南明离火
移动应用检测平台

ANDROID 静态分析报告

NeroCredit - v1.9.0

分析日期: 2025-08-27 16:46:12

应用概览

文件名称:	com.credit.prestamos.rapido.cash.efectivo.nero.apk
文件大小:	14.41MB
应用名称:	NeroCredit
软件包名:	com.credit.prestamos.rapido.cash.efectivo.nero
主活动:	com.nc.NcMainActivity
版本号:	1.9.0
最小SDK:	23
目标SDK:	34
加固信息:	网易易盾
开发框架:	React Native
应用程序安全分数:	61/100 (低风险)
杀软检测:	1 个杀毒软件报毒
MD5:	df9edbe752d3e6a21bad28ceba5abea7
SHA1:	94afcea003e1537e2bd67a0cc5156c8e658a534d1
SHA256:	624a736385643f2dcb4ac596e18880002a8b2471aa60a6372d2cf1baf9e84f8c

分析结果严重性分布

高危	中危	信息	安全	关注
0	10	0	2	0

四大组件导出状态统计

Activity组件：8个，其中export的有： 1个
Service组件：12个，其中export的有： 2个
Receiver组件：13个，其中export的有： 4个
Provider组件：7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: 2023-11-24 08:34:01+00:00
有效期至: 2053-11-24 08:34:01+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xb5ba348427e4f06d5d6045bdb72e303bb66a626c
哈希算法: sha256
证书MD5: 805fda2c382dfbc316ce05fec711c612
证书SHA1: de72d02827afe9a23fc61b96f3bce0c20442d522
证书SHA256: b63cb7c18f0b57b70ed84589d48d7dc0d6c43f821f2d5106129019ea767c797b
证书SHA512:
7e0d0fb42781417ae5802cb91edfb851641b073fb8dbbde46f7c4d4fcf017ac475a7868d3837bd984a92d4c3bbf0709146c72ef06a10c4cf86d515b0dc2559bb

公钥算法: rsa
密钥长度: 4096
指纹: 94cb3fa78bce28c7c3f2df7bef7eb5158ca7665d51ffc1b7a90d63a81b68b477
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.ACCESS_MEMORY_USAGE_STATS	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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.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.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.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.GET_META_DATA	未知	未知权限	来自 android 引用的未知权限。
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.ACCESS_NOTIFICATION_POLICY	普通	标记访问通知策略的权限	对希望访问通知政策的应用程序的标记许可。
android.permission.READ_CALENDAR	危险	读取日历活动	允许应用程序读取您手机上存储的所有日历活动。恶意应用程序可借此将您的日历活动发送给其他人。
android.permission.WRITE_CALENDAR	危险	添加或修改日历活动以及向邀请对象发送电子邮件	允许应用程序添加或更改日历中的活动，这可能会向邀请对象发送电子邮件。恶意应用程序可能会借此清除或修改您的日历活动，或者向邀请对象发送电子邮件。
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.READ_PRIVILEGED_PHONE_STATE	签名(系统)	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。
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。
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.credit.prestamos.rapido.cash.efectivo.nero.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.nc.launchActivity	Schemes: http://, https://, nativa://, nero://, Hosts: nativatech.mx, nativatech, www.nativatech.mx,

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: **9** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已配置网络安全策略 [android:networkSecurityConfig=@7F120005]	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	应用数据存在泄露风险 未设置[android:allowBackup]标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。
3	Activity-Alias (com.nc.launchActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。
4	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 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	Broadcast Receiver (com.adjust.sdk.AdjustReferrerReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.INSTALL_PACKAGES [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	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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。

本报告由南明离火移动安全分析平台生成

7	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。
8	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。
9	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。
10	高优先级 Intent（1000） -{1} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

序号	问题	等级	参考标准	文件位置

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	9/30	android.permission.CAMERA android.permission.ACCESS_COARSE_LOCATION android.permission.READ_SMS android.permission.READ_PHONE_STATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.READ_CALENDAR android.permission.WRITE_CALENDAR

其它常用权限	10/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.gms.permission.AD_ID android.permission.ACCESS_NOTIFICATION_POLICY android.permission.CHANGE_WIFI_STATE com.google.android.c2dm.permission.RECEIVE 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。

URL 链接安全分析

URL信息	源码文件
• https://docs.swmansion.com/react-native-reanimated/docs/guides/troubleshooting • http://fb.me/use-check-prop-typescriptURLongNonPercentSizeCSSPropertyValidatorequestSentbaseUrlawngreenqueueNativeCalling • https://docs.swmansion.com/react-native-reanimated/docs/fundamentals/glossary • https://github.com/microsoft/appcenter-sdk-react-native.gitoLoanContractPagetIteratorFnc-face-cancelBtnCallbackTakePhotoResultPaget • https://dev.to/li/how-to-requestpermission-for-devicemotion-and-devicеorientation-events-inios-13-46g2.33emitEventbtnString.logoutAppCenter.jsxscrollViewOffsetAdImpressionsCountZoomOutUpackage_sizeLargetInverseObjustifyContent • http://momentjs.com/guides	自研引擎-A

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/660041194602/namespaces/firebase:fetch?key=AIzaSyCYvQR3_zcymIx3Pdx5YBVpDCdQJE_CZs0 ）已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

敏感凭证泄露检测

可能的密钥
"CodePushDeploymentKey" : "aFRPmBG0ScGfTayxseMdl58VFBT4JXUPYx-CW"
"google_api_key" : "AIzaSyCYvQR3_zcymIx3Pdx5YBVpDCdQJE_CZs0"
"google_app_id" : "1:660041194602:android:cca9454966f557c4953e13"

"google_crash_reporting_api_key" : "AIzaSyCYvQR3_zcymIx3Pdx5YBVpDCdQJE_CZs0"
"key_agreement_image_center" : "liveness_image_center"
"key_eye_close" : "liveness_blink_eye_close"
"key_eye_open" : "liveness_blink_eye_open"
"key_livenessGuideImageSize" : "livenessGuideImageSize"
"key_liveness_exit_icon" : "liveness_exit2_icon"
"key_liveness_guide_read_color" : "livenessGuideReadColor"
"key_liveness_home_background_color" : "livenessHomeBackgroundColor"
"key_liveness_home_brand_material" : "liveness_home_brand"
"key_liveness_home_closeIcon_material" : "liveness_home_closeicon"
"key_liveness_home_loadingIcon_material" : "liveness_home_loadingicon"
"key_liveness_home_processBar_color" : "livenessHomeProcessBarColor"
"key_liveness_home_ring_color" : "livenessHomeRingColor"
"key_liveness_home_validationFailProcessBar_color" : "livenessHomeValidationFailProcessBarColor"
"key_liveness_look_mirror" : "liveness_look_mirror"
"key_meglive_eye_blink_m4a" : "liveness_blink"
"key_meglive_mouth_open_m4a" : "liveness_mouth_open"
"key_meglive_pitch_down_m4a" : "liveness_nod"
"key_meglive_well_done_m4a" : "liveness_well_done"
"key_meglive_yaw_m4a" : "liveness_shakehead"
"key_mouth_close" : "liveness_mouth_close"
"key_mouth_open" : "liveness_mouth_open"
"key_nod_down" : "liveness_nod_down"
"key_nod_up" : "liveness_nod_up"
"key_shakehead_left" : "liveness_shakehead_left"
"key_shakehead_right" : "liveness_shakehead_right"

Google Play 应用市场信息

标题: NeroCredit: Prestamos Rapidos

评分: 4.8172994 安装: 1,000,000+ 价格: 0 **Android**版本支持: 分类: 财务 **Play Store URL:** com.credit.prestamos.rapido.cash.efectivo.nero

开发者信息: nerocredit_dev, 6935987043567998874, None, https://www.nativatech.mx, ayuda@nativatech.mx,

发布日期: None 隐私政策: Privacy link

关于此应用:

只需几分钟，我们的贷款即可为您带来所需的财务自由！无论您是想度假、聚会还是购物，我们都会随时为您提供支持。 关于 NeroCredit 贷款 – 金额：最高 25,000 美元 – 最短还款期限：91 天 – 最长还款期限：365 天 – 最高年利率 (APR)：36%（每日 0.1%） – 服务费：0% - 10% – 增值税：16% 示例：如果您申请贷款 2,000 比索，期限为 180 天，日利率为 0.05%，服务费为 5%，则总成本计算如下： – 利息：2,000 × 0.05% × 180 = 180 – 服务费：2,000 × 5% = 100 – 增值税：(180 + 100) × 16% = 44.80 – 总还款额：2,000 + 180 + 100 + 44.80 = 2,324.80 为什么选择 NeroCredit？ – 快速高效的流程：几分钟内即可正确填写您的信息，款项将直接转入您的银行账户。 – 安全保障：为了让您安心无虞，我们绝不会与第三方共享您的信息，尤其是在未经您许可的情况下。保护您的隐私是我们的首要任务。 – 卓越服务：我们全天候提供优质服务。 – 贷款额度更高：如果您在我们的应用程序上拥有良好的信用记录，您将有机会获得更高额度的贷款。 – 灵活的付款方式：我们接受在线或现金支付。 – 费用透明：无隐藏费用。 如何获得贷款？ – 在 Google Play 下载我们的应用程序 – 使用您的手机号码注册 – 填写您的信息 – 提交您的申请 – 贷款将直接存入您的银行账户 谁可以申请贷款？ – 年满 18 周岁 – 拥有手机号码 – 是墨西哥公民并拥有国家统计局 (INE) – 持有您选择的银行的跨行 CLABE（国家信用卡） 如何获得贷款？ 款项将直接转入您提供的银行账户。隐私 – 我们收到的信息将用于验证您的身份并创建您的信用档案。我们绝不会分享您的信息：https://www.nativatech.mx/privacy/ 如果您有其他问题，请联系我们： – 邮箱：ayuda@nativatech.mx – 网址：https://www.nativatech.mx/ – 地址：AVENIDA PASEO DE LA REFORMA, 222 TOWER 3, CUAUHTEMOC, C.P. 06500

免责声明及风险提示:

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患。