



ANDROID 静态分析报告



📱 VidMate Cash • v7.2001

分析日期: 2025-04-01 22:06:47

i应用概览

文件名称:	VidMate Cash v7.2001.apk
文件大小:	26.55MB
应用名称:	VidMate Cash
软件包名:	com.video.cash.app
主活动:	com.nemo.vidmate.host.WelcomeActivity
版本号:	7.2001
最小SDK:	18
目标SDK:	28
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	30/100 (高风险)
跟踪器检测:	3/432
杀软检测:	经检测, 该文件安全
MD5:	cb6d9dcce88a8ec3b5bf2e452691537f
SHA1:	bb02eca94fb2e8f9ae4ee1cd092e94d5d0b6be1d
SHA256:	f696033b17841e8b2f5d28c0c02fdcd5dab1d4fcd0c59939afc9263ddcd1699a

📊分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✅ 安全	🔍 关注
26	26	1	3	2

📦四大组件导出状态统计

Activity组件: 30个, 其中export的有: 10个
Service组件: 18个, 其中export的有: 4个
Receiver组件: 10个, 其中export的有: 1个
Provider组件: 3个, 其中export的有: 0个

🔑应用签名证书信息

二进制文件已签名
 v1 签名: True
 v2 签名: False
 v3 签名: False
 v4 签名: False
 主题: C=cash, ST=cash, L=cash, O=cash, OU=cash, CN=cash
 签名算法: rsassa_pkcs1v15
 有效期自: 2022-01-28 10:37:26+00:00
 有效期至: 2047-01-22 10:37:26+00:00
 发行人: C=cash, ST=cash, L=cash, O=cash, OU=cash, CN=cash
 序列号: 0x2efe3af9
 哈希算法: sha256
 证书MD5: 12db31168c848281dcbe26f68ae780a8
 证书SHA1: 77e0d52efa3a30c83dbb99ccfa0e41038844ee93
 证书SHA256: ac3acc4bab32960b449535c9323bb78310f0e3e35e46b5a5405ec26e79b387e9
 证书SHA512:
 32089f97430be4432520ff6307b39794e7fe3913d912a71a229f8b553d82c579a5e548d7ebdb224d57347e4456267e2912b17c584624a7a1b2557cd3d0d39af7

找到 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.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_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
com.video.cash.app.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
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_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_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.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.BROADCAST_STICKY	普通	发送置顶广播	允许应用程序发送顽固广播，这些广播在结束后仍会保留。恶意应用程序可能会借此使手机耗用太多内存，从而降低其速度或稳定性。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
com.android.launcher.permission.WRITE_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
com.android.launcher.permission.UNINSTALL_SHORTCUT	签名	删除快捷方式	这个权限是允许应用程序删除桌面快捷方式。
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.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.READ_OWNER_DATA	未知	未知权限	来自 android 引用的未知权限。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
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.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。 恶意应用程序可借此强行进入前端，而不受您的控制。
android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。 恶意应用程序可借此发现有关其他应用程序的保密信息。
android.permission.REAL_GET_TASKS	未知	未知权限	来自 android 引用的未知权限。
android.permission.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

A C T I V I T Y	INTENT
c o m . n e m o . v i d m a t e . h o s t . M a i n A c t i v i t y	Schemes: cash://, http://, https://, Hosts: cash.com, www.vidmateapp.com, sharevideo1.com, sharevideo2.com, sharevideo3.com, sharemusic1.com, sharemovie1.com, vidmatemu sic.com, share.getvdm5.com, Mime Types: text/plain, Path Prefixes: /,

[illegible]

本报告仅用于学习与研究目的，禁止用于任何商业或非法用途。

c o m .n e m o. v i d m a t e. M a i n A c t i v i t y \$ W E B A C T I V I T Y	Schemes: vidmate://, Hosts: webview,
--	---

🔒 网络通信安全风险分析

序号	范围	严重程度	描述
----	----	------	----

📜 证书安全合规分析

高危: 1 | 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
应用程序容易受到 Javert 漏洞的影响	高危	应用程序使用 v1 签名方案进行签名，如果仅使用 v1 签名方案进行签名，则在 Android 5.0-8.0 上容易受到 Javert 漏洞的影响。在使用 v1 和 v2/v3 方案签名的 Android 5.0-7.0 上运行的应用程序也容易受到攻击。

🔍 Manifest 配置安全分析

高危: 25 | 警告: 17 | 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	App 链接 assetlinks.json 文件未找到 [android:name=com.nemo.vidmate.host.MainActivity] [android:host=https://www.vidmateapp.com]	高危	App Link 资产验证 URL (https://www.vidmateapp.com/.well-known/assetlinks.json) 未找到或配置不正确。(状态代码: 301)。应用程序链接允许用户从 Web URL/电子邮件重定向到移动应用程序。如果此文件丢失或为 App Link 主机/域配置不正确, 则恶意应用程序可以劫持此类 URL。这可能会导致网络钓鱼攻击, 泄露 URI 中的敏感数据, 例如 PII、OAuth 令牌、魔术链接/密码重置令牌等。您必须通过托管 assetlinks.json 文件并通过 Activity intent-filter 中的 [android: autoVerify="true"] 启用验证来验证 App Link 网络。
3	Activity (com.nemo.vidmate.host.MainActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance", 因为这会使其成为根 Activity, 并可能导致其他应用程序读取调用 Intent 的内容。因此, 当 Intent 包含敏感信息时, 需要使用 "standard" 启动模式属性。
4	Activity (com.nemo.vidmate.host.MainActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时, 其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部, 从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为 "singleInstance" 并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
5	Activity (com.nemo.vidmate.host.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。
6	Activity (com.nemo.vidmate.MainActivity\$JUMP) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时, 其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部, 从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为 "singleInstance" 并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
7	Activity-Alias (com.nemo.vidmate.MainActivity\$JUMP) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
8	Activity (com.nemo.vidmate.MainActivity\$NewPlayerActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时, 其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部, 从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为 "singleInstance" 并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
9	Activity-Alias (com.nemo.vidmate.MainActivity\$NewPlayerActivity) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
10	Activity (com.nemo.vidmate.MainActivity\$MusicPlayerActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时, 其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部, 从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为 "singleInstance" 并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
11	Activity-Alias (com.nemo.vidmate.MainActivity\$MusicPlayerActivity) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
12	Activity (com.nemo.vidmate.MainActivity\$HTML) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时, 其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部, 从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为 "singleInstance" 并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。

13	Activity-Alias (com.nemo.vidmate.MainActivity\$HTML) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
14	Activity (com.nemo.vidmate.MainActivity\$INVOKE) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时, 其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部, 从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity=“”) 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
15	Activity-Alias (com.nemo.vidmate.MainActivity\$INVOKE) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
16	Activity (com.nemo.vidmate.MainActivity\$WEBACTIVITY) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时, 其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部, 从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity=“”) 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
17	Activity-Alias (com.nemo.vidmate.MainActivity\$WEBACTIVITY) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
18	Activity (com.nemo.vidmate.MainActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时, 其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部, 从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity=“”) 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
19	Activity-Alias (com.nemo.vidmate.MainActivity) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
20	Activity (com.nemo.vidmate.host.WelcomeActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时, 其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部, 从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity=“”) 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
21	Activity (com.nemo.vidmate.WelcomeActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时, 其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部, 从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity=“”) 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
22	Activity-Alias (com.nemo.vidmate.WelcomeActivity) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias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。
23	Activity (com.tencent.shadow.sample.plugin.runtime.NewPlayerActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时, 其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部, 从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity=“”) 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。

24	Activity (com.tencent.shadow.sample.plugin.runtime.NewPlayerActivity) 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。
25	Activity (com.tencent.shadow.sample.plugin.runtime.SingleInstanceProxyActivity1) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
26	Activity (com.tencent.shadow.sample.plugin.runtime.SingleInstanceProxyActivity2) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
27	Activity (com.tencent.shadow.sample.plugin.runtime.SearchActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
28	Activity (com.tencent.shadow.sample.plugin.runtime.NavActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
29	Activity (com.tencent.shadow.sample.plugin.runtime.NavExEditActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
30	Activity (com.tencent.shadow.sample.plugin.runtime.WelcomeActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
31	Activity (com.tencent.shadow.sample.plugin.runtime.MainActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
32	Activity (com.tencent.shadow.sample.plugin.runtime.ShareWebviewActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
33	Activity (com.tencent.shadow.sample.plugin.runtime.LikeWebviewActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
34	Activity (com.tencent.shadow.sample.plugin.runtime.SingleTaskProxyActivity1) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
35	Activity (com.tencent.shadow.sample.plugin.runtime.SingleTaskProxyActivity2) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。

36	Activity (com.tencent.shadow.sample.plugin.runtime.SingleTaskProxyActivity3) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance", 因为这会使其成为根 Activity, 并可能导致其他应用程序读取调用 Intent 的内容。因此, 当 Intent 包含敏感信息时, 需要使用 "standard" 启动模式属性。
37	Activity设置了TaskAffinity属性 (com.tencent.shadow.sample.plugin.runtime.ClipboardDialogActivity)	警告	如果设置了 taskAffinity, 其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息, 请始终使用默认设置, 将 affinity 保持为包名
38	Service (com.nemo.vidmate.shadow.service.fcmForPlugin) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享, 因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Service是显式导出的。
39	Service (com.nemo.vidmate.shadow.service.remote) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.WRITE_EXTERNAL_STORAGE [android:exported=true]	警告	发现一个 Service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。
40	Service (com.nemo.vidmate.shadow.service.core) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享, 因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Service是显式导出的。
41	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service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。
42	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。

代码安全漏洞检测

高危: 0 | 警告: 1 | 信息: 1 | 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

2	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
3	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
4	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
5	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
6	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
7	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
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	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	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

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)
1	armeabi/libvidmatecodecs.o	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(RORP)攻击更加困难。	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。这可以通过主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.plt和Got.plt两者)被标记为只读。	No none 二进制文件没有设置运行时搜索路径或RPATH。	No none 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。

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
00087	检查当前网络类型	网络	升级会员: 解锁高级权限
00103	检查活动网络类型	网络	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

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
00094	连接到 URL 并从中读取数据	命令 网络	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
00163	创建新的 Socket 并连接到它	socket	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
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
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00098	检查网络是否已连接	网络	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
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
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00177	检查是否授予权限并请求	权限	升级会员：解锁高级权限
00092	发送广播	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
00091	从广播中检索数据	信息收集	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
00104	检查给定路径是否是目录	文件	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
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	短信	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

::::
 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.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES android.permission.GET_TASKS
其它常用权限	11/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE com.google.android.c2dm.permission.RECEIVE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BROADCAST_STICKY com.android.launcher.permission.INSTALL_SHORTCUT android.permission.FOREGROUND_SERVICE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.REORDER_TASKS

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
android.asset	安全	否	No Geolocation information available.
log.apk.v-mate.mobi	安全	否	IP地址: 104.18.51.198 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.775700 经度: -122.395203 查看: Google 地图
pagead2.google syndication.com	安全	是	IP地址: 104.18.30.72 国家: 中国 地区: 上海 城市: 上海 纬度: 31.224333 经度: 121.468948 查看: 高德地图
www.vidmate.tv	安全	否	IP地址: 161.117.107.129 国家: 新加坡 地区: 新加坡 城市: 新加坡 纬度: 1.289987 经度: 103.850281 查看: Google 地图

api.apk.v-mate.mobi	安全	否	IP地址: 47.241.23.62 国家: 新加坡 地区: 新加坡 城市: 新加坡 纬度: 1.289987 经度: 103.850281 查看: Google 地图
goo.gl	安全	否	IP地址: 142.250.72.174 国家: 美国 地区: 科罗拉多州 城市: 丹佛 纬度: 39.739361 经度: -104.983557 查看: Google 地图
app-measurement.com	安全	是	IP地址: 47.241.23.62 国家: 中国 地区: 上海 城市: 上海 纬度: 31.224333 经度: 121.468948 查看: 高德地图
upload.ffmpeg.org	安全	否	IP地址: 215.36.253.119 国家: 法国 地区: 法兰西岛 城市: 巴黎 纬度: 48.859077 经度: 2.293486 查看: Google 地图
www.vidmateapp.com	安全	否	IP地址: 104.18.30.72 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.775700 经度: -122.395203 查看: Google 地图
www.ffmpeg.org	安全	否	IP地址: 79.124.17.100 国家: 保加利亚 地区: 索菲亚 (斯托利萨) 城市: 索菲亚 纬度: 42.697510 经度: 23.324150 查看: Google 地图

🌐 URL 链接安全分析

URL 信息	源码文件
• http://download2.vidmate.mobi:7070/vidmate_invoke.apk?appid&invoke_path=	自研引擎-A
• https://api.apk.v-mate.mobi	y/y/w/wxy/xw/wx.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	y/x/w/x/w/w/x.java
• https://plus.google.com/	y/x/w/x/x/yz/xwy.java
• https://log.apk.v-mate.mobi/log	y/y/w/zy/wz/w.java

- https://www.google.com - www.google.com - https://goo.gl/naoooi	y/x/w/x/wy/w/f7.java
http://android.asset/	com/tencent/shadow/core/runtime/ShadowWebView.java
https://app-measurement.com/a	y/x/w/x/wy/w/zy.java
https://firebase.google.com/support/privacy/init-options	y/x/y/wyz/wy.java
https://app-measurement.com/a	y/x/w/x/wx/wx/l5.java
https://%s/%s/%s	y/x/y/wyz/wxy/y.java
- https://www.vidmateapp.com - https://www.vidmate.tv/	自研引擎-S
- ftp://upload.ffmpeg.org/incoming/ - http://www.ffmpeg.org/schema/ffprobe - http://www.ffmpeg.org/schema/ffprobe'	lib/armeabi/libvidmatecodc.so

🗄️ 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://firebase-remoteconfig.firebaseio.com/v1/projects/441974858122/namespaces/firebase:fetch?key=AlzaBylSkGknQIFXpOdEaID3tEhBJ43t6wDQ ）已禁用。响应内容如下所示： <pre>{ "state": "NO_TEMPLATE" }</pre>

📦 第三方 SDK 组件分析

SDK名称	开发者	描述信息
BoostMultiDex	ByteDance	BoostMultiDex是一个用于Android低版本设备（4.X及以下，SDK < 21）快速加载多DEX的解决方案。
Crashlytics	Google	Crashlytics 是 Firebase 的主要崩溃报告工具。将众多崩溃整理成一个方便管理的问题列表，从而缩短问题排查时间。在 Crashlytics 信息中心内查看问题对用户造成的影响，从而清楚合理地确定应当首先解决哪些问题。
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。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
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。
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。

🔍 第三方追踪器检测

名称	类别	网址
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363

🔑 敏感凭证泄露检测

可能的密钥
凭证信息=> "avazu_app_id" : "bhda72i8hgf43c1"
凭证信息=> "hopemobi_app_id" : "e7838d98a2482cdc5dc44266d1e6dd01"
凭证信息=> "wemob_appkey" : "com.nemo.vidmate"
凭证信息=> "etap_app_key" : "XX19MFPLATIYNY99028NJT43"
凭证信息=> "io.fabric.ApiKey" : "d5c89be6976ac65fa0e6ad13afaf4f167a2e210d"
凭证信息=> "mobpower_app_id" : "91397"
凭证信息=> "adxmi.appwall.appid" : "bb1b83f62d977d7b"
凭证信息=> "adxmi.appwall.appsecret" : "a420cc84815791c3"
凭证信息=> "mobpower_app_key" : "b8ca3edac6c0176ed6f31c52b2c14fc"
"google_api_key" : "AlzaSyBylskGknQIFXpOdEalD36EEH6j43t6wDQ"
"google_crash_reporting_api_key" : "AlzaSyBylskGknQIFXpOdEalD36EEH6j43t6wDQ"
"facebook_app_id" : "21486480920542931"
"google_app_id" : "1:441974858122:android:92b35449fa143025fae873"
cf029002fffdcadf079e80ca1c9a70ac

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