南明离火
移动应用检测平台

ANDROID 静态分析报告

PrestaMax • v1.0.9

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 11:58:41

应用概览

文件名称:	com.prestamx.max.apk
文件大小:	12.81MB
应用名称:	PrestaMax
软件包名:	com.prestamx.max
主活动:	com.prestamx.max.MainActivity
版本号:	1.0.9
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	52/100 (中风险)
跟踪器检测:	2/432
杀软检测:	6 个杀毒软件报毒
MD5:	9f4ccaf5796b2f3093bec1fd26bfad3e
SHA1:	3bf328cf7e287e6d5c3663fe9eb2f05ca6a54285
SHA256:	4bbea8a3d3c60a44a55a882473b49d37720a6af3f552a1d8b3517a30f916e615

分析结果严重性分布

高危	中危	信息	安全	关注
2	15	2	2	0

四大组件导出状态统计

Activity组件：26个，其中export的有： 1个
Service组件：12个，其中export的有： 1个
Receiver组件：12个，其中export的有： 3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

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=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2023-07-21 10:54:14+00:00
有效期至: 2053-07-21 10:54:14+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xc96a92cfbbb865555bfee74b0725ab9d7e273913
哈希算法: sha256
证书MD5: 019529822ef304825310bf25f75806e0
证书SHA1: 1399532d85c711f53748ce394b8f6505add9e5b4
证书SHA256: b5c032b039aff0a8349848d0d92c067798a9513f828d77d76d524a3e07f8fb49
证书SHA512:
68183d851d6fed771997fbcec7d3cb49945503933a95443a65dacd0ef59e99a63f7f9fa7f219b7ef3c94a039c4316c1c3e5d4a0[illegible]3072b48cfa0617ae2e8e

公钥算法: rsa
密钥长度: 4096
指纹: 281a80a26d52c9aa60044b272917a14eb29b7c984f5bb695e759671c3a0e64a7
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.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.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.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.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.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
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.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_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。

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.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.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.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_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。
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。
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
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）
com.prestamx.max.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.prestamx.max.MainActivity	Schemes: maxapp://, Hosts: maxhostappclient, Path Prefixes: /openapp,

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**

本报告由南明离火移动安全分析平台生成

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: **7** | 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	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	Activity (com.prestamx.max.activity.DelAccountSmsActivity) 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。
4	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。
5	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 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.work.impl.diagnostics.DiagnosticsReceiver) 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。

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

7	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: **2** | 警告: **6** | 信息: **2** | 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	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
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	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
5	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
6	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	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

7	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
8	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
9	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
10	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
11	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

应用行为分析

编号	行为	标签	文件
00036	从 res/raw 目录获取资源文件	反射	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
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
00013	读取文件并将其放入流中	文件	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

00012	读取数据并放入缓冲流	文件	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
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
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
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
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00134	获取当前WiFi IP地址	WiFi 信息收集	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
00191	获取短信收件箱中的消息	短信	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
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
00189	获取短信内容	短信	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
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	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
00091	从广播中检索数据	信息收集	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

00025	监视要执行的一般操作	反射	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
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

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.CAMERA android.permission.READ_SMS android.permission.SYSTEM_ALERT_WINDOW android.permission.VIBRATE android.permission.ACCESS_COARSE_LOCATION android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	9/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.ACCESS_WIFI_STATE com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.gms.permission.AD_ID android.permission.FOREGROUND_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
sinapps.s	安全	否	No Geolocation information available.
sonelink.s	安全	否	No Geolocation information available.
simpression.s	安全	否	No Geolocation information available.
scdn-ssettings.s	安全	否	No Geolocation information available.
sadrevenue.s	安全	否	No Geolocation information available.
sgcdsdk.s	安全	否	No Geolocation information available.
axpre.s	安全	否	No Geolocation information available.

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

sattr.s	安全	否	No Geolocation information available.
sdlsdk.s	安全	否	No Geolocation information available.
ssdk-services.s	安全	否	No Geolocation information available.
sars.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.
sregister.s	安全	否	No Geolocation information available.
sviap.s	安全	否	No Geolocation information available.
smonitorsdk.s	安全	否	No Geolocation information available.
slaunches.s	安全	否	No Geolocation information available.
svalidate.s	安全	否	No Geolocation information available.
sconversions.s	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://%sapp.%s	com/appsflyer/internal/AFg1zSDK.java
• https://%sattr.%s/api/v • https://%sdlsdk.%s/v1.0/android/ • https://%ssdk-services.%s/validate-android-signature • https://%sinapps.%s/api/v • https://%sars.%s/api/v2/android/validate_subscription?app_id= • https://%sviap.%s/api/v1/android/validate_purchase?app_id= • https://%sars.%s/api/v2/android/validate_subscription_v2?app_id= • https://%sconversions.%s/api/v • https://%sadrevenue.%s/api/v2/log/adimpression/v6.12.3/android?app_id= • https://%sviap.%s/api/v1/android/validate_purchase_v2?app_id= • https://%slaunches.%s/api/v • https://%svalidate.%s/api/v • https://%sadrevenue.%s/api/v2/generic/v6.12.3/android?app_id=	com/appsflyer/internal/AFg1wSDK.java
• https://%scdn-%ssettings.%s/android/v1/%s/settings • https://%scdn-%stestsettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFd1ySDK.java
• https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
• https://%xpre.%s/stam/	com/prestamx/max/java_calss/vikxvh.java
• https://%smonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFc1pSDK.java

本报告由南明离火移动安全分析平台生成

• https://%smonitorsdk.%s/remote-debug?app_id= • https://%sonelink.%s/shortlink-sdk/v2 • https://%sgcdsdk.%s/install_data/v5.0/	com/appsflyer/internal/AFc1oSDK.java
• https://%sregister.%s/api/v	com/appsflyer/internal/AFe1sSDK.java
• https://axpre.%s/stam/	com/prestamx/max/java_calss/ksocihbb.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/133730352502/namespaces/firebase:fetch?key=AIzaSyBbtYLqdxwxh0V8O_37UYcZTvnzCPwg2s ） 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 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。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
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 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。

本报告由南明离火移动安全分析平台生成

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 Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
"google_api_key" : "AIzaSyBbtYLqdxwxh0V8Q_f37UYcZTvnzCPwg2s"
"google_app_id" : "1:133730352502:android:e8a8ce91358c3c8a4ace57"
"google_crash_reporting_api_key" : "AIzaSyBbtYLqdxwxh0V8Q_f37UYcZTvnzCPwg2s"
68HDpV9YK1g6GSAIiLc/S68CFhsN76AUilVJyLhvgZo=
62khOpNX6oXW8WKtZsnuDb3eVcrxQL5uSMtMbmO6Hf4=
rWPBXEoLkhlZQV8u3BHjyaZqkRni6OfUr/dkjL25f5w=
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC4327ED0FDC1
6SSu7jnG1m+gOhTWwiUC3zk5Gwprx8eUS9uPi2i4xlg=
9dc3c5d73af5bb259afdba155f5fcc7b
aR+oaYq8xRvykWjmEKFDCRG5DloZNbJiICJhNX5S0XI=
Igp/Fewy+xBi4ii30UAjU0ELwkYfUE307EzOfbvSYJ4=
STzszbAIFM87pbbvtCMkbcKWpsBY8zNFQlNTnlhBIGSn3EfbJX5pQVj6jJ6eiQx
ljS9gJrKI4IV7+fFX8SK9ROOMOosdYNBD795MAgxaCI=
oBmGmKOfwzyzObO1RKzmD03PoftkWQlTYWx5uKqFy8o=
FFE391E0EA186[illegible]073ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
FBA3AF4E7757D9016E953FB3EE467[illegible]A2BD9AF725F9A53D52ED4A38EAAA08901
zfLMwQNcxmnP9YQ298xVev[illegible]5v[illegible]m9seey233XjbDTX3g=
P7CtgNlvl1ZZzS8[illegible]se+0TBPEuGNJyL7f4YE7Nxki/SI=
VMaV5jmwzdQj[illegible]6G7TE2WSQf2FWwkH4suLVg4Zrn7c=
6SSu7jnG1m+gOhTWwiUC3xG1HXZccOMyaiNPxEuThHI=
ccf689421bb4ab9a0d8357eaf2f437ff

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

Hl6/+FlieXvQfoHoAS2U5t6Oyp8LLcbMp+NOIJhhooU=
rd8TTTFJn6Vx6h0YQnM6FHftVqS/Wemmcfmtozwcrdk=
hW2uKob8L3MJ64aBXZ+I/Q==
NtwThYl5HPykL8SasJSVxtQz9KO49y4v0TuXbHDNzM0=
xy1KJsGe6eij0TXBkuXv1ZHoWp+yvLWIO9zTL0onHoo=
WHH4uAcHAlvtzJFdtixvPzjO2JFid8clyDaAwXJyzcw=
Ba2pS5+soQg6GgDaND9SfS5oz+sU+pD1JJl+QElVsx4=
PhjqiZWakLJrSq+cXsF1hOv7e3AayCQRe/lBtNP+gZY=
afq8gapGQHV3gXp85BI7dMzeBd6Hi0V0mG93ODm+okLFK0nA0Ie/n+PGX77deXWK
hP3cs11l+6fNUCol7ZDrVA8rylCHEx0pjbQdAWxsrsc=
XkXSicu2M8i2GgH2pOobzA9KHvB0RnQ28EFaAgGMjahFk8cn7FAsonsSApuN1Qc2
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F

Google Play 应用市场信息

标题: PrestaMax - Préstamos Flash

评分: 4.6207 **安装:** 1,000,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** com.prestamx.max

开发者信息: RIZKY RAMADHAN, RIZKY+RAMADHAN, None, https://www.prestamax.asia.com, moldydoraemon@gmail.com,

发布日期: None **隐私政策:** Privacy link

关于此应用:

PrestaMax 的优点 1、快速解决：个人消费贷款、续贷、旅游贷款等。 2、贷款快捷：贷款流程简单，网上征信全自动，5分钟到账。 3.金额灵活：小额轻松贷款，大额最高可达20,000比索（需审批）！ 4.超低门槛：在线完成申请，无需房贷。 5. PrestaMax：每日最高信用利率不超过0.04%。 6、信息保密：用户信息严格保密、可靠。 7、操作便捷：贷款进度实时查询，到期提醒，借贷还款便捷。 8、找小额贷款快速贷款（钱、手机贷）。 **使用 PrestaMax 必须满足以下要求** 1.良好的信用记录：PrestaMax会检查您的信用记录，以评估用户的支付能力和信用风险。拥有良好的信用记录，如按时还款、无拖欠记录等，可以增加用户申请贷款的机会。 2、稳定的收入来源：需要能够证明用户有稳定的收入来源，有按时偿还贷款的能力。 3、还款能力：PrestaMax会评估用户的债务承受能力，确保用户有足够的收入按时偿还贷款。 4.年满18岁：必须是年满18岁的墨西哥公民。 **PrestaMax 产品简介** 1. 高额贷款：最高可达 20,000 美元（须经批准）。 2. 快速贷款审批——提供安全、可靠、便捷的贷款服务。 3.长期贷款：最短91天，最长365天 4、利率透明，还款灵活：贷款最高年利率15%，贷款日利率不超过0.04%。支持多种支付方式。 5.数据安全：个人信息时刻加密，为您提供全面保护。 6.周期范围：最低贷款$500~最高$20,000 - 如果您在PrestaMax借出10,000美元，期限为120天（4个月），利息为每日0.04%（最高年利率为15%），除利息外不收取任何佣金，将支付以下佣金：- 每日利息 = $10,000 x 0.04% = $4 - 每月利息 = $4x30 = $120 - 每月付款 = $10,000 / 4 + $120 = $2,620 - 120天内到期的贷款：您的总利息 = 4 美元 x 120 天 = 480 美元 - 您的退款总额 = $10,000 + $480 = $10,480 *这些数字仅供参考，最终利率可能会根据借款人的信用评估而有所不同。（如果您想借更多的钱，可以通过以上方法快速计算出合适的贷款利率，且所有贷款产品均不收取额外费用） 关于用户信息安全 PrestaMax 保护所有用户的信息。未经用户许可，我们承诺不会向任何人透露您的信息。 联系我们 -电子邮件：moldydoraemon@gmail.com 我们的办公时间为周一至周五上午 9:00 至下午 6:00。 - 办公地址：C JUAN ESCUTIA 513 COL BENITO JUAREZ 82180 MAZATLAN, SIN。

本报告由南明离火移动安全分析平台生成

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。

© 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