南明离火
移动应用检测平台

ANDROID 静态分析报告

Uptodown App Store · v6.89

分析日期: 2025-11-21 17:07:40

应用概览

文件名称:	Uptodown App Store v6.89.apk
文件大小:	12.05MB
应用名称:	Uptodown App Store
软件包名:	com.uptodown
主活动:	com.uptodown.activities.MainActivity
版本号:	6.89
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:	50/100 (中风险)
跟踪器检测:	5/432
杀软检测:	经检测，该文件安全
MD5:	b9091066302369e3f5abcdb6486dfddd
SHA1:	32acb5cdadf32cce2f115818ef917f7c454343dc
SHA256:	d9bd1f11c5351fa6e520918e94e58607a4fa0288000eedb81047e124dd0f8e8

分析结果严重性分布

高危	中危	信息	安全	关注
4	27	2	3	0

四大组件导出状态统计

Activity组件：64个，其中export的有： 4个
Service组件：15个，其中export的有： 2个
Receiver组件：18个，其中export的有： 9个
Provider组件：4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=ES, ST=Málaga, L=Málaga, O=Uptodown, OU=Uptodown, CN=Uptodown Technologies SL
签名算法: rsassa_pkcs1v15
有效期自: 2024-05-02 15:16:15+00:00
有效期至: 2051-09-18 15:16:15+00:00
发行人: C=ES, ST=Málaga, L=Málaga, O=Uptodown, OU=Uptodown, CN=Uptodown Technologies SL
序列号: 0x4976173c
哈希算法: sha256
证书MD5: ed86b3c7d53cba96769d1b431108e398
证书SHA1: 4b64559bc35829fd427bf65985ffdd9a88909fc4
证书SHA256: 822b9ca12b534ebcf426632221d951bfc60eb08f9f0cf2839c321b0685c2e8a4
证书SHA512:
45efe48cdaf6f380cb874193acd01d5469ef7fe38e338455817694b3c4d635c16228bd25bb02bb5a402888c35415f165d[illegible]94588c827709826397def703b2a9ab

公钥算法: rsa
密钥长度: 2048
指纹: 051d3f50665ccdf9ecda376f1c8051d410ef4312c7e745f16fb6d4d0ddebfbc9
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.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.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.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
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.GET_PACKAGE_SIZE	普通	测量应用程序空间大小	允许一个程序获取任何package占用空间容量。
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.USE_CREDENTIALS	危险	使用帐户的身份验证凭据	允许应用程序请求身份验证标记。
android.permission.AUTHENTICATE_ACCOUNTS	危险	作为帐户身份验证程序	允许应用程序使用 AccountManager 的帐户身份验证程序功能，包括创建帐户以及获取和设置其密码。
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加、删除帐户及删除其密码之类的操作。
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.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.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。

android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
android.permission.UPDATE_PACKAGES_WITHOUT_USER_ACTION	普通	允许更新包而不需要用户操作	允许应用程序通过 PackageInstaller.SessionParams.setRequireUserAction(int) 该用户操作指示应用程序更新不需要。
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.ENFORCE_UPDATE_OWNERSHIP	普通	表明意图通过 PackageInstaller 成为更新所有者。	允许应用程序通过 PackageInstaller.SessionParams.setRequestUpdateOwnership(boolean) 表明它有意成为更新所有者。
android.permission.INSTALL_PACKAGES	签名(系统)	请求安装APP	允许应用程序安装全新的或更新的 Android 包。恶意应用程序可能会借此添加其具有任意权限的新应用程序。
android.permission.DELETE_PACKAGES	签名(系统)	删除应用程序	允许应用程序删除 Android 包。恶意应用程序可借此删除重要的应用程序。
android.permission.ACCESS_SUPERUSER	危险	获取超级用户权限	有root的设备声明超级用户权限。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	允应用程序使用 Google 广告 ID，并且可能会投放广告。
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_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。
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.uptodown.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.uptodown.activities.MainActivity	Schemes: https://, utd://, market://, http://, content://, file://, *://, package://, Hosts: www.uptodown.com, market.android.com, play.google.com, dw.uptodown.com, *, Mime Types: */*, application/xapk-package-archive, application/vnd.xapk, application/*, application/apkm-package-archive, application/vnd.apkm, application/apks-package-archive, application/vnd.apks, application/vnd.android.package-archive, Path Prefixes: /preregister-available, /dwn, Path Patterns: .*.xapk, .*..*.xapk, .*..*..*.xapk, .*..*..*..*.xapk, .*..*..*..*..*.xapk, .*..*..*..*..*..*.xapk, .*..*..*..*..*..*..*.xapk, .*..*..*..*..*..*..*..*.xapk, .*..*..*..*..*..*..*..*..*.xapk, .*..*..*..*..*..*..*..*..*..*.xapk, .*.apkm, .*..*.apkm, .*..*..*.apkm, .*..*..*..*.apkm, .*..*..*..*..*.apkm, .*..*..*..*..*..*.apkm, .*..*..*..*..*..*..*.apkm, .*..*..*..*..*..*..*..*.apkm, .*..*..*..*..*..*..*..*..*.apkm, .*..*..*..*..*..*..*..*..*..*.apkm, .*..*..*..*..*..*..*..*..*..*..*.apkm, .*.apks, .*..*.apks, .*..*..*.apks, .*..*..*..*.apks, .*..*..*..*..*.apks, .*..*..*..*..*..*.apks, .*..*..*..*..*..*..*.apks, .*..*..*..*..*..*..*..*.apks, .*..*..*..*..*..*..*..*..*.apks, .*..*..*..*..*..*..*..*..*..*.apks, .*..*..*..*..*..*..*..*..*..*..*.apks,

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全分析

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: **2** | 警告: **17** | 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	App 链接 assetlinks.json 文件未找到 [android:name=com.uptodown.activities.MainActivity] [android:host=https://www.uptodown.com]	高危	App Link 资产验证 URL（https://www.uptodown.com/.well-known/assetlinks.json）未找到或配置不正确。（状态码：404）。应用程序链接允许用户通过 Web URL 或电子邮件直接跳转到移动应用。如果 assetlinks.json 文件缺失或主机/域配置错误，恶意应用可劫持此类 URL，导致网络钓鱼攻击，泄露 URI 中的敏感信息（如 PII、OAuth 令牌、魔术链接/重置令牌等）。请务必通过托管 assetlinks.json 文件并在 Activity 的 intent-filter 中设置 [android:autoVerify="true"] 来完成 App Link 域名验证。
3	App 链接 assetlinks.json 文件未找到 [android:name=com.uptodown.activities.MainActivity] [android:host=https://dw.uptodown.com]	高危	App Link 资产验证 URL（https://dw.uptodown.com/.well-known/assetlinks.json）未找到或配置不正确。（状态码：404）。应用程序链接允许用户通过 Web URL 或电子邮件直接跳转到移动应用。如果 assetlinks.json 文件缺失或主机/域配置错误，恶意应用可劫持此类 URL，导致网络钓鱼攻击，泄露 URI 中的敏感信息（如 PII、OAuth 令牌、魔术链接/重置令牌等）。请务必通过托管 assetlinks.json 文件并在 Activity 的 intent-filter 中设置 [android:autoVerify="true"] 来完成 App Link 域名验证。
4	Activity (com.uptodown.tv.ui.activity.TvMainActivity) 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。
5	Activity (com.uptodown.core.activities.InstallerActivity) 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.uptodown.activities.SearchActivity) 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	Broadcast Receiver (com.uptodown.receivers.BootDeviceReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。

本报告由南明离火移动安全分析平台生成

8	Broadcast Receiver (com.uptodown.receivers.MyAppUpdatedReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
9	Broadcast Receiver (com.uptodown.receivers.DownloadNotificationReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
10	Broadcast Receiver (com.uptodown.receivers.DownloadUpdateNotificationReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
11	Activity (com.inmobi.cmp.presentation.components.CmpActivity) 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。
12	Broadcast Receiver (org.matomo.sdk.extra.InstallReferrerReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
13	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。
14	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。
15	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [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。
16	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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。

17	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。
18	Broadcast Receiver (com.mbridge.msdk.foundation.same.broadcast.NetWorkChangeReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
19	高优先级 Intent（999） - {17} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

高危: **1** | 警告: **9** | 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	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	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
4	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用很可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
5	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

本报告由南明离火移动安全分析平台生成

6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	SHA-1是已知存在冲突的弱哈希	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

应用行为分析

编号	行为	标签	文件
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
00091	从广播中检索数据	信息收集	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
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
00023	从当前应用程序启动另一个应用程序	反射 控制	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
00036	从 res/raw 目录获取资源文件	反射	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
00085	获取ISO国家代码并将其放入JSON中	信息收集 电话服务	升级会员：解锁高级权限
00132	查询ISO国家代码	电话服务 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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00045	查询当前运行的应用程序名称	信息收集 反射	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
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
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00028	从assets目录中读取文件	文件	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
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
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
00121	创建目录	文件 命令	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
00153	通过 HTTP 发送二进制数据	http	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
00112	获取日历事件的日期	信息收集 日历	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	5/30	android.permission.GET_ACCOUNTS android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED android.permission.REQUEST_INSTALL_PACKAGES android.permission.RECORD_AUDIO
其它常用权限	10/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.AUTHENTICATE_ACCOUNTS android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_SUPERUSER com.google.android.c2dm.permission.RECEIVE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.FOREGROUND_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
firebase-settings.crashlytics.com	安全	是	**IP地址:** 220.181.174.162 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图

www.linkedin.com	安全	否	**IP地址:** 104.18.41.41 **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
whatwg.org	安全	否	**IP地址:** 165.227.248.76 **国家:** 美国 **地区:** 新泽西州 **城市:** 克利夫顿 **纬度:** 40.858585 **经度:** -74.163605 **查看:** Google 地图
app-measurement.com	安全	是	**IP地址:** 220.181.174.97 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
www.uptodown.app	安全	否	**IP地址:** 51.210.117.80 **国家:** 法国 **地区:** 上法兰西岛 **城市:** 鲁拜克斯 **纬度:** 50.693710 **经度:** 3.174439 **查看:** Google 地图
u.uptodown.app	安全	否	**IP地址:** 51.210.117.112 **国家:** 法国 **地区:** 上法兰西岛 **城市:** 鲁拜克斯 **纬度:** 50.693710 **经度:** 3.174439 **查看:** Google 地图
goo.gl	安全	否	**IP地址:** 142.250.179.142 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
pagead2.googlesyndication.com	安全	是	**IP地址:** 220.181.174.102 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
youtrack.jetbrains.com	安全	否	**IP地址:** 63.33.88.220 **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

kr.uptodown.com	安全	否	**IP地址:** 151.101.3.52 **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
google.com	安全	否	**IP地址:** 142.250.179.206 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
br.uptodown.com	安全	否	**IP地址:** 151.101.67.52 **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
cmp.inmobi.com	安全	否	**IP地址:** 79.86.240.21 **国家:** 奥地利 **地区:** Wien **城市:** 维也纳 **纬度:** 48.208889 **经度:** 16.372080 **查看:** Google 地图
ar.uptodown.com	安全	否	**IP地址:** 151.101.131.52 **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
jp.uptodown.com	安全	否	**IP地址:** 151.101.195.52 **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
t.uptodown.app	安全	否	**IP地址:** 51.210.117.80 **国家:** 法国 **地区:** 上法兰西岛 **城市:** 鲁拜克斯 **纬度:** 50.693710 **经度:** 3.174439 **查看:** Google 地图
it.uptodown.com	安全	否	**IP地址:** 151.101.67.52 **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

tr.uptodown.com	安全	否	**IP地址:** 151.101.195.52 **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
th.uptodown.com	安全	否	**IP地址:** 151.101.67.52 **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
id.uptodown.com	安全	否	**IP地址:** 151.101.131.52 **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
www.uptodown.com	安全	否	**IP地址:** 151.101.195.52 **国家:** 美国 **地区:** 美国加利福尼亚州 **城市:** 旧金山 **纬度:** 37.718128 **经度:** -122.4343849 **查看:** Google 地图
m.uptodown.net	安全	否	**IP地址:** 151.101.3.52 **国家:** 美国 **地区:** 美国加利福尼亚州 **城市:** 旧金山 **纬度:** 37.718128 **经度:** -122.4343849 **查看:** Google 地图
dw.uptodown.com	安全	否	**IP地址:** 51.210.117.80 **国家:** 法国 **地区:** 上法兰西岛 **城市:** 鲁拜克斯 **纬度:** 50.693710 **经度:** 3.174439 **查看:** Google 地图
secure.uptodown.com	安全	否	**IP地址:** 51.210.117.80 **国家:** 法国 **地区:** 上法兰西岛 **城市:** 鲁拜克斯 **纬度:** 50.693710 **经度:** 3.174439 **查看:** Google 地图
in.uptodown.com	安全	否	**IP地址:** 151.101.195.52 **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

support.uptodown.com	安全	否	**IP地址:** 216.198.54.6 **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
api.cmp.inmobi.com	安全	否	**IP地址:** 18.158.183.66 **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
vi.uptodown.com	安全	否	**IP地址:** 151.101.195.52 **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
www.virustotal.com	安全	否	**IP地址:** 34.54.88.138 **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
uptodown-android.uptodown.com	安全	否	**IP地址:** 151.101.195.52 **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
en.uptodown.com	安全	否	**IP地址:** 151.101.131.52 **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
de.uptodown.com	安全	否	**IP地址:** 151.101.131.52 **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
stripe.com	安全	否	**IP地址:** 54.76.53.164 **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

ro.uptodown.com	安全	否	**IP地址:** 151.101.195.52 **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
fr.uptodown.com	安全	否	**IP地址:** 151.101.67.52 **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
x.com	安全	否	**IP地址:** 104.244.42.227 **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
www.tiktok.com	安全	否	**IP地址:** 23.72.252.121 **国家:** 荷兰 (王国) **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
www.xxxyyyxxx.com	安全	否	No Geolocation information available.
ru.uptodown.com	安全	否	**IP地址:** 151.101.195.52 **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
cn.uptodown.com	安全	否	**IP地址:** 151.101.67.52 **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

URL 链接安全分析

URL信息	源码文件
• https://dw.uptodown.com/dwn/ • https://uptodown-android.uptodown.com/android	com/uptodown/activities/MainActivity.java
• https://secure.uptodown.com:443	l2/C1056a.java
• https://accounts.google.com/o/oauth2/revoke?token=	G/f.java

• https://secure.uptodown.com:443	l2/C2150a.java
• https://secure.uptodown.com • www.xxxyyyxxx.com	M2/C1090a.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	Y0/C2740x.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	Y0/C1393x.java
• https://secure.uptodown.com • www.xxxyyyxxx.com	M2/C2191a.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	G0/g.java
• https://play.google.com/store/apps/details?id=	com/mbridge/msdk/foundation/webview/a.java
• https://play.google.com/store/apps/details?id= • https://play.google.com/	com/mbridge/msdk/foundation/tools/aj.java
• file:////android_asset/mbridge_jscommon_authtext.html	com/mbridge/msdk/a.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	C/b.java
• https://play.google.com/store/apps/details?id= • https://play.google.com/	com/mbridge/msdk/click/c.java
• https://play.google.com/	com/mbridge/msdk/click/a.java
• https://play.google.com	com/mbridge/msdk/mbsignalcommon/windvane/WindVaneWebView.java
• javascript:window.mraidbridge.firereadyevent	com/mbridge/msdk/newreward/player/view/hybrid/util/MRAIDCommunicatorUtil.java
• https://www.virustotal.com/gui/file/	U2/C1262m.java
• https://m.uptodown.net/matomo.php	U2/z.java
• https://www.uptodown.com/turbo?platform=android • https://adservice.google.com/getconfig/pubvendors	U2/S.java
• https://play.google.com • http://play.google.com	U2/C2541p.java
• https://www.uptodown.com:443 • https://u.uptodown.app:443 • https://t.uptodown.app:443 • https://www.uptodown.app:443	U2/C1266q.java
• https://www.uptodown.com:443 • https://u.uptodown.app:443 • https://t.uptodown.app:443 • https://www.uptodown.app:443	U2/C2542q.java
• https://www.virustotal.com/gui/file/	U2/C2538m.java

• https://%s/%s/%s	U0/c.java
• javascript:window.navigator.vibrate	com/mbridge/msdk/click/m.java
• http://whatwg.org/html/common-microsyntaxes.html#space-character • http://whatwg.org/html/webappapis.html#dom-windowbase64-atob • http://whatwg.org/c#alphanumeric-ascii-characters • https://gist.github.com/atk/1020396 • http://whatwg.org/html/webappapis.html#dom-windowbase64-btoa	com/mbridge/msdk/c/b/b.java
• javascript:window.mraidbridge.firereadyevent	com/mbridge/msdk/mbsignalcommon/mraid/a.java
• https://cmp.inmobi.com/	X3/x.java
• https://cmp.inmobi.com/	X3/l.java
• https://cmp.inmobi.com/	X3/v.java
• file:////android_asset/mbridge_jscommon_authtext.html • https://goo.gl/naoooi • https://www.facebook.com/uptodown • https://de.uptodown.com • https://t.uptodown.app:443 • https://stripe.com/ • https://firebase.google.com/docs/analytics • https://vi.uptodown.com • https://%s/%s/%s • https://support.uptodown.com/hc/es/articles/360062090652 • https://cmp.inmobi.com/ • javascript:window.navigator.vibrate • https://fr.uptodown.com • https://api.cmp.inmobi.com/ • https://www.uptodown.com • https://app-measurement.com/s/d • https://en.uptodown.com/aboutus/services • https://cn.uptodown.com • https://ru.uptodown.com • https://www.instagram.com/uptodown/ • https://x.com/uptodown_es • https://support.uptodown.com/hc/en-us/articles/12536945642509 • https://adservice.google.com/getconfig/pubvendors • https://dw.uptodown.com/dwn/ • http://whatwg.org/html/webappapis.html#dom-windowbase64-atob • https://www.uptodown.com:443 • http://whatwg.org/c#alphanumeric-ascii-characters • https://it.uptodown.com • https://google.com/search? • https://tr.uptodown.com • https://www.uptodown.com/turbo?platform=android • https://kr.uptodown.com • https://www.tiktok.com/@uptodown_com • www.google.com • https://en.uptodown.com/developers-zone • https://en.uptodown.com/dmca • https://www.google.com • https://br.uptodown.com • https://th.uptodown.com • https://t.uptodown.app:443 • https://www.linkedin.com/company/uptodown/ • https://secure.uptodown.com:443 • https://id.uptodown.com • http://whatwg.org/html/webappapis.html#dom-windowbase64-btoa • https://youtrack.jetbrains.com/issue/kt-55980	自研引擎-S

本报告由南明离火移动安全分析平台生成

- https://www.virustotal.com/gui/file/
- https://ro.uptodown.com
- https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps
- https://in.uptodown.com
- https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin
- https://firebase.google.com/support/privacy/init-options
- https://en.uptodown.com/advertising
- https://en.uptodown.com/aboutus/privacy
- https://support.uptodown.com/hc/es
- https://play.google.com/store/apps/details?id=
- 127.0.0.1
- https://app-measurement.com/s
- javascript:window.mraidbridge.firereadyevent
- https://secure.uptodown.com
- http://play.google.com
- https://jp.uptodown.com
- www.xxxyyyxxx.com
- https://support.uptodown.com/hc/en-us
- https://play.google.com
- https://en.uptodown.com/aboutus/services#in-app-purchases
- http://www.uptodown.com
- https://play.google.com/
- https://ar.uptodown.com
- https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings
- https://m.uptodown.net/matomo.php
- https://support.uptodown.com/hc/es/articles/12536945642509
- https://app-measurement.com/a
- http://whatwg.org/html/common-microsyntaxes.html#space-character
- https://firebase.google.com/support/guides/disable-analytics
- https://en.uptodown.com
- https://www.uptodown.app:443
- https://accounts.google.com/o/oauth2/revoke?token=
- https://support.uptodown.com/hc/en-us/requests/new
- https://uptodown-android.uptodown.com/android
- https://gist.github.com/atk/1020396

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/171380306104/namespaces/firebase:fetch?key=AIzaSyBaooNElLxTgeKdljNdrXJQg5-mA_U1Lko ） 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
Jetpack DataStore	Google	Jetpack DataStore 是一种数据存储解决方案，允许您使用协议缓冲区存储键值对或类型化对象。Data Store 使用 Kotlin 协程和 Flow 以异步、一致的事务方式存储数据。
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。
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。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地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。
Picasso	Square	一个强大的 Android 图片下载缓存库。
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。
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).
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
Inmobi		https://reports.exodus-privacy.eu.org/trackers/106
Matomo (Piwik)	Analytics	https://reports.exodus-privacy.eu.org/trackers/138
Mintegral	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/200

敏感凭证泄露检测

可能的密钥
"com.google.firebase.crashlytics.mapping_file_id" : "c23a3151cf7b4976ace8682c2a7baf6f"
"dyStrategy.privateAddress" : "privateAddress"
"google_api_key" : "AIzaSyBaooNElLxTgeKdljNdrXJQg5-mA_U1Lko"
"google_app_id" : "1:171380306104:android:4e827fc7c388aeec79c44d"

"google_crash_reporting_api_key" : "AIzaSyBaooNElLxTgeKdljNdrXJQg5-mA_U1Lko"
"more_info_author" : "Author"
"username_edit_change" : "Change"
"more_info_author" : "Autor"
"recuperar_pass" : "Passwortwiederherstellung"
"more_info_author" : "Autor"
"more_info_author" : "Autor"
"username_edit_change" : "Cambiar"
"more_info_author" : "Pencipta"
"username_edit_change" : "Ubah"
"more_info_author" : "Autor"
"username_edit_change" : "Alterar"
"more_info_author" : "Auteur"
"username_edit_change" : "Changement"
"more_info_author" : "Yazar"
"more_info_author" : "Autore"
"username_edit_change" : "Cambia"
936dcbdd57fe235fd7cf61c2e93da3c4
LdxThdi1WBKUL75ULBPwJ7JgY7K0DkeAWrfXYN==
0000016742C00BDA259000000168CE0F13200000016588840DCE7[illegible]A0002FBF1C31C3275D78
h7KsLkfPW+xUhoPwJ7JgY7K0DkeAWrfXYN==
HkzwDFeD4QuyLdx5igfZYeu9xPM9NN==
7e5347690cfae30a3111fd31465c33f6
DFKwWgtuDkKwLZPwD+z8H+N/xj26VjcdX5KjVJCxVN=
470fa2b4ae8[illegible]cd56ecbcda973580343[illegible]e[illegible]91fa
eyJ2YWx1ZSI6IjRhOTRiN2I1MTk1NGVkNGMyMjZjZGM1MGMxZDE5Yjk2MTY4MzY5OTE1NCJ9
DFeuWkH0W+xUhoPwJ7JgY7K0DkeAWrfXYN==
LdxThdi1WBKUL75ULBPBD+QqJk2MWrfXYN==
DFKwWgtuDkKwLZPwD+z8H+N/xj26Vjcdx5KanjKnxVN=
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
h7KsLkfPW+xUhoPBD+QqJk2MWrfXYN==

DFK/HrQgJ+zQW+xUhoPwJ7JgY7K0DkeAWrfXYN==
Y7c14Z2TDbv/Y+xgHFeXDrcshBPUYFT=
DFKwWgtuDkKwLZPwD+z8H+N/xjQZxVfV+T2SZVe6V2xS5c5n
92762936dcbdd57fe235fd7cf61c2e93da3c4
DkP3hrKuHoPMH+zwL+fALkK/WQc5x5zH+TcincKNNVfWNVJcVM==
DkPtYdQTLkfAW+xUhoPwJ7JgY7K0DkeAWrfXYN==
DFK/HrQgJ+zQW+xUhoPBD+QqJk2MWrfXYN==
DFKwWgtuDkKwLZPwD+z8H+N/xjK+n3eyNVx6ZVPn5jcincKZx5f5ncN=
822b9ca12b534ebcf426632221d951bfc60eb08f9f0cf2839c321b0685c2e8a4

免责声明及风险提示:

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。