南明离火
移动应用检测平台

ANDROID 静态分析报告

Credito365 • v1.2.0

分析日期: 2025-08-27 14:40:10

应用概览

文件名称:	mx.credito365.mobile.apk
文件大小:	4.37MB
应用名称:	Credito365
软件包名:	mx.credito365.mobile
主活动:	com.example.mexico.MainActivity
版本号:	1.2.0
最小SDK:	23
目标SDK:	34
加固信息:	未加壳
开发框架:	Flutter
应用程序安全分数:	51/100 (中风险)
跟踪器检测:	6/432
杀软检测:	9 个杀毒软件报毒
MD5:	f2248653b314908de5dda8e569c3800d
SHA1:	c403641ac31c67[illegible]ee0f8c54e57a7ab7ea142
SHA256:	ae3301ea16310cc1abdf00b23e552f0e56ad65950783f860fde02f1569071363

分析结果严重性分布

高危	中危	信息	安全	关注
1	11	1	1	0

四大组件导出状态统计

Activity组件：9个，其中export的有： 1个
Service组件：15个，其中export的有： 2个
Receiver组件：10个，其中export的有： 3个

Provider组件：9个，其中export的有： 1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: 2023-12-21 15:29:26+00:00
有效期至: 2053-12-21 15:29:26+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xcdd950510fda68a734903b275c595b610b20e957
哈希算法: sha256
证书MD5: 25e34f02c40db5d352696f7eed66a970
证书SHA1: 172bb98211ed15b6449b2b0aed7aef96de05f1f0
证书SHA256: bd6cf3f3c2fba9c955df15afe37874959c6c5790c1d8ca41e635564d4248a1d0
证书SHA512:
0feb44f426f420f697aecdeb16047e565b5d88fc583a61029cd95fad19c55e82afcd1d26dd41fc29[illegible]8f88421f60800ed81[illegible]eb592d41c560699d81

公钥算法: rsa
密钥长度: 4096
指纹: 782729abb9cf52e9bc5c90836f34ab4a8f56c56aee8fd2d2da626d9208efa[illegible]
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_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。
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.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.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.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_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。
com.samsung.android.mapsagent.permission.READ_APP_INFO	未知	未知权限	来自 android 引用的未知权限。
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	未知权限	来自 android 引用的未知权限。
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。
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。
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。
mx.credito365.mobile.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
mx.credito365.mobile.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
mx.credito365.mobile.permission.PUSH_PROVIDER	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.example.mexico.MainActivity	Schemes: https://, Hosts: credito-365.mx, Paths: /,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.mx.credito365.mobile,

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: **8** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	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。
2	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) 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。
3	Service (com.huawei.hms.flutter.push.backgroundmessaging.BackgroundMessagingService) 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。
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。

7	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护。 Permission: mx.credito365.mobile.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	检测到 Broadcast Receiver 已导出，但受权限保护。
8	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护。 Permission: mx.credito365.mobile.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	检测到 Broadcast Receiver 已导出，但受权限保护。
9	Service (com.huawei.hms.support.api.push.service.HmsMsgService) 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。
10	Content Provider (com.huawei.hms.support.api.push.PushProvider) 未受保护。 [android:exported=true]	警告	检测到 Content Provider 已导出，未受任何权限保护，任意应用均可访问。

代码安全漏洞检测

高危: **0** | 警告: **2** | 信息: **1** | 安全: **0** | 审计: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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

3	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

应用行为分析

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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	5/30	android.permission.CAMERA android.permission.ACCESS_COARSE_LOCATION android.permission.READ_SMS android.permission.WAKE_LOCK android.permission.VIBRATE

其它常用权限	5/46	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 com.google.android.c2dm.permission.RECEIVE

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.
privacy-sandbox.appsflyersdk.com	安全	否	**IP地址:** 1[illegible].155.202.48 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
sadrevenue.s	安全	否	No Geolocation information available.
sgcdsdk.s	安全	否	No Geolocation information available.
scdn-ssettings.s	安全	否	No Geolocation information available.
spia.s	安全	否	No Geolocation information available.
sattr.s	安全	否	No Geolocation information available.
sdlsdk.s	安全	否	No Geolocation information available.
svalidate-and-log.s	安全	否	No Geolocation information available.
ssdk-services.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.
smonitorsdk.s	安全	否	No Geolocation information available.
slaunches.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

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://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
• https://%smonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFd1aSDK.java
• https://%sregister.%s/api/v	com/appsflyer/internal/AFg1jSDK.java
• https://%sapp.%s	com/appsflyer/internal/AFj1fSDK.java
• https://%sattr.%s/api/v • https://%ssdk-services.%s/validate-android-signature • https://%sdlsdk.%s/v1.0/android/ • https://%sinapps.%s/api/v • https://%sconversions.%s/api/v • https://%sadrevenue.%s/api/v2/generic/v6.15.2/android?app_id= • https://%smonitorsdk.%s/api/remote-debug/v2.0?app_id= • https://privacy-sandbox.appsflyersdk.com/api/trigger • https://%slaunches.%s/api/v • https://%svalidate.%s/api/v	com/appsflyer/internal/AFj1jSDK.java
• https://%svalidate-and-log.%s/api/v1.0/android/validateandlog?app_id= • https://%sonelink.%s/shortlink-sdk/v2 • https://%sgcdsdk.%s/install_data/v5.0/	com/appsflyer/internal/AFe1qSDK.java
• https://%spia.%s/api/v1.0/pia-android-event?app_id=	com/appsflyer/internal/AFf1jSDK.java
• https://%scdn-%ssettings.%s/android/v1/%s/settings • https://%scdn-%stestsettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFe1iSDK.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/918304421002/namespaces/firebase:fetch?key=AIzaSyCOrLP1WJqoKft6hg0LgxZN-Z43N1iwWG4 ） 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。
HMS Core	Huawei	HMS Core 是华为终端云服务提供的端、云开放能力的合集，助您高效构建精品应用。
Huawei Push	Huawei	华为推送服务（HUAWEI Push Kit）是华为为开发者提供的消息推送平台，建立了从云端到终端的消息推送通道。开发者通过集成 HUAWEI Push Kit 可以实时推送消息到用户终端应用，构筑良好的用户关系，提升用户的感知度和活跃度。
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。
AppGallery Connect	Huawei	为开发者提供移动应用全生命周期服务，覆盖全终端全场景，降低开发成本，提升运营效率，助力商业成功。
HMS Core AAID	Huawei	华为推送服务开放能力合集提供的匿名设备标识(AAID) 实体类与令牌实体类包。异步方式获取的 AAID 与令牌通过此包中对应的类承载返回。
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。

第三方追踪器检测

名称	类别	网址
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
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
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333

敏感凭证泄露检测

可能的密钥
华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "appid=111815175"

"facebook_app_id" : "207232322430799"
"facebook_client_token" : "4fb764d979a07409ac23396825fb8ed1"
"google_api_key" : "AIzaSyCOrLP1WJqoKft6hg0LgxZN-Z43N1iwWG4"
"google_app_id" : "1:918304421002:android:c3d4112f506e2497e4a973"
"google_crash_reporting_api_key" : "AIzaSyCOrLP1WJqoKft6hg0LgxZN-Z43N1iwWG4"
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1

Google Play 应用市场信息

标题: Credito365: préstamos rápidos

评分: 3.5344827 **安装:** 500,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** mx.credito365.mobile

开发者信息: Crédito365, S.A.P.I. de C.V., Cr%C3%A9dito365,+S.A.P.I.+de+C.V., None, https://credito-365.mx/, soporte@credito-365.mx,

发布日期: None **隐私政策:** Privacy link

关于此应用:

使用 Credito365 移动应用程序，您足不出户只需 3 分钟即可轻松快速地获得高达 20,000 MXN 的贷款。 如何使用 Credito365 应用程序获得个人贷款？： 在您的手机上安装该应用程序。 使用贷款计算器选择贷款金额和期限，然后单击“获取资金”按钮。 注册您的详细信息并完成一份简短的申请，然后输入您的银行帐户，以便我们可以将钱存入您的账户。 等待验证，如果您的请求获得批准，请对您的合同进行数字签名，我们将立即将资金存入您的帐户。 谁可以在 Credito365 获得快速贷款？ 所有 18 岁至 65 岁之间的成年公民都可以在墨西哥获得贷款。我们为所有人提供现金贷款，包括学生、雇员和失业者。 要在线获得贷款，您只需： 墨西哥国籍； 注册时年龄在18岁至65岁之间； 有效的官方身份证明（INE 或护照）。 有效的电话号码。 墨西哥任何机构开立的银行账户。 要收到这笔钱，您不需要证书、背书或担保。 注册期间，您将完成验证过程。 如何网上支付贷款？ Credito365 有多种支付贷款的方式 （同样适用于应计利息的支付）。通过我们的移动应用程序或网站访问您的帐户， 输入“付款”选项： 将出现 3 个付款选项； 借记卡或信用卡 它会要求您提供持卡人信息、号码和有效期； 您将被重定向以接收付款确认信息。 转学（SPEI） 输入您的银行帐户，然后输入门户上显示的信息以进行付款。 现金支付（便利店） 下载您的优惠券并在允许的商店付款。 状况： -最短贷款期限：61天。 -最长贷款期限：90天。 -贷款最低年龄：18岁。 -最低年利率为728%。 - 最高年利率（不包括促销）为728%。 以最低利率计算贷款的示例： 您以 % 的利率（年利率 447.63%）申请了一笔 10,000.00 比索的贷款，为期 61 天。 计算：10,000 * 61 * 2% = 22,400 MXN *。 以最高利率计算贷款的示例： 您将收到 90 天的 10,000.00 比索，利率为 2%（年利率 2333.95%），外加第一笔贷款的佣金 - 200 MXN。 计算：10,000 * 90 * 2% + 200 = 28,200。 *考虑到当前的折扣和促销活动，收到的金额可能会减少。 联邦预防和识别非法来源资源经营法： 《联邦防止和识别非法来源资源经营法》第 17 条第二节第四节。 Crédito365、S.A.P.I.简历Rousseau No. 14, Floor 1 Anzures, Miguel Hidalgo 墨西哥 Miguel Hidalgo - 11560 墨西哥 (MX)

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隐患。