南明离火
移动应用检测平台

ANDROID 静态分析报告

JuanHand • v6.4.2

分析日期: 2024-09-29 13:49:28

应用概览

文件名称:	com.juanhand.fast.cash.peso.loan.app_642_apksos.com.apk
文件大小:	23.67MB
应用名称:	JuanHand
软件包名:	com.juanhand.fast.cash.peso.loan.app
主活动:	com.global.loan.activity.ALaunch
版本号:	6.4.2
最小SDK:	21
目标SDK:	34
加固信息:	爱加密5代壳 加固
应用程序安全分数:	39/100 (高风险)
跟踪器检测:	6/432
杀软检测:	经检测，该文件安全
MD5:	a4de77ff69177afde4346bff4893ceb9
SHA1:	38b15a230e7237ab3677eb0b68258cecf2a09343
SHA256:	2d98dcbb4158cc84160dac6eca637d17dd34582c172de1d86463637cc24363a

分析结果严重性

高危	中危	信息	安全	关注
4	15	1	0	2

四大组件信息

Activity组件：106个，其中export的有：2个
Service组件：10个，其中export的有：1个
Receiver组件：7个，其中export的有：3个
Provider组件：3个，其中export的有：0个

证书信息

二进制文件已签名
v1 签名: True

v2 签名: True
v3 签名: True
v4 签名: False
主题: OU=ppd, CN=Hongwu Lu
签名算法: rsassa_pkcs1v15
有效期自: 2019-10-21 03:04:42+00:00
有效期至: 2044-10-14 03:04:42+00:00
发行人: OU=ppd, CN=Hongwu Lu
序列号: 0x58a62562
哈希算法: sha256
证书MD5: 3412cd505aaaf5fd80a5df6890c308bb
证书SHA1: 7ef4a6e4771cd741c8d93e9142832193a61d7537
证书SHA256: cfff917db460d0d2dbf5f692df05fa6341213dd7d3b1261c8916c97fe44be735
证书SHA512:
958b736716c6858cf813eee4643b9275c8110dbc83c10738632684362d1506604c562fde7a8918c61cf93c07e28011c9ce257e131403e62480e53aee3142a4b5

公钥算法: rsa
密钥长度: 2048
指纹: 442cbe24d21f0b0ba2777292be51c740cca6b76bd2c3020cdd5356e7746c722a
找到 1 个唯一证书

应用权限

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.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.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。
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.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
android.permission.PACKAGE_USAGE_STATS	签名	更新组件使用统计	允许修改组件使用情况统计
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.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.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。
com.juanhand.fast.cash.peso.loan.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

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，以衡量广告活动的有效性。
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。

可浏览的Activity组件

ACTIVITY	INTENT
com.global.loan.activity.ALaunch	Schemes: @string/a15://, @string/b7://, @string/b8://, Hosts: @string/b5, @string/ix, @string/b4, Path Prefixes: @string/b6,
com.sensorsdata.analytics.android.sdk.dialog.SchemeActivity	Schemes: sa8ca07aa7://,

网络通信安全

高危: **1** | 警告: **0** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

证书安全分析

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分析

高危: **0** | 警告: **6** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
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	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/c]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
3	Broadcast Receiver (com.globalloan.receiver.SMSBroadcastReceiver) 受权限保护，但是应该检查权限的保护级别 Permission: com.google.android.gms.auth.api.phone.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让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。

4	Activity (com.sensorsdata.analytics.android.sdk.dialog.SchemeActivity) 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。
5	Activity (androidx.compose.ui.tooling.PreviewActivity) 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	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但是应该检查权限的保护级别。Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让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。
7	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让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。
8	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但是应该检查权限的保护级别。Permission: android.permission.DUMP [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让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。

</> 安全漏洞检测

高危: **2** | 警告: **8** | 信息: **1** | 安全: **0** | 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

3	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
4	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
5	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
6	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 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
7	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
8	不安全的Web视图实现。Web视图忽略SSL证书错误并接受自签名SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	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

11	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

动态库分析

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/libliveness detection_v2.7.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。	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	False warning 符号可用

2	arm64-v8a/libMegActionFmpJni.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。		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	False warning 符号可用
3	arm64-v8a/libmegface.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。		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	No RELRO high 此共享对象未启用 RELRO。整个 GOT（.got 和 .got.plt 两者）都是可写的。如果没有此编译器标志，全局变量上的缓冲区溢出可能会覆盖 GOT 条目。使用选项 -z,relro,-z,now 启用完整 RELRO，仅使用 -z,relro 启用部分 RELRO。	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: ['__memcpy_chk', '__memmove_chk', '__vsnprintf_chk', '__vsprintf_chk']	False warning 符号可用

4	arm64-v8a/libtoolChecker.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。		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	False warning 符号可用

敏感权限分析

类型	匹配	权限
恶意软件常用权限	5/30	android.permission.READ_PHONE_STATE android.permission.READ_SMS android.permission.CAMERA android.permission.PACKAGE_USAGE_STATS android.permission.WAKE_LOCK
其它常用权限	7/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE com.google.android.gms.permission.AD_ID android.permission.FOREGROUND_SERVICE com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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。

域名检测

域名	状态	中国境内	位置信息
h5.juanhand.com	安全	是	**IP地址:** 47.88.144.56 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图

sgcdsdk.s	安全	否	No Geolocation information available.
aps-webhandler.appsflyer.com	安全	否	**IP地址:** 13.226.210.33 **国家:** 美利坚合众国 **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
simpression.s	安全	否	No Geolocation information available.
apiuat.juanhand.com	安全	否	**IP地址:** 47.88.144.56 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
bucket-download.slamtec.com	安全	是	**IP地址:** 47.88.144.56 **国家:** 中国 **地区:** 山东 **城市:** 青岛 **纬度:** 36.09[illegible]10 **经度:** 120.37[illegible]41 **查看:** 高德地图
api-idn.megvii.com	安全	否	**IP地址:** 47.88.144.56 **国家:** 印度尼西亚 **地区:** 雅加达雷亚 **城市:** 雅加达 **纬度:** -6.208678 **经度:** 106.845490 **查看:** Google 地图
api.juanhand.com	安全	否	**IP地址:** 10.114.161.188 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
new-juanhand.firebaseio.com	安全	否	**IP地址:** 34.120.206.254 **国家:** 美利坚合众国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
sensors.juanhand.com	安全	否	**IP地址:** 10.114.161.188 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
svalidate-and-log.s	安全	否	No Geolocation information available.
ssdk-services.s	安全	否	No Geolocation information available.

sadrevenue.s	安全	否	No Geolocation information available.
svalidate.s	安全	否	No Geolocation information available.
sattr.s	安全	否	No Geolocation information available.
sinapps.s	安全	否	No Geolocation information available.
fat-api.juanhand.com	安全	否	**IP地址:** 10.114.161.188 **国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看:** Google 地图
sonelink.s	安全	否	No Geolocation information available.
apidev.juanhand.com	安全	否	No Geolocation information available.
userim.juanhand.com	安全	否	**IP地址:** 47.88.144.56 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289087 **经度:** 103.850281 **查看:** Google 地图
new.globe.com.ph	安全	否	**IP地址:** 162.159.136.37 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
slaunches.s	安全	否	No Geolocation information available.
scdn-stestsettings.s	安全	否	No Geolocation information available.
sconversions.s	安全	否	No Geolocation information available.
scdn-ssettings.s	安全	否	No Geolocation information available.
app.juanhand.com	安全	否	No Geolocation information available.
sregister.s	安全	否	No Geolocation information available.
apifat.juanhand.com	安全	否	No Geolocation information available.
sapp.s	安全	否	No Geolocation information available.
privacy-test.juanhand.com	安全	否	**IP地址:** 10.114.30.207 **国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看:** Google 地图

simreg.smart.com.ph	安全	否	**IP地址:** 107.178.248.103 **国家:** 美利坚合众国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
jhdp.ph	安全	否	**IP地址:** 8.212.182.223 **国家:** 菲律宾 **地区:** 国家首都地区 **城市:** 马尼拉纸 **纬度:** 14.604200 **经度:** 120.982201 **查看:** Google 地图
privacy.juanhand.com	安全	否	**IP地址:** 163.181.228.231 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图
smonitorsdk.s	安全	否	No Geolocation information available.

URL链接分析

URL信息	源码文件

• https://h5.juanhand.com/apply/withdraw/add/lazada/ • https://privacy.juanhand.com/html/loan-agreement-seabank.html • https://h5.juanhand.com/apply/confirm • https://web.smileapi.io/v1/smile.v1.js • https://sensors.juanhand.com/sa?project=default • https://github.com/surmon-china • https://privacy.adakami.id/deeplink?page=45&id=1001&s=0&m=0 • https://privacy.juanhand.com/html/privacy.html • http://modernizr.com/ • https://static.juanhand.com/image/j-3%402x.png • https://link.smileapi.io/v1 • https://privacy.juanhand.com/html/user-agreement.html • https://link-sandbox.smileapi.io/v1 • https://privacy.juanhand.com/html/qualification.html • https://h5.juanhand.com/apply/chooseStore • https://github.com/zloirock/core-js/blob/v3.22.3/LICENSE • https://privacy.juanhand.com/html/about.html • https://privacy.juanhand.com/html/calcuFee.html • https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_link-1573913.html • https://h5.juanhand.com/repayment/loan/progress/detail • https://h5.juanhand.com/certification/list • https://privacy.juanhand.com/html/privacy-new.html • https://static.juanhand.com/image/j-6%402x.png • https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_web_all-1573964.html • https://api.juanhand.com • https://privacy.juanhand.com/html/img/logo.png • https://fat-h5.adakami.id/communal/protocol/detail?download=1&title=&doc=https%3A%2F%2Fbucket-in-static-res.oss-ap-southeast-5.aliyuncs.com%2Fhtml%2Fpdf%2FcertificateSample.pdf • https://privacy.juanhand.com/html/privacy-new-sms.html • https://privacy.juanhand.com/h5/index.html • https://play.google.com/store/apps/details?id=com.juanhand.fast.cash.peso.loan.app • https://privacy.juanhand.com/html/loan-agreement-maya.html • https://static.juanhand.com/image/j-1%402x.png • https://privacy.juanhand.com/html/announcement.html?id=136 • https://privacy.juanhand.com/html/facebook.html • https://static.juanhand.com/image/DPO.png • https://github.com/zloirock/core-js • https://privacy.juanhand.com/html/loan_agreement_lightning.html • https://h5.juanhand.com/auth/review • https://h5.juanhand.com/apply/privacyAndLoanAgreement • https://static.juanhand.com/image/j-2%402x.png • https://static.juanhand.com/image/AMLC.png • https://www.baidu.com/ • https://h5.juanhand.com/communal/deeplink/redirect • https://bucket-manila-ph-static-res-test.oss-ap-southeast-6.aliyuncs.com/offlinePackage/permission_policy.zip • http://bucket-manila-ph-static-res.oss-ap-southeast-6.aliyuncs.com/image/N_2x.png • https://h5.juanhand.com/communal/site/message • https://userim.juanhand.com • https://privacy.juanhand.com/html/loan-agreement-entrance.html • https://www.facebook.com/JuanHandOffical/ • https://bucket-in-static-res.oss-ap-southeast-5.aliyuncs.com/html/pdf/certificateSample.pdf • https://h5.juanhand.com/introduction/aboutus • https://static.juanhand.com/image/j-4%402x.png • https://bucket-manila-ph-static-res-test.oss-ap-southeast-6.aliyuncs.com/offlinePackage/zip/react.juanhand.com/current.zip • https://privacy.juanhand.com/dp • https://apifat.juanhand.com • https://h5.juanhand.com/repayment/loan/list/?cacheMode=browser • https://h5.juanhand.com/cancellation/protocol?showNav=1 • https://static.juanhand.com/image/SEC.png • https://h5.juanhand.com/repayment/coupon/list • https://privacy.juanhand.com/html/friend.html	自研引擎-A

• http://h5.juanhand.com/apply/loanprocessdetail • http://h5.juanhand.com/repayment/installmentdetail	com/global/loan/viewmodel/HomeViewModel$handleLoanCardDetailButtonClick$1.java
• https://%sregister.%s/api/v	com/appsflyer/internal/AFg1nSDK.java
• https://%smonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFd1aSDK.java
• https://www.baidu.com/ • https://t7.baidu.com/it/u=1595072465,3644073269&fm=193&f=gif	com/global/loan/viewmodel/HomeViewModel.java
• https://privacy.juanhand.com/html/privacy.html • https://privacy.juanhand.com/h5/index.html#/appauthoritystatement-v4 • https://privacy.juanhand.com/html/user-agreement.html • https://privacy.juanhand.com/h5/index.html#/appauthoritystatement-sms • https://privacy.juanhand.com/html/qualification.html • https://privacy.juanhand.com/h5/index.html#/qalist • https://privacy.juanhand.com/html/about.html • https://privacy.juanhand.com/h5/index.html#/guide/howtoloan • https://h5.juanhand.com/cancellation/protocol • https://h5.juanhand.com/repayment/loan/progress/detail • https://h5.juanhand.com/certification/list • https://userim.juanhand.com/ • https://privacy.juanhand.com/html/privacy-new.html • https://h5.juanhand.com/apply/loanprocessdetail • https://h5.juanhand.com/apply/privacyandloanagreement • https://privacy.juanhand.com/html/privacy-new-sms.html • https://h5.juanhand.com/repayment/loan/list • https://privacy.juanhand.com/html/facebook.html • https://privacy.juanhand.com/html/calcufee.html • https://privacy.juanhand.com/html/loan-agreement.html • https://privacy.juanhand.com/h5/index.html#/appauthoritystatement-new • https://privacy.juanhand.com/h5/index.html#/appauthoritystatement-gps • https://h5.juanhand.com/communal/site/message • https://h5.juanhand.com/apply/pplloanapply • https://h5.juanhand.com/introduction/aboutus • https://privacy.juanhand.com/h5/index.html#/appauthoritystatement • https://privacy.juanhand.com/html/friend.html	com/global/loan/util/C5.java
• https://t7.baidu.com/it/u=963301259,1983296977&fm=193&f=gif • https://t7.baidu.com/it/u=916730607,[illegible]&fm=193&f=gif • https://t7.baidu.com/it/u=1595072465,3644073269&fm=193&f=gif	com/global/loan/composition/banner/BannerKt.java
• https://privacy.juanhand.com/image/20call.png	com/global/loan/model/bean/api/QueryGoodsList.java
• http://121.41.76.188/creditmanager/v1.0.0/creditmanager-1.0.0.apk	com/global/loan/model/bean/api/VerUpgrade.java
• https://api-idn.megvii.com	com/global/loan/activity/AStartLiveness.java
• https://privacy.juanhand.com/dp?p=4 • https://www.baidu.com • https://privacy.juanhand.com/dp?p=7 • http://172.20.128.46:8006/turnplate/turnplate.html • https://privacy.juanhand.com/dp?p=5&id=1&s=3 • https://privacy.juanhand.com/dp?p=1 • https://privacy.juanhand.com/dp?p=3 • https://privacy.juanhand.com/dp?p=6 • www.baidu.com • https://privacy.juanhand.com/dp?p=2	com/global/loan/model/bean/api/QueryMsgList.java
• https://%sapp.%s	com/appsflyer/internal/AFj1qSDK.java

• http://app.juanhand.com/privacy.html • https://privacy.juanhand.com/offlinepackage/permission_policy/index.html	com/global/loan/controller/Controller$queryAuthorizeInfo$2.java
• https://bucket-ph-static-res.oss-cn-hongkong.aliyuncs.com/image/facebook.png	com/global/loan/model/bean/api/GetRepayChannelList.java
• https://%sonelink.%s/shortlink-sdk/v2 • https://%svalidate-and-log.%s/api/v1.0/android/validateandlog?app_id= • https://%sgcdsdk.%s/install_data/v5.0/	com/appsflyer/internal/AFe1ySDK.java
• https://www.baidu.com	com/global/loan/model/bean/api/GetRepayCodeByChannel.java
• https://privacy.juanhand.com/image/facebook.png	com/global/loan/model/bean/api/CertItemList.java
• 127.0.0.1	com/snail/antifake/deviceid/IpScanner.java
• https://%sadrevenue.%s/api/v2/generic/v6.14.0/android?app_id= • https://%sadrevenue.%s/api/v2/log/adimpression/v6.14.0/android?app_id= • https://%ssdk-services.%s/validate-android-signature • https://%slaunches.%s/api/v • https://%svalidate.%s/api/v • https://%sattr.%s/api/v • https://%sinapps.%s/api/v • https://aps-webhandler.appsflyer.com/api/trigger • https://%smonitorsdk.%s/api/remote-debug/v2.0?app_id= • https://%sconversions.%s/api/v	com/appsflyer/internal/AFj1xSDK.java
• https://privacy.juanhand.com • https://www.baidu.com • https://privacy-test.juanhand.com • http://172.20.128.141:8080 • https://jhdp.ph?p= • http://172.20.129.155:3000/ • http://172.20.128.141:8080/loan-agreement.html • https://bucket-download.slamtec.com/68b1f506b9f1036892dcf6d0fd463c9c0d2aec0d/lm310_slamtec_rplidarkit_usermanual_a3m1_v1.3_cn.pdf	com/global/loan/activity/ADebug.java
• https://docs.google.com/viewer?embedded=true&url=	com/global/loan/activity/AGoogleDocWeb.java
• https://privacy.juanhand.com/image/facebook.png	com/global/loan/model/bean/api/GetIdTypeDictionary.java
• http://172.20.128.46:8005/turnplate/turnplate.html	com/global/loan/model/bean/api/Activity.java
• https://www.baidu.com	com/global/loan/model/bean/api/GetExtensionRepayCodeByChannel.java
• https://firebase.google.com/docs/crashlytics/get-deobfuscated-reports?platform=android	com/global/loan/activity/ACrashlytics.java
• https://api-idn.megvii.com	com/global/loan/activity/ActivityFaceStart.java
• https://api-idn.megvii.com	com/global/loan/activity/ActivityFaceStartForOld.java
• https://sensors.juanhand.com/sa?project=production	com/global/loan/thirdpart/SensorsDataUtil.java

• https://api-idn.megvii.com	com/global/loan/activity/progress/v4/ActivityFaceStartV4.java
• https://www.baidu.com • https://privacy.juanhand.com/dp?p= • https://privacy.juanhand.com/dp?p=3 • www.baidu.com • https://privacy.juanhand.com/dp?p=2	com/global/loan/model/bean/api/FullMemberMessage.java
• https://new.globe.com.ph/simreg • https://simreg.smart.com.ph	com/global/loan/dialog/FSimRegisterDialog$registerSim$1.java
• https://%scdn-%ssettings.%s/android/v1/%s/settings • https://%scdn-%stestsettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFe1gSDK.java
• https://apidev.juanhand.com • http://fat-api.juanhand.com • https://apiuat.juanhand.com • http://app.juanhand.com/dialogs/interestfree.html • https://api.juanhand.com • https://apifat.juanhand.com	com/global/loan/controller/Controller.java
• http://app.juanhand.com/dialogs/applyinginterestfree.html	com/global/loan/activity/ABaseInfo.java
• https://api.juanhand.com • http://172.20.131.214:8080/repayment/extension/apply?debtid=2963&loanamount=1234511	com/global/loan/model/Model.java
• https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
• https://userim.juanhand.com/	com/global/loan/model/bean/api/UserConf.java
• www.facebook.com • https://github.com/vinc3m1/roundedimageview.git • https://github.com/vinc3m1 • https://github.com/vinc3m1/roundedimageview • https://new-juanhand.firebaseio.com	自研引擎-S

FIREBASE数据库分析

标题	严重程度	描述信息

第三方SDK

SDK名称	开发者	描述信息
旷视 SDK	旷视	检测图片或视频流中的人脸，支持针对检测出的人脸进行属性分析。
AntiFakerAndroidChecker	happylishang	Android 模拟器检测，检测 Android 模拟器，作为可信 DeviceID，应对防刷需求等。
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。
RootBeer	Scott Alexander-Bown	A tasty root checker library and sample app. We've scoured the internets for different methods of answering that age old question... Has this device got root?

Jetpack Compose	Google	Jetpack Compose 是用于构建原生 Android 界面的新工具包。Jetpack Compose 使用更少的代码、强大的工具和直观的 Kotlin API 简化并加快了 Android 上的界面开发。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。
Google Sign-In	Google	提供使用 Google 登录的 API。
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。
神策分析 SDK	神策	神策分析，是针对企业级客户推出的深度用户行为分析产品，支持私有化部署，客户端、服务器、业务数据、第三方数据的全端采集和建模，驱动营销渠道效果评估、用户精细化运营改进、产品功能及用户体验优化、老板看板辅助管理决策、产品个性化推荐改造、用户标签体系构建等应用场景。作为 PaaS 平台支持二次开发，可通过 BI、大数据平台、CRM、ERP 等内部 IT 系统，构建用户数据体系，让用户行为数据发挥深远的价值。
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 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 Performance	Google	Firebase 性能监控服务可帮助您深入了解您的 iOS 应用、Android 应用和网页应用的性能特点。
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）是一款免费的应用测量解决方案，可提供关于应用使用情况和用户互动度的分析数据。

邮箱

EMAIL	源码文件
luhongwu@ppdai.com	com/global/loan/model/bean/api/QueryMsgList.java
luhongwu@ppdai.com	com/global/loan/model/bean/api/FullMemberMessage.java

追踪器

名称	类别	网址
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sensors Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/248

密钥凭证

可能的密钥
"google_api_key" : "AIzaSyD0eGSKm33CbcIsfL4NuLCDC4cLQW3ATDQ"
"firebase_database_url" : "https://new-juanhand.firebaseio.com"
"google_crash_reporting_api_key" : "AIzaSyD0eGSKm33CbcIsfL4NuLCDC4cLQW3ATDQ"
809bd36cf78612fd1f11b739c382bfac
5f389fef5fd41c84a33a91c6574cbf51
bc8f6a70d138545889109d126886bd98
b62f7aea9613b98976498a9ecabe537b
6d906db145cb4547aba86ddf75edfcef
b3c61531d3a785d8af140218304940e5b24834d3
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
68b1f506b9f9036892dcf6d0fd463c0c0d2aec0d
a01625815f3428cb69100cc5d613fa7d
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6E[illegible]27E0FDC1
W6VLf6PitAlkKiFuVXBeTe54CSc8jB
8cd0604ba33e2ba7f38a56f0aec08a54
FBA3AF4E7757D9016E953FB3EE4671CA2BD[illegible]F725F9A53D52ED4A38EA[illegible]A08201
49668163590f816aaf863df014568115
889109d126886bd98bc8f6a70d138545
e2380b201325a8f2526[illegible]350338eeae8
37dbd151eb3ca24477bc27cf0febcbe3
3412CD505[illegible]AAF5FD80A5DF6890C3085F
cb072839e1e240a23baae123ca6c[illegible]165

GooglePlay应用信息

标题: JuanHand-Mobile Cash Loan App

评分: 4.437875 **安装:** 5,000,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** com.juanhand.fast.cash.peso.loan.app

开发者信息: Wefund Lending corp, Wefund+Lending+corp, None, http://www.juanhand.com, cs@ph.juanhand.com,

发布日期: 2019年11月29日 **隐私政策:** Privacy link

关于此应用:

□□JuanHand产品介绍： 贷款金额：2,000.00 比索 - 25,000.00 比索 贷款期限：91天-180天 最高年利率：30% 交易费用：0 例如： 91天（3个月）贷款，利率12%，本金为₱10000 总利息费用：₱10000*12%/365*91= ₱299.17 服务费10%：10000₱10%=1000₱1000 还款总额：₱10000*12%/365*91+10000+1000=₱11299.17 每月还款额：₱11299.17/3=₱3766.39 □□JuanHand获得SEC许可的公司名称：WeFund Lending Corp. 我们的SEC 注册号CS201825672，授权证书编号： 2844 注意：在进行任何交易之前，请务必研究条款和条件以及披露声明。https://privacy.juanhand.com/html/privacy.html □□为什么要使用JuanHand现金贷应用程序？ JuanHand是您现金贷款的合作伙伴。它是菲律宾独特的金融科技平台之一，随时随地为您提供安全、便捷的在线现金贷款服务。 □□ 贷款申请要求： □ 18岁以上 □ 菲律宾公民 □ 拥有 1 个政府颁发的身份证件 □ 有稳定的收入 □□现金贷款流程有多简单？ • 下载JuanHand网贷APP • 在JuanHand贷款应用程序中填写我们的快速贷款申请表 • 等待评估 • 快速将现金直接发送至您的银行账户/Gcash/Coins ph □ 娟手优势： □□便捷的在线应用程序 □即时现金贷款 □□简单的比索罗流程 □ 轻松审批 □□联系我们： 如有任何问题、反馈或犹豫，请通过以下方式联系我们： □脸书：@JuanHandOfficial □□网站：www.juanhand.com □ 客服电话：+63285390150 □电子邮件：cs@juanhand.com □□地址：Trade and Financial Tower, 32nd St.科。第七大道，BGC 塔吉格，菲律宾 1630

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。