



ANDROID 静态分析报告



Android 24 • v1.0.1

本报告由南明离火移动安全分析平台生成

分析日期: 2025-04-05 13:18:22

i应用概览

文件名称:	????24 v1.0.1.apk
文件大小:	7.31MB
应用名称:	????24
软件包名:	ft3rnw0.fm66dj7wctupl
主活动:	not_found_main_activity!!
版本号:	1.0.1
最小SDK:	26
目标SDK:	32
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	52/100 (中风险)
杀软检测:	22 个杀毒软件报毒
MD5:	55b92326cb5ff84745a3fc737b0c28fb
SHA1:	2feb19e23b7ed56937a077d1efaf70aca2f305b0
SHA256:	07a27dc8e85df937767863e00e2157a900950645f83092894876164e7a2fccad

分析结果严重性

高危	中危	信息	安全	关注
1	3	0	1	0

四大组件信息

Activity组件: 1个, 其中export的有: 1个
Service组件: 4个, 其中export的有: 1个
Receiver组件: 9个, 其中export的有: 2个
Provider组件: 1个, 其中export的有: 0个

证书信息

二进制文件已签名

v1 签名: False
 v2 签名: True
 v3 签名: False
 v4 签名: False
 主题: C=tV, ST=oZHj, L=s4fVt, O=a2sHa8.sVrl, OU=rqV.h9y3ob, CN=hr2zxcgYTkfq05l
 签名算法: rsassa_pkcs1v15
 有效期自: 2024-02-23 06:14:47+00:00
 有效期至: 2051-07-11 06:14:47+00:00
 发行人: C=tV, ST=oZHj, L=s4fVt, O=a2sHa8.sVrl, OU=rqV.h9y3ob, CN=hr2zxcgYTkfq05l
 序列号: 0x3cf9943
 哈希算法: sha256
 证书MD5: c08cc43ce8d12d67b958255007900c81
 证书SHA1: bbfed9e48f7f04aa436131c3e86e41cf9c28dfdf
 证书SHA256: 896d754c3c929f15fb7ef1b9230ed304946b2a6003f521ed18d998216775f660
 证书SHA512: 0ef3f9db2bfe78247c0bf268c3394a14edbed3e51f835ded63c057f83419ea11a1196312c9be0b15a96fd60f5fb479a2df1e8ef13c52af4b0cb20624aa5a81b
 公钥算法: rsa
 密钥长度: 2048
 指纹: 225646aef448317f7e4447c4cf5d95f7754c7c2c922b4dbc04e663ae002ee7f5
 找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
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.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.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息, 给您带来费用。
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.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集, 但对即时应用程序公开。
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.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或SIM卡中存储的短信。恶意应用程序可借此读取您的机密信息。
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.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.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.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。恶意程序会在用户未知的情况下监视或删除。

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.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.READ_PRIVILEGED_PHONE_STATE	签名(系统)	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.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人(地址)数据。恶意应用程序可借此将您的数据发送给其他人。

🔒 网络通信安全

序号	范围	严重级别	描述
----	----	------	----

📄 证书安全分析

高危: 0 | 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

🔍 MANIFEST分析

高危: 1 | 警告: 7 | 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	应用程序具有网络安全配置 [android:networkSecurityConfig=@7F120002]	信息	网络安全配置功能让应用程序可以在一个安全的、声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
3	程序可被任意调试 [android:debuggable=true]	高危	应用可调试标签被开启，这使得逆向工程师更容易将调试器挂接到应用程序上。这允许导出堆栈跟踪和访问调试助手类。
4	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。

5	Broadcast Receiver (com.tenxuncc.commsgapp.receiver.MsgReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BROADCAST_SMS [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。
6	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [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。
7	Activity (com.tenxuncc.commsgapp.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。
8	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。
9	高优先级的Intent (2147483647) - {1} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级, 应用程序有效地覆盖了其他请求。

</> 安全漏洞检测

序号	问题	等级	参考标准	文件位置
----	----	----	------	------

::: 敏感权限分析

类型	匹配	权限
恶意软件常用权限	9/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.SEND_SMS android.permission.READ_PHONE_STATE android.permission.READ_SMS android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.RECEIVE_SMS android.permission.GET_ACCOUNTS android.permission.READ_CONTACTS

其它常用权限	6/46	android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.FOREGROUND_SERVICE android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE
--------	------	--

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。

第三方SDK

SDK名称	开发者	描述信息
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。

密钥凭证

可能的密钥
BRYRLAwtcxEAPjAJCj0RMhcvEj4kA3lyHQawcyUEdjYFPQI3DQMvMgJ1KGoALp3AAKMEyYtMD0PhJzCCA
FyowcgwtKzELEHNwJS8kcBc9BSgNAysyJQYOfwo9LCsXLzA
CAYSNwsGETEmBCBqCj0rLAh1fzMILXMBDzASagETEis

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成