南明离火

移动应用检测平台

ANDROID 静态分析报告

TRU CRED

TruCred : v1.1.3

本报告由南明离火移动安全分析平台生成

分析日期: 2025-08-27 16:34:35

应用概览

文件名称:	com.conveniente.trucred.apk
文件大小:	25.51MB
应用名称:	TruCred
软件包名:	com.conveniente.trucred
主活动:	com.veloz.app.ui.SplashActivity
版本号:	1.1.3
最小SDK:	26
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:	55/100 (中风险)
跟踪器检测:	2/432
杀软检测:	AI评估：安全
MD5:	94467e324f9e674406bcbf0206e58920
SHA1:	6e20e8638b00c0[illegible]16157dff11ae8c76a[illegible]dd78
SHA256:	802046d3d9[illegible]4722d0223daeff413c[illegible]4789dd2278d441753156be448658f

分析结果严重性分布

高危	中危	信息	安全	关注
2	17	1	3	0

四大组件导出状态统计

Activity组件：11个，其中export的有： 2个
Service组件：12个，其中export的有： 1个
Receiver组件：4个，其中export的有： 2个
Provider组件：6个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: False
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: 2025-07-01 06:10:43+00:00
有效期至: 2055-07-01 06:10:43+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x3db977e9718d2a781f1e1730d93cb1dbe7133cd
哈希算法: sha256
证书MD5: 09194aac0a4e9ef854071decda36f651
证书SHA1: 153658f241faa4e15ce8de32525b379898455c0e
证书SHA256: 2a63c2797a34325a4d361a17003e15024af6eca3db9a6212fa3580ded40d5143
证书SHA512:
3449a4a0af726a8e1ac26d87030bf2e72a5f2f62156e53f24f36a3751caa755072bed24853e178adb660140dd242a12eccda1db2200c80[illegible]4fa76e8f1912ebd

公钥算法: rsa
密钥长度: 4096
指纹: 3f87334ef1e405681a73ac90a9dd73e39df5750996c8cc5a37cc398726c72101
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.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.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.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.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.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
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。
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.conveniente.trucred.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.android.vending.CHECK_LICENSE	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.veloz.app.ui.SplashActivity	Schemes: trucred://,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

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: **0** | 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: **1** | 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=@7F140003]	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	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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。
3	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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	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。
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: **2** | 警告: **10** | 信息: **1** | 安全: **2** | 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，不应记录敏感信息	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
3	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

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	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	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
7	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
8	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
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	该文件是World Readable。任何应用程序都可以读取文件	高危	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	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

12	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
13	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
14	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
15	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

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	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
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
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
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
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
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
00030	通过给定的 URL 连接到远程服务器	网络	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
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
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限

00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限
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
00146	获取网络运营商名称和 IMSI	电话服务 信息收集	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
00171	将网络运算符与字符串进行比较	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
00117	获取 IMSI 和网络运营商名称	电话服务 信息收集	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	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
00066	查询ICCID号码	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
00076	获取当前WiFi信息并放入JSON中	信息收集 WiFi	升级会员：解锁高级权限
00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限
00113	获取位置并将其放入 JSON	信息收集 位置	升级会员：解锁高级权限
00035	查询已安装的包列表	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
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
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	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
00062	查询WiFi信息和WiFi Mac地址	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
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限

00108	从给定的 URL 读取输入流	网络 命令	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	3/30	android.permission.READ_SMS android.permission.CAMERA android.permission.WAKE_LOCK
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE 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
collect.creditumex.com	安全	否	**IP**地址: 199.91.74.184 **国家**: 墨西哥 **地区**: 墨西哥城 **城市**: 墨西哥城 **纬度**: 19.428471 **经度**: -99.127609 **查看**: Google 地图
cum.creditumex.com	安全	否	**IP**地址: 98.98.253.32 **国家**: 墨西哥 **地区**: 墨西哥城 **城市**: 墨西哥城 **纬度**: 19.428471 **经度**: -99.127609 **查看**: Google 地图
api.whatsapp.com	安全	否	**IP**地址: 31.13.70.49 **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
acs.amazonaws.com	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://play.google.com/store/apps/details?id=com.example.app • javascript:location.reload	com/veloz/app/ui/web/CommonWebViewActivity.java
• https://api.whatsapp.com/send?phone=	com/veloz/app/utils/LoginUtils.java
• https://api.whatsapp.com/send?phone=	com/veloz/app/ui/home/fragment/MineFragment.java
• javascript:location.reload • https://play.google.com/store/apps/details?id=	com/veloz/app/ui/home/fragment/MemberFragment.java
• javascript:findwebrtcinfo	com/datavisorobfus/h.java
• http://acs.amazonaws.com/groups/global/authenticatedusers • http://acs.amazonaws.com/groups/global/allusers • http://acs.amazonaws.com/groups/s3/logdelivery	com/amazonaws/services/s3/model/GroupGrantee.java
• https://play.google.com/store/apps/details?id=com.example.app • javascript:location.reload	com/veloz/app/ui/home/fragment/FacturaFragment.java
• https://play.google.com/store/apps/details?id=	com/veloz/app/ui/home/HomeActivity.java
• https://cum.creditumex.com/appweb/customer.html • https://cum.creditumex.com/appweb/#/	com/veloz/app/utils/Constants.java
• https://play.google.com/store/apps/details?id=com.example.app • https://cum.creditumex.com/	com/veloz/app/ui/SplashActivity.java
• https://collect.creditumex.com/sensorsdata/api/common/log.json	自研引擎-S

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/41243651840/namespaces/firebase:fetch?key=AIzaSyDujHfunlv922nAS8C7CEERtu4GvkxYqwQ ）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

本报告由南明离火移动安全分析平台生成

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。
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。
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).

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 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" : "AIzaSyDujHfunlv922nAS8C7CEERtu4GvkxYqwQ"
"google_app_id" : "1:412436518410:android:d9819b8c0cc439cdc14de5"
"google_crash_reporting_api_key" : "AIzaSyDujHfunlv922nAS8C7CEERtu4GvkxYqwQ"
MJCR3nbjtc8ARKt/AP82SzhTxLPuFzw=
MJCR3nbjtc8ARKt9HOAI/AZAzrHiEyhubQ==
KZGR3Uffn88OW6tuEewC9j5V3A==
dI2H2mzZqo8OQIQxI/oZ8itF3Lf7XC57dQ==

H6ik7UfoqtAwYIZxE9A68jVW8J/oAjw=

Google Play 应用市场信息

标题: TruCred-Préstamo Expreso Móvil

评分: 4.66 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** com.conveniente.trucred

开发者信息: CADENA DE EXTENSION SA DE CV, CADENA+DE+EXTENSION+SA+DE+CV, None, https://www.creditumex.com, service@creditumex.com,

发布日期: None **隐私政策:** Privacy link

关于此应用:

TruCred：快速可靠的金融解决方案 TruCred 是一个数字平台，提供快速、安全且价格合理的在线贷款。TruCred 旨在满足您即时的财务需求，简化流程，让您足不出户即可在几分钟内获得资金，无需繁琐的文书工作。 为什么选择 TruCred？ 1. 快速便捷的贷款：贷款批准后几分钟内即可收到款项。 2. 100% 在线：整个流程只需通过手机即可完成，无需前往实体分行。 3. 灵活便捷：贷款旨在应对紧急情况或重要项目。 4. 安全保障：您的个人数据受到严格的隐私政策保护。 5. 高效支持：周到的客户服务随时为您解答疑问。 贷款特点： ● 金额：500 至 50,000 比索。 ● 期限：91 至 210 天。 ● 利率：每日 0.01% 至 0.1%（最高年利率 36%）。 ● 增值税：费用和利息加收 16%。 ● 示例：贷款 2,000 美元，期限 91 天：利息：182 美元（每日 0.1%）。 ○ 增值税：61.12 美元。 ○ 应付总额：2,243.12 美元。 如何申请贷款？ 1. 使用您的个人信息注册。 2. 申请所需金额。 3. 等待几分钟内获得批准。 4. 资金直接存入您的账户。 贷款申请要求： ● 必须是 18 岁以上的墨西哥公民。 ● 拥有官方身份证件 (INE) 和您名下的银行账户。 ● 可验证的稳定收入。 联系方式 ● 电话：5516961526 邮箱：service@creditumex.com ● 营业时间：周一至周五，上午 9:00 至下午 6:30 TruCred 致力于您的财务健康。下载我们的应用程序，快速、安全、高效地解决您的财务需求。

免责声明及风险提示: