南明离火
移动应用检测平台

ANDROID 静态分析报告

LoanMax • v2.0.6

分析日期: 2025-04-26 15:20:53

应用概览

文件名称:	com.cash.bintup.tala.prestamo.baubap.rapido.dinero v2.0.6.apk
文件大小:	7.03MB
应用名称:	LoanMax
软件包名:	com.cash.bintup.tala.prestamo.baubap.rapido.dinero
主活动:	com.catchpig.kmvvm.main.WelcomeActivity
版本号:	2.0.6
最小SDK:	24
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:	51/100 (中风险)
跟踪器检测:	3/432
杀软检测:	3 个杀毒软件报毒
MD5:	02aca8399f4c99130452ddd290b42b35
SHA1:	fa48b6ddacf8e10921966a9f4b71844321e98fc
SHA256:	8bbec363f238c973f043d1030f260cd291c83ac763d7b767927fb65212ae22f0

分析结果严重性

高危	中危	信息	安全	关注
1	15	2	1	0

四大组件信息

Activity组件：35个，其中export的有： 5个
Service组件：3个，其中export的有： 0个
Receiver组件：4个，其中export的有： 1个
Provider组件：4个，其中export的有： 0个

证书信息

二进制文件已签名
v1 签名: False
v2 签名: True
v3 签名: False
v4 签名: False
主题: CN=Bintup, OU=Bintup, O=Bintup MX, L=Mexcio city, ST=Mexcio, C=MX
签名算法: rsassa_pkcs1v15
有效期自: 2023-12-03 05:31:24+00:00
有效期至: 2048-11-26 05:31:24+00:00
发行人: CN=Bintup, OU=Bintup, O=Bintup MX, L=Mexcio city, ST=Mexcio, C=MX
序列号: 0x1
哈希算法: sha256
证书MD5: f98e355fb44094854e3392594f85734a
证书SHA1: 385fcfc4808491c258226ae3ddbfe6571eae81ec
证书SHA256: a96148d81ddc277a4079eabe043cd2e111fb4c99eb281bee93da78c3b05b0aef
证书SHA512:
2fdad8596f5ac4d1cf91cec0005e5138dcd02bfbe2ca4ee70ffe22c2106e79efdba375c1b34369f1717c737d8674e6bc4deb0a34a2082359786b6eacdc0f5623

公钥算法: rsa
密钥长度: 2048
指纹: 8a052ba86c4c79216754e6cc2475da72bf989f79215ae418d03e102760a69d5e
找到 1 个唯一证书

应用权限

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.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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	普通	后台下载文件	这个权限是允许应用通过下载管理器下载文件，且不对用户进行任何提示。
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_PROFILE	危险	读取用户资料	允许应用程序读取用户个人信息。
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.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。
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。
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。
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.cash.bintup.tala.prestamo.baubap.rapido.dinero.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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	应用程序使用代码签名证书进行签名

MANIFEST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	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
2	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
3	Activity (com.catchpig.kmvvm.main.LoadHtmlAc) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
4	Activity (com.catchpig.kmvvm.main.view.MainActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
5	Activity (com.catchpig.kmvvm.main.login.LoginAc) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

6	Activity (com.catchpig.kmvvm.main.mine.BalanceAc) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
7	Broadcast Receiver (com.catchpig.mvvm.receiver.InstallReferrerReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
8	Activity (com.catchpig.kmvvm.main.mine.TakePicturesAc) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

</> 安全漏洞检测

高危: **1** | 警告: **5** | 信息: **2** | 安全: **0** | 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

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	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
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

行为分析

编号	行为	标签	文件
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
00013	读取文件并将其放入流中	文件	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
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
00015	将缓冲流（数据）放入 JSON 对象	文件	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
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
00191	获取短信收件箱中的消息	短信	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
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
00053	监视给定内容 URI 标识的数据更改（SMS、MMS 等）	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
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
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
00003	将压缩后的位图数据放入JSON对象中	相机	升级会员：解锁高级权限
00159	使用辅助服务执行通过文本获取节点信息的操作	无障碍服务	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
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	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
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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	4/30	android.permission.CAMERA android.permission.ACCESS_COARSE_LOCATION android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK
其它常用权限	8/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES 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。

域名检测

域名	状态	中国境内	位置信息
svalidate.s	安全	否	No Geolocation information available.
aps-webhandler.appsflyer.com	安全	否	**IP地址:** 13.226.210.33 **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
sregister.s	安全	否	No Geolocation information available.
smonitorsdk.s	安全	否	No Geolocation information available.
app-measurement.com	安全	否	**IP地址:** 142.250.189.14 **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
ssdk-services.s	安全	否	No Geolocation information available.
scdn-ssettings.s	安全	否	No Geolocation information available.
facebook.com	安全	否	**IP地址:** 31.13.70.36 **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
graph.s	安全	否	No Geolocation information available.
sinapps.s	安全	否	No Geolocation information available.
scdn-stestsettings.s	安全	否	No Geolocation information available.
sapp.s	安全	否	No Geolocation information available.
graph-video.s	安全	否	No Geolocation information available.
goo.gl	安全	否	**IP地址:** 142.250.72.238 **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
sadrevenue.s	安全	否	No Geolocation information available.

pagead2.googlesyndication.com	安全	否	**IP地址:** 142.250.68.66 **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
slaunches.s	安全	否	No Geolocation information available.
sgcdsdk.s	安全	否	No Geolocation information available.
sconversions.s	安全	否	No Geolocation information available.
sattr.s	安全	否	No Geolocation information available.
svalidate-and-log.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.

URL链接分析

URL信息	源码文件
• https://%scdn-%stestsettings.%s/android/v1/%s/settings • https://%scdn-%ssettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFe1gSDK.java
• https://goo.gl/j1swqy	w2/p2.java
• https://goo.gl/naoooi	a3/ga.java
• https://app-measurement.com/a	w2/gb.java
• https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
• https://.facebook.com • https://facebook.com	x1/x.java
• https://graph-video.%s • https://graph.%s	x1/u.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	j2/b.java
• https://%sapp.%s	com/appsflyer/internal/AFj1qSDK.java

本报告由南明离火移动安全分析平台生成

• https://%sadrevenue.%s/api/v2/log/adimpression/v6.14.0/android?app_id= • https://%slaunches.%s/api/v • https://%sinapps.%s/api/v • https://%sconversions.%s/api/v • https://aps-webhandler.appsflyer.com/api/trigger • https://%ssdk-services.%s/validate-android-signature • https://%svalidate.%s/api/v • https://%sadrevenue.%s/api/v2/generic/v6.14.0/android?app_id= • https://%sattr.%s/api/v • https://%smonitorsdk.%s/api/remote-debug/v2.0?app_id=	com/appsflyer/internal/AFj1xSDK.java
• https://www.google.com • www.google.com	a3/z6.java
• https://%smonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFd1aSDK.java
• https://app-measurement.com/a	a3/u2.java
• https://%sregister.%s/api/v	com/appsflyer/internal/AFg1nSDK.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/AFe1ySDK.java

FIREBASE数据库分析

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/644108561098/namespaces/firebase:fetch?key=AIzaSyDMUeB6apMxXWZWbUrASiHAsgyKySaUP7A ）已禁用。响应内容如下所示:
		{
		"state": "NO_TEMPLATE"
		}

第三方SDK

SDK名称	开发者	描述信息
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
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。
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。

追踪器

名称	类别	网址
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

密钥凭证

可能的密钥
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"google_api_key" : "AIzaSyDMUeB6apMxXWZWbUrASiHAsgyKy3[illegible]P7A"
"google_app_id" : "1:644108561098:android:0b543273a2[illegible]306b2233"
"google_crash_reporting_api_key" : "AIzaSyDMUeB6apMxXWZWbUrASiHAsgyKy3aUP7A"
FFE391E0EA186D0734ED601E4E70E3224B[illegible]48E2075BAC46D8C667EAE7212
8a3c4b262d721acd49a4bf97d5213[illegible]6fa2b9
2438bce1ddb7bd026d5ff89f59[illegible]5e5bb824b3
df6b721c8b4d3b6eb44[illegible]4415007e5a35fc95
c56fb7d591ba6[illegible]047fd98f535372fea00211
a4b7452[illegible]ed8f5f[illegible]1058ca7bbfd26b[illegible]214bfc
FBA3AF4E7757D9016E953FB3[illegible]671CA2BD9AF725F9A53D52ED4A38EAAA08901
E3F9E1E0CF99D0E56A05[illegible]41B3399F7CEA524326B0CDD6EC1327ED0FDC1
3BAF59A2E5331[illegible]675FA[illegible]35FF5FFF0D116142D3D4664F1C3CB804068B40614F
9b8f518b086098de3d77736f9458a3d2f6f95a37
cc2751449a350f668590264ed76692694a80308a

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。