比索。 信用期为90天至720天（例如还款期最短90天，最长720天）。 贷款成本计算： 返还金额=贷款金额（1+贷款期限*利率/100） 所有适用的费用已包含在贷款总成本中。 年利率最大范围为 0% 到 180%。 代表性例子：您申请 10'000 比索在 3 个月内偿还。每月支付 4,833 比索，返还金额为 14,500 比索。年利率为180%。 使用快速预借现金无担保贷款申请来满足您的紧急需求。在发薪日之前拿钱，用于药品、礼物和其他财务需求。当工资不够时，申请可靠且安全的贷款服务。 常见问题解答：比索现金借贷货币应用程序服务的条件 如何通过应用程序申请轻松发薪日在线贷款？ 预支现金的快速流程： 1. 使用您的智能手机或平板电脑。 2. 下载OLP - 快速审批贷款应用程序。 4. 选择您的贷款金额。 5. 5 分钟内填写表格。 6.等待短信审核。 7. 将 1,000 比索 - 30,000 比索的资金存入您的银行账户或电子钱包（GCash 等）。 好处： 每位新客户均享有绝对低的 0% 利率。 无抵押——无担保贷款。 无需花时间去办公室拜访。 没有不便，使用 1 个 id。 首次借款人无需支付其他费用。除了贷款金额外，无需支付任何费用。 批准后5分钟内即时付款。 审批量不断增长。随时开始一段赚大钱的旅程。将您的财务负担从 1,000 比索增加到 30,000 比索。 谁可以获得现金贷款？ 是菲律宾公民，年满 18 岁。 至少有1个id并有一个手机号码。 有工作或自营职业。 您需要什么才能获得个人贷款？ 只有 1 个文档。从列表中选择：驾驶执照 / GSIS / SSS / TIN / 护照 / PRC / UMID / 邮政 ID / PhilHealth ID / 选民 ID / PhilSys ID。 智能手机或平板电脑，或互联网接入。 银行账户或电子钱包（GCash 等）。 借钱的目的是什么？ • 账单。 • 药品。 • 自行车修理。 • 礼物。 • 灾难。 • 闲暇。 如何获得比索贷款？ 将钱存入您的银行帐户或电子钱包（GCash 等）。 要等多久才能收到钱？ 大多数情况下，您会收到自动短信通知；否则，您会接到电话。审核通过后，5分钟即可通过InstaPay获得现金。 我可以借多少现金？ 我们目前首次申请者的可贷款金额范围为 1,000 比索至 7,000 比索。信誉良好的重复借款人最多可借款 30,000 比索。 如何偿还您的信用？ 还款后，请使用您的参考号。您可以选择以下选项： 1. 通过电子钱包（GCash 等）或使用 Dragonpay 的网上银行进行支付。 2. 前往任意7-11，通过DRAGON LOANS使用Cliqq机器。 3. 使用 DRAGONPAY 访问任何 Bayad Centre、LBC、Cebuana、SM 或 Robinsons Payment 中心、RD Pawnshop 和 Palawan Express。 信用应用公司信息： 融资公司地址：601 Summit One Office Tower, 530 Shaw Boulevard, Barangay Highway Hills, Mandaluyong City。 在线贷款 Pilipinas Financing Inc. SEC 注册号：CS201726430。 授权证书#1181。 电子邮件：help@olp.ph

---

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。