南明离火
移动应用检测平台

ANDROID 静态分析报告

CashVia • v1.6.02

分析日期: 2025-08-26 11:36:48

应用概览

文件名称:	com.cashvia.prestamos.apk
文件大小:	17.99MB
应用名称:	CashVia
软件包名:	com.cashvia.prestamos
主活动:	com.xy.credyclub.view.XYStartUpActivity
版本号:	1.6.02
最小SDK:	21
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:	55/100 (中风险)
跟踪器检测:	4/432
杀软检测:	经检测，该文件安全
MD5:	f4bef292cb3912c6a191e5abf4a20806
SHA1:	821257345f86bbf03b170a6d6238dae61d4d52c6
SHA256:	f4ecf92a2ffc43aefab868f1562154004b7ef04780ac65e3ad55224fc9e26ed8

分析结果严重性分布

高危	中危	信息	安全	关注
2	16	2	3	0

四大组件导出状态统计

Activity组件：21个，其中export的有： 0个
Service组件：10个，其中export的有： 1个
Receiver组件：4个，其中export的有： 2个
Provider组件：5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: 2024-09-09 16:37:46+00:00
有效期至: 2054-09-09 16:37:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x6a87f04fe0628d142b9a8d02d35d4f14af503994
哈希算法: sha256
证书MD5: 023d12b1923a2fdba36a56c0b7ebb053
证书SHA1: 7f653dd5eb670e3057bbb34602f45e317a168cde
证书SHA256: 61879822e839fbe4382e4b1d6dada8b1c585540af514211366ebb28e70774962
证书SHA512:
9c247f3bf74b885b8e9f70d775803517208ed76e7ccb6cf33b9869325e31b605c859228a2cba7b4105eebb0a6526db4b55bd674afb505d508dbdc3b02747eb99

公钥算法: rsa
密钥长度: 4096
指纹: 983dd1b96f7d9236b75ec459e45e778b9941feadf1415bcbe3721edd19f55120
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.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_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.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.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_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.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_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.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.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	未知权限	来自 android 引用的未知权限。

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.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.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.cashvia.prestamos.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.xy.credyclub.view.XYStartUpActivity	Schemes: cashvia://,

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: **4** | 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 (com.xy.release.SmsAutoFileReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.phone.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.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。
4	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: **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	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	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

5	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
6	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
7	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
8	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	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-2	升级会员：解锁高级权限
9	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
10	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
11	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
12	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
13	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

14	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
15	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
16	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

应用行为分析

编号	行为	标签	文件
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
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
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
00123	连接到远程服务器后将响应保存为JSON	网络 命令	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
00025	监视要执行的一般操作	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
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
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
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
00130	获取当前WIFI信息	WiFi 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
00116	获取当前WiFi MAC地址并放入JSON中	WiFi 信息收集	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
00082	获取当前WiFi MAC地址	信息收集 WiFi	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
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
00153	通过 HTTP 发送二进制数据	http	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
00126	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
00188	获取短信地址	短信	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	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
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
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
00114	创建到代理地址的安全套接字连接	网络 命令	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

00162	创建 InetSocketAddress 对象并连接到它	socket	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
00163	创建新的 Socket 并连接到它	socket	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
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
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
00134	获取当前WiFi IP地址	WiFi 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
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
00115	获取设备的最后已知位置	信息收集 位置	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
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
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
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
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
00042	查询WiFi BSSID及扫描结果	信息收集 WiFi	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

敏感权限滥用分析

类型	匹配	权限

本报告由南明离火移动安全分析平台生成

恶意软件常用权限	5/30	android.permission.READ_SMS android.permission.ACCESS_COARSE_LOCATION android.permission.READ_PHONE_STATE android.permission.CAMERA android.permission.WAKE_LOCK
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE 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
scdn-stestsettings.s	安全	否	No Geolocation information available.
slaunches.s	安全	否	No Geolocation information available.
app-measurement.com	安全	是	**IP地址:** 180.163.151.33 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图
goo.gl	安全	否	**IP地址:** 216.58.214.14 **国家:** 德国 **地区:** 黑森 **城市:** 美因河畔法兰克福 **纬度:** 50.110882 **经度:** 8.681996 **查看:** Google 地图
scdn-ssettings.s	安全	否	No Geolocation information available.
sonelink.s	安全	否	No Geolocation information available.
svalidate-and-log.s	安全	否	No Geolocation information available.
sapp.s	安全	否	No Geolocation information available.
firebase-settings.crashlytics.com	安全	是	**IP地址:** 180.163.150.162 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.230416 **经度:** 121.473701 **查看:** 高德地图

sregister.s	安全	否	No Geolocation information available.
simpression.s	安全	否	No Geolocation information available.
smonitorsdk.s	安全	否	No Geolocation information available.
sgcdsdk.s	安全	否	No Geolocation information available.
app.cashvia.mx	安全	否	**IP地址:** 18.238.243.47 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
ssdk-services.s	安全	否	No Geolocation information available.
sinapps.s	安全	否	No Geolocation information available.
aps-webhandler.appsflyer.com	安全	否	**IP地址:** 18.238.243.47 国家: 荷兰（王国） 地区: 北荷兰省 城市: Cook IslandsCopan CopperbeltCoquimbo CordilleraCordobaCorkCoronie Corozal CorrientesCorseCort 纬度: 52.378502 经度: 4.899980 查看: Google 地图
sviap.s	安全	否	No Geolocation information available.
svalidate.s	安全	否	No Geolocation information available.
tracker.cashvia.mx	安全	否	**IP地址:** 18.238.243.47 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:** 122.8.178.157 国家: 爱尔兰 地区: 都柏林 城市: 都柏林 纬度: 53.344151 经度: -6.267249 查看: Google 地图
sconversions.s	安全	否	No Geolocation information available.
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.151.38 国家: 中国 地区: 上海 城市: 上海 纬度: 31.230416 经度: 121.473701 查看: 高德地图

sattr.s	安全	否	No Geolocation information available.
sadrevenue.s	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://%sapp.%s	com/appsflyer/internal/AFj1mSDK.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/ • https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	A2/C0026a.java
• https://sites.google.com/view/cashvia-customer-agreement/home	B2/g.java
• https://tracker.cashvia.mx/sa?project=production	com/xy/credyclub/MineApp.java
• https://app-measurement.com/a • https://app-measurement.com/s	d1/r.java
• https://%sregister.%s/api/v	com/appsflyer/internal/AFg1lSDK.java
• https://%sadrevenue.%s/api/v2/log/adimpression/v6.14.1/android?app_id= • https://%slaunches.%s/api/v • https://%sadrevenue.%s/api/v2/generic/v6.14.1/android?app_id= • https://%svalidate.%s/api/v • https://%ssdk-services.%s/validate-android-signature • https://%sconversions.%s/api/v • https://%sinapps.%s/api/v • https://%smonitorsdk.%s/api/remote-debug/v2.0?app_id= • https://aps-webhandler.appsflyer.com/api/trigger • https://%sattr.%s/api/v	com/appsflyer/internal/AFj1uSDK.java
• www.google.com • https://www.google.com • https://goo.gl/naoooi	d1/w1.java
• https://%smonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFd1dSDK.java
• https://firebase.google.com/support/guides/disable-analytics	d1/C0346C.java
• https://%scdn-%stestsettings.%s/android/v1/%s/settings • https://%scdn-%ssettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFe1bSDK.java
• javascript:findwebrtcinfo	com/datavisorobfus/h.java
• https://%sviap.%s/api/v1/android/validate_purchase_v2?app_id= • https://%sviap.%s/api/v1/android/validate_purchase?app_id= • https://%sgcdsdk.%s/install_data/v5.0/ • https://%svalidate-and-log.%s/api/v1.0/android/validateandlog?app_id= • https://%sonelink.%s/shortlink-sdk/v2	com/appsflyer/internal/AFe1rSDK.java
• https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
• https://accounts.google.com/o/oauth2/revoke?token=	E0/b.java

• https://app.cashvia.mx/cashvia/	j2/e.java
• https://sites.google.com/view/cashvia-privacy-agreement/home	L0/d.java
• https://play.google.com/store/apps/details?id=	N2/w.java
• https://firebase.google.com/support/privacy/init-options	Q1/e.java
• https://api.whatsapp.com/send?phone=	u2/j.java
• https://tracker.cashvia.mx/sa?project=production	V2/C0286a.java
• https://tracker.cashvia.mx/sa?project=production	V2/C0667a.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	w0/b.java
• https://sites.google.com/view/cashvia-customer-agreement/home	w2/i.java
• https://sites.google.com/view/cashvia-loan-agreement/home	Z2/C0391e.java
• https://sites.google.com/view/cashvia-loan-agreement/home	Z2/C0790e.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/1048986715349/namespaces/firebase:fetch?key=AIzaSyBmYnDJti6ZmJs6WCHuCymaeBU0BnwKzew) 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
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。
神策分析 SDK	神策	神策分析，是针对企业级客户推出的深度用户行为分析产品，支持私有化部署，客户端、服务器、业务数据、第三方数据的全端采集和建模，驱动营销渠道效果评估、用户精细化运营改进、产品功能及用户体验优化、老板看板辅助管理决策、产品个性化推荐改造、用户标签体系构建等应用场景。作为 PaaS 平台支持二次开发，可通过 BI、大数据平台、CRM、ERP 等内部 IT 系统，构建用户数据体系，让用户行为数据发挥深远的价值。

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).

邮箱地址敏感信息提取

EMAIL	源码文件
service@cashvia.mx	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
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sensors Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/248

敏感凭证泄露检测

可能的密钥
"com.google.firebase.crashlytics.mapping_file_id" : "603a826298a743769f99c0011cb2fb9c"
"google_api_key" : "AIzaSyBmYnDJtf6ZmJs6WCHuCymaeBU0BnwKzew"
"google_app_id" : "1:1041986715349:android:5223ad223b157d834fce5c"
"google_crash_reporting_api_key" : "AIzaSyBmYnDJtf6ZmJs6WCHuCymaeBU0BnwKzew"
"local_key" : "6LJHsi98e4"
470fa2b4ae81cd56ecbcda9735803434cec591fa

E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
dI2H2mzZqo8OQIQxI/oZ8itF3Lf7XC57dQ==
MJCR3nbjtc8ARKt9HOAI/AZAzrHiEyhubQ==
H6ik7UfoqtAwYIZxE9A68jVW8J/oAjw=
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
KZGR3Uffq88OW6tuEewC9j5V3A==
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
MJCR3nbjtc8ARKt/AP825zhTxLPuFzw=

Google Play 应用市场信息

标题: CashVia-Crédito Ágil y Seguro

评分: 4.8195014 安装: 500,000+ 价格: 0 **Android**版本支持: 分类: 财务 **Play Store URL:** com.cashvia.prestamos

开发者信息: Cashvia, Cashvia, None, https://www.cashvia.mx, service@cashvia.mx

发布日期: None 隐私政策: Privacy link

关于此应用:

CashVia 是一款在线个人贷款应用程序。我们为墨西哥居民提供优质个人贷款。信用良好且按时还款的用户可以持续提升贷款额度。申请流程简单透明，只需下载应用程序即可享受我们的贷款服务。 产品信息 高额贷款：1,000 至 20,000 美元。最高贷款额为 20,000 美元。 还款期限长：最短还款期限为 91 天，最长还款期限为 180 天。 低利率： 最低日利率为 0.01%，最低年利率 (APR) 为 3.6%。 最高日利率为 0.08%，最高年利率 (APR) 为 28.8%。 产品信息不固定，贷款金额、还款期限和利率均需经批准。 产品特点： 分期贷款，即时到账。 无纸化在线流程，快速申请。 安全便捷，无需担保人。 只需有效身份证件。 从申请到付款，交易透明透明。 零用户骚扰。 信用记录良好的用户可享受更高的贷款额度、更长的贷款期限和更多优惠。 成本示例：如果您申请一笔 20,000 美元的贷款，期限为 120 天（4 个月），日利率为 0.08%（年利率 28.8%），您的成本如下： 每日应付利息：20,000 美元 * 0.08% = 16 美元 每月应付利息：20,000 美元 * 0.08% / 120 * 30 = 480 美元 应付利息总额：20,000 美元 * 0.08% * 120 = 1,920 美元 每月应付本金：20,000 美元 / 4 = 5,000 美元 每月应付总额：5,000 美元 + 1,920 美元 = 6,920 美元 应付总额：20,000 美元 + 1,920 美元 = 21,920 美元 以上金额仅供参考，实际金额以实际为准批准。 如何获得资格？ 年满 18 周岁。 是墨西哥公民并居住在墨西哥。 拥有有效的手机号码。 拥有政府签发的有效身份证件。 隐私 我们致力于保护所有用户的信息。我们的隐私政策在应用程序的各个部分都有维护，因此您可以放心，我们不会与第三方共享您的个人信息。您可以随时在此处查看我们的隐私政策：https://sites.google.com/view/cashvia-privacy-policy 联系我们 电话：+52 5596523553 邮箱：service@cashvia.mx 地址：墨西哥城，库奥特莫克市政厅，中心区，Regina 94，204 号公寓，邮编 06090 网站：https://www.cashvia.mx/ 营业时间：周一至周六，上午 8:30 至下午 5:30

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。