南明离火
移动应用检测平台

ANDROID 静态分析报告

CreditoYa - v2.1.0

分析日期: 2025-08-26 11:20:21

应用概览

文件名称:	CreditoYa Dinero Fácil Rápido_2.1.0.apk
文件大小:	21.94MB
应用名称:	CreditoYa
软件包名:	prestamos.creditoya.urgente.dinero.peso.cash.credito.rapido
主活动:	mx.apoyo.cash.MainActivity
版本号:	2.1.0
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	62/100 (低风险)
跟踪器检测:	3/432
杀软检测:	5 个杀毒软件报毒
MD5:	d720545daaee8fffe83af2e3c29aa7c5
SHA1:	abf95c86eee5d8[illegible]5d7ab3d6d3e08557[illegible]44854
SHA256:	fabdd734f4[illegible]7b[illegible]62bfddba54df355190[illegible]64a1[illegible]85ba29f597cb3b1190d621cb3

分析结果严重性分布

高危	中危	信息	安全	关注
0	9	2	2	0

四大组件导出状态统计

Activity组件：51个，其中export的有： 0个
Service组件：6个，其中export的有： 0个
Receiver组件：3个，其中export的有： 1个
Provider组件：4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: 2021-11-18 06:53:31+00:00
有效期至: 2051-11-18 06:53:31+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xfe391bef1b151a5f57b83b13229db02999fdfe96
哈希算法: sha256
证书MD5: 512d8d9c76243c6f70c056ea49122104
证书SHA1: b67c6fac4e2f73c7952681dfc6587e0b9262c93a
证书SHA256: 2e224a7091883b24a6ee15ea08bc6c36348bbd99a56efdb77fe597e0d63f1109
证书SHA512:
222e7c97ed1ccdd6159912877a2c2f421ac584ccd5aed8174b6328dad499743e565b042bc22aeb9c33807c95381821b5339080153bfe0[illegible]13f4bbf346cd0fe

公钥算法: rsa
密钥长度: 4096
指纹: 91d42622279e82d013a4431eb424697641a5e2c9c9fcb03e2a9eb32c36155808
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.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.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.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。
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。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
mx.apoyo.cash.MainActivity	Schemes: @7F0F0003://,

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: **2** | 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=@7F120002]	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	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。

代码安全漏洞检测

高危: **0** | 警告: **5** | 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	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
3	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
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	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
6	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
7	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
8	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

Native 库安全加固检测

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/libapp.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。	动态共享对象(DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	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	Not Applicable info RELRO 检查不适用于 Flutter/Dart 二进制文件	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 info 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	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
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

本报告由南明离火移动安全分析平台生成

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
00191	获取短信收件箱中的消息	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
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
00046	方法反射	反射	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
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
00026	方法反射	反射	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
00013	读取文件并将其放入流中	文件	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
00067	查询IMSI号码	信息收集	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

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.READ_CALENDAR android.permission.WRITE_CALENDAR android.permission.READ_SMS
其它常用权限	4/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE com.google.android.gms.permission.AD_ID 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
api.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:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
greenrobot.org	安全	否	**IP地址:** 85.13.163.69 **国家:** 德国 **地区:** 图林根 **城市:** 弗里德斯多夫 **纬度:** 50.604919 **经度:** 11.035770 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/database/b.java
• https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so

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/1080940344665/namespaces/firebase:fetch?key=AIzaSyCpl7IIbEkmJWQ4HcBnQzE01XyA5v-RcAY ） 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
Flutter	Google	Flutter 是谷歌的移动 UI 框架，可以快速在 iOS 和 Android 上构建高质量的原生用户界面。
Jetpack Camera	Google	CameraX 是 Jetpack 的新增库。利用该库，可以更轻松地向应用添加相机功能。该库提供了很多兼容性修复程序和解决方法，有助于在众多设备上打造一致的开发者体验。
Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
this@abstracttypeconstructor.builtins this@abstracttypeconstructor.parameter	h4/g.java
boohee@boohee.com	n5/c.java
this@createcapturedifneeded.type	i3/d.java

第三方追踪器检测

名称	类别	网址
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
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
"google_app_id" : "1:1080940344665:android:0ea07a832717ef0baf8848"
"google_api_key" : "AIzaSyCpl7IIbEkmJWQ4HcBnQzE01XyA5v-RcAY"
"google_crash_reporting_api_key" : "AIzaSyCpl7IIbEkmJWQ4HcBnQzE01XyA5v-RcAY"
"ADJUST_KEY" : "vxm9cfp4baww"

Google Play 应用市场信息

标题: CreditoYa: Dinero Fácil Rápido

评分: 4.856272 **安装:** 1,000,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** prestamos.creditoya.urgente.dinero.peso.cash.credito.rapido

开发者信息: Ronald Thompson, Ronald+Thompson, None, https://creditoya.cc/home, call@creditoya.cc,

发布日期: None **隐私政策:** Privacy link

关于此应用:

不到 10 分钟即可获得贷款。过程快速简单！没有认可或保证。授权金额100%的存款。 信用额度：$800 ~ $20,000 比索 - 贷款期限：91天~180天； - 利息：每天0.01% - 0.1%（年利率3.6% - 36%）； - 增值税：佣金和利息的 16% - 佣金：金额的 5% - 20% - 猫：270% - 540% 举例如： 如果用户请求贷款金额为 2,000 比索的个人贷款，则贷款详细信息为： - 金额：2,000 比索美元 - 持续时间：91天 - 利息：182 比索 - 佣金和增值税：$365比索（（2000*14.5%=290）佣金和75比索（（佣金145+利息91）*16%=75）增值税 上述贷款总额为 2,548 比索。对应CAT值：343% 要求： - 年满 18 岁 - 拥有自己的银行账户 - IFE/INE 电流 如何申请贷款？ - 在 Google Play 上下载 CreditoYa 应用程序。 -三步，不超过5分钟完成您的贷款申请信息 - 不到 3 分钟即可将钱从您的卡转入您的帐户。 看看这个！ CreditoYa 奖励您的准时付款！如果您按时付款，则限额 贷款增加，您的付款日期会更长。 安全 所有交易均受 256 位 SSL 加密保护。所有数据都通过安全连接传输。未经您的许可，我们不会与任何人分享。我们建议您通过以下链接查看我们的隐私声明：https://m.creditoya.cc/creditoya/privacyagreement。如果您对我们的隐私声明有任何疑问，请随时通过电子邮件联系我们的客户服务团队。 联系我们获取更多信息： 电子邮件：call@creditoya.cc 网站：https://creditoya.cc/home 服务时间：周一至周六上午9:30至下午6:30 公司地址：Calle Lázaro Cárdenas 196 B302 Guerrero 06300 Cuauhtémoc, Mexico City

---

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。