南明离火
移动应用检测平台

ANDROID 静态分析报告

推特 • v1.4.6

分析日期: 2025-05-15 16:39:26

应用概览

文件名称:	mdxqs39_1.4.6_35212575.apk
文件大小:	25.9MB
应用名称:	推特
软件包名:	com.aqndtuijks.tawitpterem.d1744735099024003819
主活动:	com.grass.mh.SplashActivity
版本号:	1.4.6
最小SDK:	22
目标SDK:	29
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	44/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：安全
MD5:	abe3374b72cdc7c524427ff29237b5cc
SHA1:	cd8121e87e406b7a2207057711a50b638858e9f8
SHA256:	01565aa36eed7bd37e0e7105f280474cce2c187909845607c54d517474b6c9

分析结果严重性分布

高危	中危	信息	安全	关注
4	18	2	1	6

四大组件导出状态统计

Activity组件：141个，其中export的有： 7个
Service组件：1个，其中export的有： 0个
Receiver组件：0个，其中export的有： 0个
Provider组件：8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=24, ST=24, L=24, O=24, OU=24, CN=24
签名算法: rsassa_pkcs1v15
有效期自: 2023-09-20 04:14:56+00:00
有效期至: 2048-09-13 04:14:56+00:00
发行人: C=24, ST=24, L=24, O=24, OU=24, CN=24
序列号: 0x76493202
哈希算法: sha256
证书MD5: 755a66bef973bda5e1db233945a21da4
证书SHA1: d719116903aec8e0b37523c7e8173320f17c11b3
证书SHA256: 1ebc59b7bd7e78e2a7fcc9000bbcab413365b503569e24dac4e346a5d56d65bb
证书SHA512:
19b24068f10980065d57dbd4d50893bf03a32433fcdd2e53f69fe677ead6ed99c8e2711f185df574c25bcac6b8e7a6a6e14a73710925fd0e077c6d10e678bc56

公钥算法: rsa
密钥长度: 2048
指纹: 9245899c2dec72fee3f9ee0cc4cfed244a217a2f2ddb845cefaf1ab6abb27ccb
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.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.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.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.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）
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_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_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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
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.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。

网络通信安全风险分析

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

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

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=@xml/network_security_config]	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。
3	Activity-Alias (com.grass.mh.FiveActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity-Alias 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity-Alias 被显式导出，存在安全风险。
4	Activity-Alias (com.grass.mh.FourActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity-Alias 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity-Alias 被显式导出，存在安全风险。
5	Activity-Alias (com.grass.mh.ThreeActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity-Alias 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity-Alias 被显式导出，存在安全风险。
6	Activity-Alias (com.grass.mh.TwoActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity-Alias 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity-Alias 被显式导出，存在安全风险。
7	Activity-Alias (com.grass.mh.OneActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity-Alias 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity-Alias 被显式导出，存在安全风险。
8	Activity-Alias (com.grass.mh.Default) 未受保护。 存在 intent-filter。	警告	检测到 Activity-Alias 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity-Alias 被显式导出，存在安全风险。
9	Activity (com.grass.mh.ui.mine.activity.LoginActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。

代码安全漏洞检测

高危: **3** | 警告: **8** | 信息: **2** | 安全: **1** | 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	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
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	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
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
6	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
7	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

本报告由南明离火移动安全分析平台生成

8	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
9	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序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
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	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
12	此应用程序使用SQL Cipher。SQLCipher为sqlite数据库文件提供256位AES加密	警告	OWASP MASVS: MSTG-CRYPTO-1	升级会员：解锁高级权限
13	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
14	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

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	arm64-v8a/libglide-webp.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得到。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/librtmp-jni.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

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
00013	读取文件并将其放入流中	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
00054	从文件安装其他APK	反射	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
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
00012	读取数据并放入缓冲流	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
00016	获取设备的位置信息并将其放入 JSON 对象	位置 信息收集	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

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
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
00121	创建目录	文件 命令	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
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
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
00075	获取设备的位置	信息收集 位置	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
00072	将 HTTP 输入流写入文件	命令 网络 文件	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
00029	动态初始化类对象	反射	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

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.REQUEST_INSTALL_PACKAGES android.permission.CAMERA android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE android.permission.SYSTEM_ALERT_WINDOW
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.ACCESS_WIFI_STATE

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
exoplayer.dev	安全	是	**IP地址:** 221.228.32.13 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图
d2pugxkmpwkrrb.cloudfront.net	安全	否	**IP地址:** 52.85.39.177 **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
dashif.org	安全	是	**IP地址:** 221.228.32.13 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图
tt.pisemx.xyz	安全	是	**IP地址:** 221.228.32.13 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图
tt.kjbiin.xyz	安全	是	**IP地址:** 221.228.32.13 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图
d3aczu6m[illegible]i77p.cloudfront.net	安全	否	**IP地址:** 52.85.39.177 **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
tt.un7zbn.xyz	安全	是	**IP地址:** 221.228.32.13 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图

data.flurry.com	安全	否	No Geolocation information available.
clsp.fun	安全	是	**IP地址:** 221.228.32.13 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• 127.0.0.1	e/p/a/e/b.java
• https://tt.kjbiin.xyz • https://d2pugxkmpwkrrb.cloudfront.net/tt.json • https://tt.un7zbn.xyz • https://tt.pisemx.xyz • https://d3aczu6m41i77p.cloudfront.net/tt.json	com/grass/mh/SplashActivity.java
• https://data.flurry.com/v1/flr.do	e/f/b/t0.java
• http://dashif.org/guidelines/last-segment-number	e/g/a/a/h1/j0/j/c.java
• https://exoplayer.dev/issues/player-accessed-on-wrong-thread	e/g/a/a/t0.java
• http://%s:%d/%s • 127.0.0.1	com/danikula/videocache/HttpProxyCacheServer.java
• http://%s:%d/%s	com/danikula/videocache/Pinger.java
• https://data.flurry.com/aap.do	e/f/b/s0.java
• https://clsp.fun	com/grass/mh/databinding/ActivityShareLayoutBindingImpl.java

第三方 SDK 组件分析

SDK名称	开发者	描述信息
GlideWebpDecoder	zjupure	GlideWebpDecoder 是一个 Glide 集成库，用于在 Android 平台上解码和显示 webp 图像。它基于 libwebp 项目，并以 Fresco 和 GlideWebpSupport 的一些实现作为参考。
IJKPlayer	b[illegible]	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
RenderScript	Android	RenderScript 是用于在 Android 上以高性能运行计算密集型任务的框架。RenderScript 主要用于数据并行计算，不过串行工作负载也可以从中受益。RenderScript 运行时可在设备上提供的多个处理器（如多核 CPU 和 GPU）间并行调度工作。这样您就能够专注于表达算法而不是调度工作。RenderScript 对于执行图像处理、计算摄影或计算机视觉的应用来说尤其有用。
AgentWeb	Justson	AgentWeb 是一个基于的 Android WebView ， 极度容易使用以及功能强大的库，提供了 Android WebView 一系列的问题解决方案 ， 并且轻量和极度灵活。

PictureSelector	LuckSiege	一款针对 Android 平台下的图片选择器，支持从相册获取图片、视频、音频 & 拍照，支持裁剪(单图 or 多图裁剪)、压缩、主题自定义配置等功能，支持动态获取权限&适配 Android 5.0+ 系统的开源图片选择框架。
XPopup	li-xiaojun	内置几种了常用的弹窗，十几种良好的动画，将弹窗和动画的自定义设计的极其简单。
Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

第三方追踪器检测

名称	类别	网址
Flurry	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/25

敏感凭证泄露检测

可能的密钥
友盟统计的=> "UMENG_CHANNEL" : "mdxqs39"
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

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。