南明离火
移动应用检测平台

ANDROID 静态分析报告

AdaModal v1.4.0

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2025-08-01 16:17:07

应用概览

文件名称:	adamodal-GooglePlayRelease-V10400-20250707.apk
文件大小:	13.4MB
应用名称:	AdaModal
软件包名:	com.adamodal.fintech
主活动:	com.common.fine.activity.SplashActivity
版本号:	1.4.0
最小SDK:	21
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:	50/100 (中风险)
跟踪器检测:	6/432
杀软检测:	AI评估：安全
MD5:	233ca07ceb0b2e4bc469b40762f833c5
SHA1:	18768b9c27ac325b786cabfb0ab1c22f6e048698
SHA256:	ac24128ec3112306118f113ad356ea0953927426ac3c6a896ffa855ae0f4cb81

分析结果严重性分布

高危	中危	信息	安全	关注
4	18	3	3	0

四大组件导出状态统计

Activity组件：14个，其中export的有： 3个
Service组件：13个，其中export的有： 0个
Receiver组件：9个，其中export的有： 4个

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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: False
v4 签名: False
主题: C=adamodal, ST=adamodal, L=adamodal, O=adamodal, OU=adamodal, CN=adamodal
签名算法: rsassa_pkcs1v15
有效期自: 2020-09-26 06:29:24+00:00
有效期至: 2096-09-07 06:29:24+00:00
发行人: C=adamodal, ST=adamodal, L=adamodal, O=adamodal, OU=adamodal, CN=adamodal
序列号: 0xd5288cf
哈希算法: sha256
证书MD5: 323f152adc67524cccdde1d45efa4db1
证书SHA1: 8b1413290e1f11890bdbecc9787ec81fd668586b
证书SHA256: e60d85864b8d4030ca1656114a6f0d2fbe18a4be4044d216f72c5f5a490d9ebd
证书SHA512:
d18667a4d4df256d48f565e3348a8256d284cdf4e29a4542d17c8181fcc6afa293683011cff35159[illegible]f8d141d9e10139da6a8[illegible]c04c9ddb2d85a27f68ca

公钥算法: rsa
密钥长度: 2048
指纹: f7329a6f3739bb1439a1697c1cbdcc1758f08688100bbe6ee3d6ff453c01c761
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.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.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_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.HIGH_SAMPLING_RATE_SENSORS	普通	传感器的数据刷新率限制	允许应用以大于 200 Hz 的采样率访问传感器数据，此数据包括由设备的加速度，陀螺仪和磁力传感器记录的值。
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。
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.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.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。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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.adamodal.fintech.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.common.fine.activity.SplashActivity	Schemes: @7F100004://, Hosts: splash,
com.common.fine.activity.ARouterActivity	Schemes: @7F100004://, Hosts: m.app.com,

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	应用已配置网络安全策略 [android:networkSecurityConfig=@7F130001]	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	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。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

3	Broadcast Receiver (com.appsflyer.MultipleInstallBroadcastReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.INSTALL_PACKAGES [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。
4	Broadcast Receiver (com.common.fine.receiver.InstallReferrerReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.INSTALL_PACKAGES [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。
5	Activity (com.common.fine.activity.FireBaseMsgActivity) 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。
6	Activity (com.common.fine.activity.ARouterActivity) 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。
7	Activity (com.common.fine.IdCardCameraActivity) 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。
8	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。
9	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: **3** | 警告: **9** | 信息: **2** | 安全: **2** | 屏蔽: **0**

本报告由南明离火移动安全分析平台生成

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	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
3	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
4	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
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	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
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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

9	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
10	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
11	该文件是World Writable。任何应用程序都可以写入文件	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
12	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
13	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
14	使用弱加密算法	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-4	升级会员：解锁高级权限
15	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

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

16	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

1	arm64-v8a/libblurdetector.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离
2	arm64-v8a/libfacial_action.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项 -fstack-protector-all 来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

3	arm64-v8a/libmontc.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__vsprintf_chk']	True info 符号被剥离

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
00036	从 res/raw 目录获取资源文件	反射	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
00091	从广播中检索数据	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
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	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
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
00038	查询电话号码	信息收集	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
本报告由南明离火移动安全分析平台生成

00043	计算WiFi信号强度	信息收集 WiFi	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
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
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
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
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
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
00153	通过 HTTP 发送二进制数据	http	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
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
00082	获取当前WiFi MAC地址	信息收集 WiFi	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

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.CAMERA android.permission.ACCESS_COARSE_LOCATION android.permission.WAKE_LOCK

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

其它常用权限	6/46	android.permission.INTERNET com.google.android.c2dm.permission.RECEIVE android.permission.ACCESS_NETWORK_STATE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.gms.permission.AD_ID android.permission.FLASHLIGHT

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
ada-modal.firebaseio.com	安全	否	**IP地址:** 34.120.206.254 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
scdn-ssettings.s	安全	否	No Geolocation information available.
sattr.s	安全	否	No Geolocation information available.
sadrevenue.s	安全	否	No Geolocation information available.
appapi.adamodal.co.id	安全	否	**IP地址:** 149.129.254.251 **国家:** 印度尼西亚 **地区:** 雅加达雷亚 **城市:** 雅加达 **纬度:** -6.208678 **经度:** 106.845490 **查看:** Google 地图
sonelink.s	安全	否	No Geolocation information available.
scdn-stestsettings.s	安全	否	No Geolocation information available.
slaunches.s	安全	否	No Geolocation information available.
sdlsdk.s	安全	否	No Geolocation information available.
overmind.datatrombem.com	安全	否	**IP地址:** 142.251.36.19 **国家:** 德国 **地区:** 拜仁 **城市:** 慕尼黑 **纬度:** 48.137428 **经度:** 11.575490 **查看:** Google 地图

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

apph5.adamodal.co.id	安全	否	**IP地址:** 149.129.254.251 **国家:** 印度尼西亚 **地区:** 雅加达雷亚 **城市:** 雅加达 **纬度:** -6.208678 **经度:** 106.845490 **查看:** Google 地图
simpression.s	安全	否	No Geolocation information available.
ssdk-services.s	安全	否	No Geolocation information available.
smonitorsdk.s	安全	否	No Geolocation information available.
sinapps.s	安全	否	No Geolocation information available.
sapp.s	安全	否	No Geolocation information available.
sconversions.s	安全	否	No Geolocation information available.
svalidate.s	安全	否	No Geolocation information available.
sgcdsdk.s	安全	否	No Geolocation information available.
sregister.s	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件
• https://%scdn-%ssettings.%s/android/v1/%s/settings • https://%scdn-%stestsettings.%s/android/v1/%s/settings	com/appsflyer/internal/AFe1jSDK.java
• javascript:webviewjavascriptbridge._fetchqueue	com/common/fine/utils/jsbridge/BridgeWebView.java
• javascript:webviewjavascriptbridge • javascript:webviewjavascriptbridge._fetchqueue	com/common/fine/utils/jsbridge/BridgeUtil.java
• https://%smonitorsdk.%s/remote-debug/exception-manager	com/appsflyer/internal/AFd1bSDK.java
• https://%sapp.%s	com/appsflyer/internal/AFj1zSDK.java
• https://%simpression.%s	com/appsflyer/share/CrossPromotionHelper.java
• https://%sdlsdk.%s/v1.0/android/	com/appsflyer/internal/AFc1qSDK.java
• https://%sregister.%s/api/v	com/appsflyer/internal/AFg1tSDK.java

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

• https://%svalidate.%s/api/v • https://%ssdk-services.%s/validate-android-signature • https://%sdlsdk.%s/v1.0/android/ • https://%sadrevenue.%s/api/v2/generic/v6.13.0/android?app_id= • https://%sattr.%s/api/v • https://%sconversions.%s/api/v • https://%slaunches.%s/api/v • https://%smonitorsdk.%s/api/remote-debug/v2.0?app_id= • https://%sinapps.%s/api/v • https://%sadrevenue.%s/api/v2/log/adimpression/v6.13.0/android?app_id=	com/appsflyer/internal/AFi1cSDK.java
• http://182.131.12.68/services/cameracoresvr.php • http://xiangji.qq.com/services/cameracoresvr.php	com/oliveapp/camerasdk/a/a.java
• https://overmind.datatheorem.com/trustkit/report	com/datatheorem/android/trustkit/config/DomainPinningPolicy.java
• https://%sgcdsdk.%s/install_data/v5.0/ • https://%sonelink.%s/shortlink-sdk/v2	com/appsflyer/internal/AFe1zSDK.java
• https://appapi.adamodal.co.id/ • https://ada-modal.firebaseio.com • https://apph5.adamodal.co.id/	自研引擎-S
• https://github.com/opencv/opencv/pull/15050	lib/arm64-v8a/libblurdetector.so

Firebase 配置安全检测

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://ada-modal.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	Firebase远程配置URL（ https://firebaseremoteconfig.googleapis.com/v1/projects/821665501456/namespaces/firebase:fetch?key=AIzaSyDI5zwtLC4-7snXYjDhy0zWKb9akKk7uas ） 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
C++ 共享库	Android	在 Android 应用中运行原生代码。
Jetpack Camera	Google	CameraX 是 Jetpack 的新增库。利用该库，可以更轻松地向应用添加相机功能。该库提供了很多兼容性修复程序和解决方法，有助于在众多设备上打造一致的开发者体验。
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。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Google Analytics	Google	提供各种 API，可帮助您收集、配置和报告用户与您的在线内容进行互动的数据。
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 Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

敏感凭证泄露检测

可能的密钥
腾讯位置服务的=> "TencentMapSDK" : "QNABZ-BRQ6F-G24J5-N3RB5-YKN6V-XRFMX"
"google_api_key" : "AIzaSyDI5zwtLC4-7snXYjDhy0zWKb9akKk7uas"
"AF_SDK_KEY" : "ZBWSDFpPsUUSXtTsNWZTr3"
"FACEBOOK_APP_ID" : "1054179072412541"
"APP_IDENTIFIER" : "adamodal"

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

"firebase_database_url" : "https://ada-modal.firebaseio.com"
"ACCOUNT_KIT_CLIENT_TOKEN" : "152639dd1b25ba10641d43f283c3f90f"
"google_app_id" : "1:821665501456:android:386eea23d222f092301595"
"google_crash_reporting_api_key" : "AIzaSyDI5zwtLC4-7snXYjDhy0zWKb9akKk7uas"
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
n2fhYkNUu36DS/4ltCkZlgZ00GXWUIks9WA1U7ACqyDvvj5MAigqS6wtONTI3wyqM
cc2751449a350f668590264ed76692694a80308a
9b8f518b086098de3d77736f9458a3d2f6f95a37
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCiLegYm89cDdcDPp8SiaRY2CLe
npviV9y1ve+zgSOz8j2aE2ous4NuxgF38OqnqCbWTzbf1B9vvWqsPW5+givHDRbo
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
c56fb7d591ba6704df047fd98f535372fea00211
a4b7452e2ed8f5f191058ca7bbfd26b0d32[illegible]

本报告由南明离火移动安全分析平台生成

Google Play 应用市场信息

标题: Ada Modal-Pinjaman Uang Online

评分: 4.5199265 **安装:** 5,000,000+ **价格:** 0 **Android版本支持:** **分类:** 财务 **Play Store URL:** com.adamodal.fintech

开发者信息: PT Solid Fintek Indonesia, PT+Solid+Fintek+Indonesia, None, https://www.adamodal.co.id/, cs@adamodal.co.id,

发布日期: None **隐私政策:** Privacy link

关于此应用:

AdaModal是一款高效、易用的在线贷款应用程序，提供安全、专业、智能、实用的贷款服务。 我们帮助您解决紧迫的资金需求，成为您值得信赖的合作伙伴。此应用程序已获得许可并受 OJK（金融服务管理局）监管。 产品介绍 AdaModal坚守核心，不做高息贷款产品，专门为年轻人提供优质、低息的贷款产品。当天申请，当天入账，且无需提供任何抵押物，贷款利率极低，无需担心借钱 产品卓越 7*24小时在线申请，无需见面，无需电话麻烦，信用良好即可申请贷款 贷款利息极低，申请IDR1,000,000，日利息仅IDR6 支付便捷，支持线上线下支付，就近即可支付 贷款产品 最低年龄：21 岁及以上 金额：IDR 1,000,000-IDR 20,000,000 贷款期限：91 - 365 天 年贷款利率（最高年利率）：21.9% 管理费：0% 示例：如果您选择为期 1 年的 2,400,000 印尼盾现金贷款，利息为 0.06% 利息总额：2,400,000 印尼盾* (21.9%/365)*365= 525,600 印尼盾 付款总额：Rp. 2,400,000 + Rp. 525,600=Rp. 2,925,600 每月利息：525,600卢比/12=43,800卢比 每月分期付款金额：Rp. 2,400,000/12 + Rp. 43,800=Rp. 243,800 如何按时付款？ 1. 您可以通过电子钱包或网上银行（BCA、Mandiri、BRI、BNI、CIMB等）或在Alfamart进行付款！ 2. 您可以在到期日或之前随时全额或部分付款。 3.简单的付款时间表，让您轻松按时付款。 联系信息 公司名称: PT Solid Fintek 印度尼西亚 公司网址：http://www.adamodal.co.id/ 联系电话：021-31196080 联系电子邮件：cs@adamodal.co.id 联系地址：Green Lake City Complex, Rukan Greet Wall Blok B no.27 Kel。 Gondrong, Cipondoh 区, 唐格朗市, 万丹省, 15147

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。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成