南明离火

移动应用检测平台

ANDROID 静态分析报告

Súper Préstamo • v1.9.1

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2025-08-28 12:20:25

应用概览

文件名称:	com.pf.prestafast.apk
文件大小:	23.5MB
应用名称:	Súper Préstamo
软件包名:	com.pf.prestafast
主活动:	com.pf.prestafast.view.activity.SplashActivity
版本号:	1.9.1
最小SDK:	21
目标SDK:	35
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	62/100 (低风险)
跟踪器检测:	7/432
杀软检测:	AI评估：可能有安全隐患
MD5:	ddc742b7aa1b49141f277ef559c9b4d1
SHA1:	bec0ed41158203ff64ca56fc369cfd8d4370f976
SHA256:	ff781ff366045be6615837b26a7256790d53c419fa004148b7ce1df21eff419

分析结果严重性分布

高危	中危	信息	安全	关注
1	9	1	3	0

四大组件导出状态统计

Activity组件：35个，其中export的有： 1个
Service组件：10个，其中export的有： 1个
Receiver组件：5个，其中export的有： 2个
Provider组件：6个，其中export的有： 0个

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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: 2021-11-30 10:04:50+00:00
有效期至: 2051-11-30 10:04:50+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xd16837c0b1eb5f9f9b791684682e7fb1865029f0
哈希算法: sha256
证书MD5: 17f560c57f5109743e2bf67616896a95
证书SHA1: 4c6d246fc5f4a0f4d9fecf4ad70919e7d2654a68
证书SHA256: 5ff0f0d04e99661858d76e5dcc2dfa894948c92f52d26f7f16b716f4f459f0ad
证书SHA512:
632d84b161afc5d0bc2e2b76d085bac9f71e159a36b3fb8e1b19df77d8be6132d03cffa46472f891e0a8086f69cb1882d88ff55629476812f811050702e2bd3

公钥算法: rsa
密钥长度: 4096
指纹: 993ad8d1dc155412836d5bb2d7f75ed1c56c4d9226aae47b161f5fa74a3e2024
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.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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
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.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.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.LOCAL_MAC_ADDRESS	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

android.permission.CALL_PRIVILEGED	签名(系统)	直接拨打任何电话号码	允许应用程序在您不介入的情况下拨打任何电话（包括紧急呼救）。恶意应用程序可借此向应急服务机构拨打骚扰电话甚至非法电话。
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.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.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.pf.prestafast.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.pf.prestafast.view.activity.SplashActivity	Schemes: superpapps://, Hosts: prestafast.com, Path Prefixes: /splash,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.pf.prestafast,

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: 5 | 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
本报告由南明离火移动安全分析平台生成

1	应用已配置网络安全策略 [android:networkSecurityConfig=@7F130001]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
2	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
3	Service (com.pf.prestafast.gms.MyFirebaseMessagingService) 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。
4	Activity (com.facebook.CustomTabActivity) 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	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。
6	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: **0** | 警告: **3** | 信息: **1** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
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	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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

4	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
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	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

应用行为分析

编号	行为	标签	文件
00183	获取当前相机参数并更改设置	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
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
00054	从文件安装其他APK	反射	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
00013	读取文件并将其放入流中	文件	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
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
00191	获取短信收件箱中的消息	短信	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

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
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	6/30	android.permission.CALL_PHONE android.permission.CAMERA android.permission.ACCESS_COARSE_LOCATION android.permission.READ_SMS android.permission.READ_CALL_LOG android.permission.WAKE_LOCK
其它常用权限	8/46	android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.INTERNET android.permission.BLUETOOTH com.google.android.gms.permission.AD_ID android.permission.ACCESS_NETWORK_STATE 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
server.superpapps.com	安全	否	**IP地址:** 18.154.144.76 **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-prestafast-dc.mx.test.ksmdev.top	安全	否	**IP地址:** 52.13.181.202 **国家:** 美国 **地区:** 俄勒冈 **城市:** 波特兰 **纬度:** 45.523460 **经度:** -122.676468 **查看:** Google 地图
www.superpapps.com	安全	否	**IP地址:** 18.154.144.55 **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

URL 链接安全分析

URL信息	源码文件

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

• https://play.google.com/store/apps/details • javascript:livingsuccess • https://play.google.com/store/apps/details?id=	com/pf/prestafast/view/activity/WebViewActivity.java
• https://www.superpapps.com/#/newpravcy	com/pf/prestafast/view/activity/SplashActivity.java
• https://server.superpapps.com/ • http://api-prestafast-dc.mx.test.ksmdev.top/	com/pf/prestafast/mryt/network/mryt Config/UrlConfig.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/535105867622/namespaces/firebase:fetch?key=AIzaSyAR_fj0SFoxCGav2wJLhRQVfbYDW2buVcQ ） 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
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 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。
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	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。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本的 Android 屏幕适配方案。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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 AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
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
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Places		https://reports.exodus-privacy.eu.org/trackers/69
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
"com.google.firebase.crashlytics.mapping_file_id" : "2f6709ad9c1a4463a11edf0d72c5d3f3"
"google_api_key" : "AIzaSyAR_fj0S[illegible]Gav2wJLhRQVfbYDW2buVcQ"
"google_app_id" : "1:635105867622:android:33a20d72ede[illegible]72f6317aa7"
"google_crash_reporting_api_key" : "AIzaSyAR_fj0S[illegible]xCGav2wJLhRQVfbYDW2buVcQ"
8a3c4b262d721[illegible]d49a4bf97d5213199c86[illegible]2b9
5e8f16062ea3[illegible]cd2c4a0d547876baa6[illegible]bf625
df6b721c8b4d3b6eb44c861d441500[illegible]7e5a35fc95
a4b7452e2ed8f5f191058ca7[illegible]bfd26b0d3214bfc
cc2751449a350[illegible]8859[illegible]0264ed76692694a80308a
36aa2ade[illegible]b67bd4bcf613253074af
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

8a01304b6428d3ab5283e1cc10122b1d
9b8f518b086098de3d77736f9458a3d2f6f95a37

Google Play 应用市场信息

标题: Crédito Loan - Súper Préstamo

评分: 4.774818 **安装:** 1,000,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** com.pf.prestafast

开发者信息: Presta Fast, Presta+Fast, None, https://www.superpapps.com/, superprestamo@outlook.com,

发布日期: None **隐私政策:** Privacy link

关于此应用:

超级贷是一款简单可靠的在线个人贷款移动应用程序！为墨西哥人提供明智且可靠的贷款。 费率说明： 贷款金额：$1000-$20,000； 贷款期限：91至180天； 最高年利率（APR）：20%； 服务费只需$5！ ！ ！ 成本示例： 如果贷款金额为1000墨西哥比索，则贷款期限为91天； 您只需支付的利息为 1000 * 91 * 0.05% = 45.5 MXN 美元， 退款总额为：1,000 + 45.5 = 1,045.5 墨西哥比索 年利率（APR）：20%。每月付款金额为 45.5 墨西哥比索。 要求 18岁或以上； 无需信用证明。 学分 及时还款有助于获得更高的信用额度。 付款方式 AppName是专门为墨西哥人设计的，因此我们提供最便捷的支付方式来方便您的付款。 ①银行转账（SPEI）：您足不出户即可通过BBVA、Banamex、Banco Azteca、Santander、Banorte、HSBC等电子银行或手机应用程序进行电子转账。 ② OXXO Pay：只需携带您的付款参考到最近的OXXO即可。 联系我们 电子邮件：superprestamo@outlook.com 地址：Centeno 768, Granjas México, Iztacalco, 08400 墨西哥城, CDMX

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。

© 2025 南明离火 - 移动安全分析平台自动生成。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成