南明离火
移动应用检测平台

ANDROID 静态分析报告

EfectivoYa • v2.3

分析日期: 2025-08-27 15:59:27

应用概览

文件名称:	mx.efectivoya.loan.apk
文件大小:	14.89MB
应用名称:	EfectivoYa
软件包名:	mx.efectivoya.loan
主活动:	com.mxff.ffxxmm.activity.FFSplashActivity
版本号:	2.3
最小SDK:	23
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:	1/432
杀软检测:	2 个杀毒软件报毒
MD5:	a75188ab7910a50b30fe4059cc7cdffc
SHA1:	e2b95b40e8fc3a[illegible]1b94e07b41bcf2e0721fc
SHA256:	cd54807b86787[illegible]ab3a6733ac417b2b142d9c5dae1689d7811ac2939ef805d0d

本报告由南明离火移动安全分析平台生成

分析结果严重性分布

高危	中危	信息	安全	关注
2	10	2	2	0

四大组件导出状态统计

Activity组件：3个，其中export的有： 1个
Service组件：2个，其中export的有： 0个
Receiver组件：1个，其中export的有： 1个

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: 2024-01-23 10:40:21+00:00
有效期至: 2054-01-23 10:40:21+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xe9170eecffaf03bf8419746b7279f891e59cc4a5
哈希算法: sha256
证书MD5: cb609bd3afd5cf21ecc7650cab5919de
证书SHA1: 7aca364a035d2188e02392aa949df4ed55c9225d
证书SHA256: fdf5f3505e5075b26dd6f1b95e7862b7c31ffb44f6e6449bd83d828a458896e6
证书SHA512:
61dcc8644d292535cd6e68897c8d8065f5e9639ff7d794f3fe1a36b559d87e9a80fc632ba2c1761b[illegible]35cb79e6338e32223be[illegible]da273f4f2ed9bc3557

公钥算法: rsa
密钥长度: 4096
指纹: 9e8e3cf0b7efa9245d3f93d40309b6ec1cf1c235fb93abe44d95a638ede16f35
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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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_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_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.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.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_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.LOCAL_MAC_ADDRESS	未知	未知权限	来自 android 引用的未知权限。
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.QUERY_ALL_PACKAGE	未知	未知权限	来自 android 引用的未知权限。
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。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
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。
mx.efectivoya.loan.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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。

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: **3** | 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	Activity (com.cnhz.android.main.view.activity.ActivitySplash) 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	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: **5** | 信息: **2** | 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	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
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	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
6	已启用远程WebView调试	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

本报告由南明离火移动安全分析平台生成

7	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
8	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
9	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
10	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
11	该文件是World Writable。任何应用程序都可以写入文件	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

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
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
00130	获取当前WIFI信息	WiFi 信息收集	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
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

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
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
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 反射 通话记录 日历	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
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
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
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
00016	获取设备的位置信息并将其放入 JSON 对象	位置 信息收集	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	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
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
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

00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00139	获取当前WiFi id	信息收集 WiFi	升级会员：解锁高级权限
00135	获取当前WiFi id并放入JSON中	WiFi 信息收集	升级会员：解锁高级权限
00010	读取敏感数据（SMS、CALLLOG）并将其放入 JSON 对象中	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	6/30	android.permission.CALL_PHONE android.permission.CAMERA android.permission.ACCESS_COARSE_LOCATION android.permission.READ_CALENDAR android.permission.WRITE_CALENDAR android.permission.READ_SMS
其它常用权限	9/46	android.permission.INTERNET android.permission.FLASHLIGHT android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN 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
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.

prod-api.efectivoya.mx	安全	否	**IP地址:** 104.21.24.111 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
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.
sstats.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.
h5.efectivoya.mx	安全	否	**IP地址:** 104.21.24.111 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
sviap.s	安全	否	No Geolocation information available.
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
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://%ssdk-services.%s/validate-android-signature • https://%svalidate.%s/api/v	com/appsflyer/internal/AFa1kSDK.java

• https://%sars.%s/api/v2/android/validate_subscription?app_id= • https://%sviap.%s/api/v1/android/validate_purchase?app_id= • https://%sgcdsdk.%s/install_data/v5.0/ • https://%sonelink.%s/shortlink-sdk/v2 • https://%smonitorsdk.%s/remote-debug?app_id=	com/appsflyer/internal/AFc1qSDK.java
• https://%sapp.%s	com/appsflyer/internal/AFg1xSDK.java
• https://%sdlsdk.%s/v1.0/android/	com/appsflyer/internal/AFb1sSDK.java
• https://%sadrevenue.%s/api/v2/generic/v6.12.1/android?app_id= • https://%sattr.%s/api/v • https://%sinapps.%s/api/v • https://%sconversions.%s/api/v • https://%sadrevenue.%s/api/v2/log/adimpression/v6.12.1/android?app_id= • https://%slaunches.%s/api/v	com/appsflyer/internal/AFg1zSDK.java
• https://%smonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFc1rSDK.java
• https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
• https://h5.efectivoya.mx/privacy.html	com/mxff/ffxxmm/activity/FFPrimaryActivity.java
• https://h5.efectivoya.mx/permission.html	com/mxff/ffxxmm/activity/FFPermissionActivity.java
• https://%sviap.%s/api/v1/android/validate_purchase?app_id=	com/appsflyer/internal/AFd1kSDK.java
• https://%sregister.%s/api/v	com/appsflyer/internal/AFe1sSDK.java
• https://%scdn-%ssettings.%s/android/v1/%s/settings • https://%scdn-%stestsettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFc1cSDK.java
• https://h5.efectivoya.mx/privacy.html • https://h5.efectivoya.mx/ • https://h5.efectivoya.mx/delete.html • https://h5.efectivoya.mx/help.html	com/mxff/ffxxmm/utils/l.java
• http://play.google.com/store/apps/details?id=	com/cnhz/android/main/usercenter/view/FragmtAuthStep4.java
• http://play.google.com/store/apps/details?id=	com/cnhz/android/main/usercenter/view/FragmtMine.java
• https://api.whatsapp.com/send?phone=	com/cnhz/android/main/view/fragment/DialogFragment.java
• https://h5.efectivoya.mx/agreement.html?	com/mxff/ffxxmm/activity/FFLoanActivity.java
• http://play.google.com/store/apps/details?id=	com/cnhz/android/main/view/activity/ActivityMain.java
• https://%sstats.%s/stats	com/appsflyer/internal/AFa1dSDK.java
• https://prod-api.efectivoya.mx	s0/a.java

• https://h5.efectivoya.mx • https://h5.efectivoya.mx/	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
EasyPermissions	Google	EasyPermissions 是一个包装器库，用于简化针对 Android M 或更高版本的基本系统权限逻辑。
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。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本的 Android 屏幕适配方案
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
android.studio@android.com	自研引擎-S

第三方追踪器检测

名称	类别	网址
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12

敏感凭证泄露检测

可能的密钥
"tip_to_private_protocol" : "Comentario"
c1fcbf843b78b13b40d6411b25989d9a
b9372d7b7870300534c063882f90f25c

a8c365097c78a355a633fd5a7cdcaa94
cb092b65ecbc0935a30f52bfb72493ea
YW5kcm9pZC5wZXJtaXNzaW9uLIJFQURfU01T
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F

Google Play 应用市场信息

标题: EfectivoYa - Préstamo rápido

评分: 4.5416465 **安装:** 500,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** mx.efectivoya.loan

开发者信息: EfectivoYa Team, EfectivoYa+Team, None, None, enquiries@efectivoya.mx,

发布日期: None **隐私政策:** Privacy link

关于此应用:

EfectivoYa 是一个数字平台，以简单、安全的方式提供在线贷款。该平台允许用户无需前往实体网点即可申请贷款，简化了紧急情况下的流程。EfectivoYa 旨在解决即时的财务需求，特别是在需要少量资金的情况下。其流程简单易行，有助于在家中获得融资。 申请贷款的要求： 是墨西哥公民且年满 18 岁。 拥有一份有稳定收入的工作。 平台使用说明： 下载 EfectivoYa 应用程序。 注册并选择所需的贷款。 等待贷款批准。 收到账户里的钱。 遵守既定付款。 提供的贷款详情： 贷款金额：500 美元至 50,000 美元墨西哥比索之间。 日利率：0.05%（年利率最高可达 18%）。 增值税 (VAT)：5%。 年等值利率 (APR)：高达 18%。 佣金：从 50 美元到 250 美元不等，具体取决于客户的信用评分。 贷款期限：91至210天。 贷款计算示例： 对于 100 天期限的 5,000 美元贷款，细目分类如下： 利息：5,000 美元 * 0.05% * 100 天 = 250 美元。 佣金：250 美元。 增值税：5,000 美元 * 5% = 250 美元。 支付总额：5,750 美元。 平台保障客户信息安全。客户必须在约定的期限内付款，以避免因逾期付款而产生拖欠利息，这一点至关重要。 接触： EfectivoYa 的客户服务时间为周一至周五上午 9:00 至下午 6:30。查询电子邮件：enquiries@efectivoya.mx。

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。