南明离火
移动应用检测平台

ANDROID 静态分析报告

24Six • v66.1.24

分析日期: 2025-08-29 16:18:39

应用概览

文件名称:	24Six v66.1.24.apk
文件大小:	25.37MB
应用名称:	24Six
软件包名:	app.tfs.prod
主活动:	app.tfs.activity.ActivityStartup
版本号:	66.1.24
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:	58/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	dac02cf07e96c3b4feeff29080c89a54
SHA1:	3bef17cf404ffc78063e81237aedcb358bd716ad
SHA256:	c0361053bc2b6e06e2882c3b532ba68a97b72fac7bcf3fc43a54d8f385303a46

分析结果严重性分布

高危	中危	信息	安全	关注
0	14	2	2	0

四大组件导出状态统计

Activity组件：7个，其中export的有： 1个
Service组件：12个，其中export的有： 2个
Receiver组件：12个，其中export的有： 3个
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: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2022-09-20 19:31:50+00:00
有效期至: 2052-09-20 19:31:50+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x6eae403c18a55d0cb2079e73c80be4416226e66c
哈希算法: sha256
证书MD5: 742c4828e48f75ee3bf95fc3f68acdfd
证书SHA1: 9e76614716972d8303f03dc7d0c69db2711d6a9a
证书SHA256: bac989dcd40d08d4c314f74f8c4dc9b8d25d5c3e26feb0cd9cadbdaaee68bf63
证书SHA512:
060e157e6eae71f20c65b1f376746053c108a3f2c57fac9d0ea918587aa3ae2271c9967dcc9820131ba023b634457d842a5c5a857c79616731731eae6b7b8ed8

公钥算法: rsa
密钥长度: 4096
指纹: c6a083c9016e876355233bbcf8f4e8ce1ca954d25752486cdec4f2974a3ed02f
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.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.FOREGROUND_SERVICE_MEDIA_PLAYBACK	普通	启用用于媒体播放的前台服务	允许常规应用程序使用类型为“mediaPlayback”的 Service.startForeground。
android.permission.POST_NOTIFICATIONS	危险	允许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.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.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.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
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.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.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。

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。
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。
app.tfs.prod.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
app.tfs.activity.ActivityMain	Schemes: https://, Hosts: 2ysi.app, Path Prefixes: /preview, /app,

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: **7** | 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	Activity (app.tfs.activity.ActivityMain) 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。

3	Service (app.tfs.media.AppMediaService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
4	Broadcast Receiver (androidx.media3.session.MediaButtonReceiver) 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。
5	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。
6	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。
7	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: **0** | 警告: **5** | 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,不得包含敏感信息	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

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	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
5	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
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	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	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

应用行为分析

编号	行为	标签	文件
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
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
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
00130	获取当前WIFI信息	WiFi 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

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	2/30	android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	7/46	android.permission.FOREGROUND_SERVICE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.INTERNET 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
24six.app	安全	否	**IP**地址: 172.67.72.61 **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://24six.app/cdn/artists/2bd286081a/dpr=2
- https://24six.app/cdn/artists/b77bd1433a/public
- https://videodelivery.net/eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IjZkMmVjN2MyMGE4MzAyMWE0YmVlNGRjZTE0NmEzMDVmIn0.eyJzdWIiOiJhN2QzYzU2Y2RlNjRhMTg1OGY3YWEwNGQzYzRjYjU0OSIsImtpZCI6IjZkMmVjN2MyMGE4MzAyMWE0YmVlNGRjZTE0NmEzMDVmIn0.ClhtM_zzwEJzonG6A8npyB45uw-fgjgjTFCdiyUDV5gSDVcInopZ-GNwq2ZUmMamSZ7Q4GZNV53OtaT59ONqrSawx3WuNgXc0cJjuLvnjl1nJZHf0e4QDmBVNK2TaamEdBiMBaHMCMZ2DpFCgfgyemmt2hdsOd-ZN3rx1MGOpIz8E6ca9WYshC6E8C40pAj4aFVPqGsrmZJ3z-DRyoCYki-C_-5JaUIDd-qmHvrBXWU7V8VO8vycciJcpFKY7K2xjZ9yEE7bfQjzbmNT0xXEMr7ILhn611XJO1mT74gfQciuLVQq07kTaTOHuWYOPVM-poNzmlonodeVNiwU_kr4Kw/thumbnails/thumbnail.jpg?fit=fill
- https://videodelivery.net/eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IjZkMmVjN2MyMGE4MzAyMWE0YmVlNGRjZTE0NmEzMDVmIn0.eyJzdWIiOiJiZGZmNjI0MmFjYWM5ODAwOWUwOWFjNjRhYTlmODlmMSIsImtpZCI6IjZkMmVjN2MyMGE4MzAyMWE0YmVlNGRjZTE0NmEzMDVmIn0.Z1V5qfHrDEm_4Fm5SH-HLb_SxHejECTxlAMq3f1yA-vl6iK_7DV-XISu5sPq27BvaQ_46f5_pyyF25NXITbEmv-skxzoP72QU-6vNJodvi19REVLbgmxwTXAZlR8S9VVsdFdKfKYDH9PcEPX7ZQWp9D87dnBE8gUIt1l7yCtIiTdn70bzBwY9bKUCQX6Y5iFL-i3z7o3_xeXSc6lpJlBMGXvNCOzF5_z8zR22i-yrCvkTauvgslKKsuaLOzQ4EFut8XPhcVF7s1VS4If0lmimEpR8fQxY8VU6k8el-Fsz9IrKpDik-cBCn6fOzulCgfUKH-tH8mWrc8IfrE1suMe7w/thumbnails/thumbnail.jpg?fit=fill
- https://videodelivery.net/eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IjZkMmVjN2MyMGE4MzAyMWE0YmVlNGRjZTE0NmEzMDVmIn0.eyJzdWIiOiJmN2VmNTZlZjNkMmNiNTA4MDRlOGI2M[illegible]3MzllMGYxOSIsImtpZCI6IjZkMmVjN2MyMGE4MzAyMWE0YmVlNGRjZTE0NmEzMDVmIn0.Grpfbx[illegible]9avlVpgjOHckVMAwbnzHnKuuuhYEm7pnUlR2yYTH6GkJK6EAZ7m8JqYeOo69UlgGyRMu[illegible]uk GJaTwtF-KYHutK2LR2juU-KKTBTyx6RcVybFlwpEL5TG6NVXcObIwMlAcPn37pPhNZ2aKCfk[illegible]v3oDgT7qzqGhYg0so3cB8hvC0E18jf9qvbPU4DeKHSswPkqMk82vSzr1Aprwe5FqBeLB[illegible]-K3c7[illegible]XOxe03gSGE2qKM9MgVzZqTQ09Tq09biJmT0GjQJpQtnUCs_1Q5qsK5KJ4o1XcdVyCF0Ral[illegible]l0Vxt1bgLN0H5Y5hv-lYr8A/thumbnails/thumbnail.jpg?fit=fill
- https://24six.app/cdn/collections/26d78775ff/public
- https://24six.app/cdn/collections/151a61bf26/public
- https://24six.app/cdn/stories/7ce04bf145/large
- https://videodelivery.net/eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IjZkMmVjN2MyMGE4MzAyMWE0YmVlNGRjZTE0NmEzMDVmIn0.eyJzdWIiOiI4Y2R[illegible]0ZDUxY2NiZTAxMG[illegible]wNjc4NmM4NCIsImtpZCI6IjZkMmVjN2MyMGE4MzAyMWE0YmVlNGRjZTE0NmEzMDVmIn0.fIjY[illegible]03QwyPm8simbMlM52o5O-l6lXqxYktbDkYCR2jyRiHM9S2prJtj[illegible]xI5EIXCtlLQhYGXlP[illegible]UXErEgWiXrC-ptR8oN-BfTHLAX31yoFohuRKvSqSPkjc-iIVBa[illegible]tzqP[illegible]CajXWlT8-8H3bq4O[illegible]Vr72cfP8LAydrsDGqqszBgdakreQoh1KwnXxo5vvDHeia5[illegible]WOxnHof4R7-Ub[illegible]BnIoTOHrusET_tfDGoVTWNzssQwq6A5ms47oTpFk0TVrnP[illegible]SmT8hC01djuhj3h[illegible]PCd9jJftFiRZmfLu6meELITDg/thumbnails/thumbnail.jpg?fit=fill
- https://videodelivery.net/eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IjZkMmVjN2MyMGE4MzAyMWE0YmVlNGRjZTE0NmEzMDVmIn0.eyJzdWIiOiIyZDA0[illegible]QyMGI3ZjI5ZDNlYWMwMjAwMjJkOTNhYyIsImtpZCI6IjZkMmVjN2MyMGE4MzAyMWE0YmVlNGRjZTE0NmEzMDVmIn0.hcL9hNJxFLOdw2a2I-BdkDRpAvlR06ssA[illegible]OCq3YhHYs2hls9[illegible]VVPhDTjR7s4Jyxoblu76-RwXSuYDUWuWZNu3jZHtLDim0xVyL8jZh[illegible]RMfC5kuLVXVMus3[illegible]EpIdZyLLop3nuYeyub13feu41sd7CWUiMNsD2CO8k52ecJ9ip[illegible]TUKMTqIuCYpKtM[illegible]hbL[illegible]qHDdCtnfGeyVqsy6aERRWCzbgnFsud0qDNnKI_qkxi41yo-z[illegible]N8dNISTymwS1S0Q[illegible]VsWivGCXGX8kARSFS2qOhXzQgjxfLTCBDnO9T14S1IQo[illegible]/thumbnails/thumbnail.jpg?fit=fill

自研引擎-A

• https://24six.app/api/v3/story/ • https://24six.app/api/v3/clip/ • https://24six.app/api/v3/content/	app/tfs/media/TfsMediaSource.java
• https://24six.app/	r/C1571t.java
• https://24six.app/app/	r/l0.java
• https://24six.app/	s/e.java

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/339171818983/namespaces/firebase:fetch?key=AIzaSyDtyCPZ5MAPdM_IWTbYDQxCYE9GIuHS7Fs ）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
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。
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

敏感凭证泄露检测

可能的密钥
"com.google.firebase.crashlytics.mapping_file_id" : "95bfa0e15d6f48aaab1ab8d2d538a05c"
"google_api_key" : "AIzaSyDtyCPZ5MAPdM_IwTbYDQxCYE9GIuHS7Fs"
"google_app_id" : "1:339171818983:android:b1f82392af46d07adc9142"
"google_crash_reporting_api_key" : "AIzaSyDtyCPZ5MAPdM_IwTbYDQxCYE9GIuHS7Fs"
"password" : "Password"

Google Play 应用市场信息

标题: 24Six

评分: 4.16 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 娱乐 **Play Store URL:** app.tfs.prod

开发者信息: 24Six, 24Six, None, https://24six.app/, info@24six.app

发布日期: 2022年11月18日 **隐私政策:** Privacy link

关于此应用:

是否曾希望您的音乐符合您的价值观？ 欢迎使用 24Six，您的音乐、您的播客、您的视频.....都在一个令人难以置信的可控应用程序中。 — 你不必一直说“不” — 您不必担心内容不当 — 您不必在家人的娱乐活动上妥协 最后，您可以根据自己的标准享受您选择的娱乐活动。 在 24Six 应用程序上，您可以：— 新：离线音乐流媒体！ 下载您喜欢的歌曲并在没有互联网连接的情况下收听它们 — 仅访问预先审查的内容 — 为每个家庭成员定制过滤器 — 创建您自己的播放列表（或为您喜爱的播放列表） — 在音乐、视频和播客之间切换 — 并返回 — 访问您最喜欢的艺术家的独家 24Six 原创内容 简而言之：您可以根据自己的标准享受娱乐，并使用让您掌控一切的尖端技术。

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。