



ANDROID 静态分析报告



◆ TinyPic • v12.03.005

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2025-04-14 02:09:03

i应用概览

文件名称:	base.apk
文件大小:	29.16MB
应用名称:	TinyPic
软件包名:	qju.roqhltx386809.edtrfytguy
主活动:	com.rnapp.MainActivity
版本号:	12.08.005
最小SDK:	21
目标SDK:	31
加固信息:	未加壳
开发框架:	React Native
应用程序安全分数:	52/100 (中风险)
杀软检测:	AI评估: 可能有安全隐患
MD5:	fc588e4cedc058e063e18505e52078e6
SHA1:	7ce5e8a60757fad97c61012de6c19716b0cb42b4
SHA256:	07347be5521f99fce629c1cb1952cfee099a36809c5151d43bad898d70db7f4e

分析结果严重性

高危	中等	信息	安全	关注
1	5	1	1	0

四大组件信息

Activity组件: 2个, 其中export的有: 0个
Service组件: 0个, 其中export的有: 0个
Receiver组件: 0个, 其中export的有: 0个
Provider组件: 2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: None
 主题: C=ddwqoqheikfgf, ST=wepcfsrhyuzrq, L=jotbzupvihzbx, O=dpo1743412769399, OU=lle1743412769399, CN=TG@apken888
 签名算法: rsassa_pkcs1v15
 有效期自: 2025-03-31 09:19:29+00:00
 有效期至: 2075-03-19 09:19:29+00:00
 发行人: C=ddwqoqheikfgf, ST=wepcfsrhyuzrq, L=jotbzupvihzbx, O=dpo1743412769399, OU=lle1743412769399, CN=TG@apken888
 序列号: 0x425502d9
 哈希算法: sha1
 证书MD5: 9de8bd4c29202e406c295718321cd02c
 证书SHA1: 3ed2dd82f4907c01e708df7adae5739248848342
 证书SHA256: 28fc5b4947a25bcd268490a45eb26317e6e9e6b0bf6ecd89a29ce88452972de8
 证书SHA512: f4c67c47af30ad22267b9a46834ba4c74c683feaf27fb726eef528be0de6395f8b3c7caabea754c74d694cb96f60e156376a07940020c757ed33e7babe1d3c65

公钥算法: rsa
 密钥长度: 1024
 指纹: bfd54dcd441989d7d815a09d84d99e21009c3a7737cfa74402c2a69953c9fbd9
 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.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.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/写入/删除外部存储内容	允许应用程序写入外部存储。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
android.permission.READ_PROFILE	危险	读取用户资料	允许应用程序读取用户个人信息。
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。
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_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.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.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.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
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.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。

qju.roqhltx386809.edtrfytguy_com.google.android.c2dm.permission.RECEIVE	未知	未知权限	来自 android 引用的未知权限。
qju.roqhltx386809.edtrfytguy_com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	未知权限	来自 android 引用的未知权限。

🔒 网络通信安全

高危: 0 | 警告: 0 | 信息: 0 | 安全: 0

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: 0 | 警告: 2 | 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, 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=@xml/network_security_config]	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	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。

</> 安全漏洞检测

高危: 1 | 警告: 3 | 信息: 1 | 安全: 0 | 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	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
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	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	应用程序创建临时文件。敏感信息永远不应该被写入临时文件	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

动态库分析

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/libfb.so	<p>True info</p> <p>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。</p>	<p>动态共享对象(DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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。</p>	True info
2	arm64-v8a/libfbjni.so	<p>True info</p> <p>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。</p>	<p>动态共享对象(DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>True info</p> <p>二进制文件有以下加固函数: ['_strlen_chk']</p>	True info

3	arm64-v8a/libglog.so	<p>True info</p> <p>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。</p>	<p>动态共享对象(DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>True info</p> <p>二进制文件有以下加固函数: ['_memcpy_chk', '_strncat_chk', '_vsnprintf_chk', '_strlen_chk']</p>	True info
4	arm64-v8a/libjsi.so	<p>True info</p> <p>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。</p>	<p>动态共享对象(DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>True info</p> <p>二进制文件有以下加固函数: ['_strlen_chk']</p>	True info

5	arm64-v8a/libreactperfloggerjni.so	<p>True info</p> <p>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。</p>	<p>动态共享对象(DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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</p>	True info
6	arm64-v8a/librcc_image.so	<p>True info</p> <p>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。</p>	<p>动态共享对象(DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	None	None	<p>False warning</p> <p>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</p>	True info

7	arm64-v8a/librcc_root.so	<p>True info</p> <p>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。</p>	<p>动态共享对象(DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	<p>Non info</p> <p>二进制文件没有设置运行时搜索路径或RPATH</p>	<p>Non info</p> <p>二进制文件没有设置RPATH</p>	<p>False warning</p> <p>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</p>	<p>True info</p> <p>符号被剥离</p>
8	arm64-v8a/librcc_scrollview.so	<p>True info</p> <p>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。</p>	<p>动态共享对象(DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	<p>Non info</p> <p>二进制文件没有设置运行时搜索路径或RPATH</p>	<p>Non info</p> <p>二进制文件没有设置RPATH</p>	<p>False warning</p> <p>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</p>	<p>True info</p> <p>符号被剥离</p>

9	arm64-v8a/librcc_text.so	<p>True info</p> <p>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。</p>	<p>动态共享对象(DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	<p>Non info</p> <p>二进制文件没有设置运行时搜索路径或RPATH</p>	<p>Non info</p> <p>二进制文件没有设置RUNPATH</p>	<p>False warning</p> <p>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</p>	<p>True info</p> <p>符号被剥离</p>
10	arm64-v8a/librcc_textinput.so	<p>True info</p> <p>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。</p>	<p>动态共享对象(DSO) info</p> <p>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。</p>	<p>True info</p> <p>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</p>	<p>Full RELRO info</p> <p>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。</p>	<p>Non info</p> <p>二进制文件没有设置运行时搜索路径或RPATH</p>	<p>Non info</p> <p>二进制文件没有设置RUNPATH</p>	<p>False warning</p> <p>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</p>	<p>True info</p> <p>符号被剥离</p>

1 1	arm64-v8a/librcc_unimplementedview.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。	Non info 二进制文件没有设置运行时搜索路径或RPATH	Non info 二进制文件没有设置RPATH	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
1 2	arm64-v8a/librcc_view.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。	Non info 二进制文件没有设置运行时搜索路径或RPATH	Non info 二进制文件没有设置RPATH	True info 二进制文件有以下加固函数:['_vsnprintf_chk']	True info 符号被剥离

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
00189	获取短信内容	短信	升级会员: 解锁高级权限
00188	获取短信地址	短信	升级会员: 解锁高级权限

00200	从联系人列表中查询数据	信息收集 联系人	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
00201	从通话记录中查询数据	信息收集 通话记录	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
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
00024	Base64解码后写入文件	反射 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
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
00001	初始化位图对象并将数据 (例如JPEG) 压缩为位图对象	相机	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
00191	获取短信收件箱中的消息	短信	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
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	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
00038	查询电话号码	信息收集	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
00134	获取当前WiFi IP地址	WiFi 信息收集	升级会员: 解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	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
00192	获取短信收件箱中的消息	短信	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

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
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
00043	计算WiFi信号强度	信息收集 WiFi	升级会员: 解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	8/30	android.permission.WRITE_CONTACTS android.permission.READ_CONTACTS android.permission.GET_ACCOUNTS android.permission.READ_SMS android.permission.READ_PHONE_STATE android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.VIBRATE
其它常用权限	5/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_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。

URL链接分析

URL信息	源码文件
<ul style="list-style-type: none"> https://clients3.google.com/generate_204 https://redux.js.org/?from_code= https://upload-250.qiniup.com https://ah.1205chitfgdl.pro https://awsapp-aa13.ap-northeast-1.amazonaws.com https://registry.npmjs.org/react-native/-/react-native-0.69.2.tgz https://github.com/callstack/react-native-slider https://react-native-async-storage.github.io/async-storage/docs/advanced/jestnlf 	自研引擎-A
<ul style="list-style-type: none"> https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067 	com/swmansion/rnscreens/ScreenStackFragment.java
<ul style="list-style-type: none"> https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067 	com/swmansion/rnscreens/ScreenFragment.java
<ul style="list-style-type: none"> file:lib 	lib/arm64-v8a/libglog.so

第三方SDK

SDK名称	开发者	描述信息
Fresco	Facebook	Fresco 是一个用于管理图像及其使用的内存的 Android 库。
C++ 共享库	Android	在 Android 应用中运行原生代码。
React Native	Facebook	React Native 使你只使用 JavaScript 也能编写原生移动应用。它在设计原理上和 React 一致，通过声明式的组件机制来搭建丰富多彩的用户界面。
Facebook SDK	Facebook	Facebook SDK是适用于 Android 的将 Facebook集成到 Android 应用程序中的最简单方法。
Folly	Facebook	An open-source C++ library developed and used at Facebook.
glog	Google	glog 是一个 C++ 日志库，它提供 C++ 流式风格的 API。
Yoga	Facebook	Yoga 意在打造一个跨 iOS、Android、Windows 平台在内的布局引擎，兼容 Flexbox 布局方式，让界面布局更加简单。
React Native App Utils	Stumble App	一个简单的 React-Native Utils 库，具有随机有用的功能。主要用于后台服务任务，例如通知 onReceive 事件。
React Native Reanimated	software-mansion	Reanimated is a React Native library that allows for creating smooth animations and interactions that run on the UI thread.
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 and 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 允许您定义共享单一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。

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