



ANDROID 静态分析报告



Scene • v8.2.0

分析日期: 2025-04-03 01:55:21

i应用概览

文件名称:	Scene v8.2.0.apk
文件大小:	8.19MB
应用名称:	Scene
软件包名:	com.omarea.vtools
主活动:	com.omarea.vtools.activities.ActivityPowerModeTile
版本号:	8.2.0
最小SDK:	23
目标SDK:	30
加固信息:	未加壳
开发框架:	Xposed
应用程序安全分数:	48/100 (中风险)
杀软检测:	3 个杀毒软件报毒
MD5:	21ccd0415cbe97884e4c3ba6afa0526e
SHA1:	d97b68677a301d7a74f68a9272f74c4df826cd3
SHA256:	09fdeb2eb3e16f954061c926e247d90a6646f49df60979acf12c735235f55155

分析结果严重性分布

高危	中危	信息	安全	关注
2	6	3	1	4

四大组件导出状态统计

Activity组件: 46个, 其中export的有: 10个
Service组件: 6个, 其中export的有: 3个
Receiver组件: 4个, 其中export的有: 2个
Provider组件: 3个, 其中export的有: 1个

应用签名证书信息

二进制文件已签名

v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfef6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccb6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
找到 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.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.RECEIVE_USER_PRESENT	普通	允许程序唤醒机器	允许应用可以接收点亮屏幕或解锁广播。
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.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.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.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	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.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.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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.REQUEST_COMPANION_RUN_IN_BACKGROUND	普通	允许配套应用程序在后台运行	允许配套应用在后台运行。
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.BIND_NOTIFICATION_LISTENER_SERVICE	签名	NotificationListenerService 需要用于系统绑定	必须是NotificationListenerService，以确保只有系统可以绑定到。
android.permission.WRITE_SECURE_SETTINGS	签名(系统)	修改安全系统设置	允许应用程序修改系统的安全设置数据。普通应用程序不能使用此权限。
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.CHANGE_CONFIGURATION	危险	改变UI设置	允许应用程序 允许应用程序更改当前配置，例如语言区域或整体的字体大小。
android.permission.BIND_ACCESSIBILITY_SERVICE	签名	AccessibilityServices 需要进行系统绑定	必须由 AccessibilityService要求，以确保只有系统可以绑定到它。
android.permission.GET_APP_OPS_STATS	未知	未知权限	来自 android 引用的未知权限。
android.permission.INTERACT_ACROSS_USERS	未知	未知权限	来自 android 引用的未知权限。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
com.android.launcher.permission.UNINSTALL_SHORTCUT	签名	删除快捷方式	这个权限是允许应用程序删除桌面快捷方式。

🔒 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	应用程序使用代码签名证书进行签名

🔍 Manifest 配置安全分析

高危: 0 | 警告: 18 | 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=@7F150000]	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。
4	Content Provider (com.omarea.vtools.SceneFreezeProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
5	Activity (com.omarea.vtools.activities.ActivityAppXposedDetails) 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。
6	Broadcast Receiver (com.omarea.scene_mode.ReceiveSceneMode) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。
7	Activity (com.omarea.vtools.activities.ActivityStartSplash) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
8	Activity (com.omarea.vtools.activities.ActivityMain) 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。
9	Activity (com.omarea.vtools.activities.ActivityAppDetails) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
10	Activity (com.omarea.vtools.activities.ActivityFileSelector) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
11	Activity (com.omarea.vtools.activities.ActivityQuitStart) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
12	Activity (com.omarea.vtools.activities.ActivityFreezeApps) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。

13	Activity (com.omarea.vtools.activities.ActionPage) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
14	Activity (com.omarea.vtools.activities.ActionPageOnline) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
15	Activity (com.omarea.vtools.activities.ActivityAutoClick) 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。
16	Broadcast Receiver (com.omarea.scene_mode.ReceiveShortcut) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。
17	Service (com.omarea.vtools.AccessibilitySceneMode) 受权限保护,但是应该检查权限的保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	警告	发现一个 Service被共享给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。
18	Service (com.omarea.scene_mode.NotificationListenerService) 受权限保护,但是应该检查权限的保护级别。 Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [android:exported=true]	警告	发现一个 Service被共享给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。
19	Service (com.omarea.scene_mode.SceneTileService) 受权限保护,但是应该检查权限的保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [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。

代码安全漏洞检测

高危: 2 | 警告: 7 | 信息: 3 | 安全: 0 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	应用没有记录日志信息,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	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
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	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
5	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
6	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
7	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
8	应用程序可以写入应用程序目录。敏感信息应加密	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
9	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
10	应用程序使用非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

11	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
12	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	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-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/libnative-lib.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。	No ne info 二进制文件没有设置运行时搜索路径或RPATH	No ne 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
00013	读取文件并将其放入流中	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
00035	查询已安装的包列表	反对	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
00192	获取短信收件箱中的消息	短信	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
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
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
00104	检查给定路径是否是目录	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
00161	对可访问性节点信息执行可访问性服务操作	无障碍服务	升级会员：解锁高级权限
00173	获取AccessibilityNodeInfo屏幕中的边界并执行操作	无障碍服务	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
00163	创建新的Socket并连接到它	socket	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
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00079	隐藏当前应用程序的图标	规避	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
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
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
00028	从assets目录中读取文件	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

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.SYSTEM_ALERT_WINDOW android.permission.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.WRITE_SETTINGS
其它常用权限	7/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS com.android.launcher.permission.INSTALL_SHORTCUT

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
source.android.com	安全	否	IP地址: 142.250.188.238 国家: 美国 地区: 加利福尼亚 城市: 山景城 纬度: 37.405991 经度: -122.078514 查看: Google 地图

vtools.omarea.com	安全	是	IP地址: 43.160.193.93 国家: 中国 地区: 广东 城市: 广州 纬度: 23.127361 经度: 113.264572 查看: 高德地图
www.paypal.me	安全	否	IP地址: 151.101.65.21 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.775700 经度: -122.395203 查看: Google 地图
fa.hsfaka.net	安全	是	IP地址: 18.123.202.88 国家: 中国 地区: 四川 城市: 成都 纬度: 30.666670 经度: 104.066269 查看: 高德地图
tinyurl.com	安全	否	IP地址: 104.11.112.233 国家: 美国 地区: 加利福尼亚 城市: 旧金山 纬度: 37.775700 经度: -122.395203 查看: Google 地图
magisk-modules-repo.github.io	安全	否	IP地址: 151.101.65.21 国家: 美国 地区: 宾夕法尼亚 城市: 加利福尼亚 纬度: 40.065647 经度: -79.891724 查看: Google 地图
scene7.omarea.com	安全	是	IP地址: 43.160.193.93 国家: 中国 地区: 广东 城市: 广州 纬度: 23.127361 经度: 113.264572 查看: 高德地图
vtools.onlife	安全	是	IP地址: 119.91.234.23 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
download.omarea.com	安全	否	IP地址: 43.160.193.93 国家: 新加坡 地区: 新加坡 城市: 新加坡 纬度: 1.289987 经度: 103.850281 查看: Google 地图

URL 链接安全分析

URL信息	源码文件
https://play.google.com/store/apps/details?id=	com/omarea/vtools/dialogs/i4.java
https://github.com/helloklf/vtools/blob/scene3/docs/miui%e6%b8%a9%e6%8e%a7%e8%af%b4%e6%98%8e.md	com/omarea/vtools/activities/ActivityMiuiThermal.java
- https://www.paypal.me/duduski - https://vtools.oss-cn-beijing.aliyuncs.com/	com/omarea/vtools/dialogs/DialogPaymentMethods.java
http://vtools.omarea.com/scene-policy.html	com/omarea/vtools/activities/ActivityOtherSettings.java
- https://play.google.com/store/apps/details?id= - https://pd.qq.com/s/92rqbetny	com/omarea/vtools/fragments/FragmentLogin.java
http://vtools.omarea.com/scene-policy.html	com/omarea/vtools/activities/ActivityStartSplash.java
http://vtools.omarea.com/	com/omarea/vtools/fragments/e0.java
https://github.com/yinwanxi/uperf-game-turbo/releases	com/omarea/vtools/fragments/v0.java
- http://vtools.online - http://scene7.omarea.com:8080	com/omarea/net/SceneServer.java
https://github.com/yc9559/uperf	com/omarea/vtools/fragments/u0.java
http://download.omarea.com/toolkit/	com/omarea/net/ScenePerf.java
https://github.com/shadow3aaa/fas-rs/releases/	com/omarea/vtools/fragments/w0.java
file:/android_asset/	com/omarea/krscript/model/NodeInfoBase.java
https://vtools.oss-cn-beijing.aliyuncs.com/vtools	com/omarea/net/k.java
http://vtools.omarea.com/	com/omarea/vtools/fragments/x.java
- http://127.0.0.1: 127.0.0.1	com/omarea/common/net/Daemon.java
http://vtools.oss-cn-beijing.aliyuncs.com/app-release	com/omarea/net/l.java
https://vtools.oss-cn-beijing.aliyuncs.com/vtoolsddin/auto-skip-config-v1.json	com/omarea/net/AutoSkipCloudData\$updateConfig\$1.java
https://magisk-modules-repo.github.io/submission/modules.json	com/omarea/library/basic/MagiskModuleRepo.java
http://vtools.omarea.com/#/email	com/omarea/vtools/dialogs/f3.java
http://vtools.omarea.com/	com/omarea/vtools/activities/ActivityAppXposedDetails.java
https://fa.hsfaka.net/orderquery	com/omarea/vtools/dialogs/x2.java
https://fa.hsfaka.net/orderquery	com/omarea/vtools/dialogs/w2.java

- https://source.android.com/devices/tech/dalvik/jit-compiler?hl=zh-cn - http://vtools.omarea.com/ - https://tinyurl.com/y3j7vszf - https://vtools.oss-cn-beijing.aliyuncs.com/addin/swap-controller-3.6.4.zip	自研引擎-S
--	--------

✉ 邮箱地址敏感信息提取

EMAIL	源码文件
helloklf@outlook.com	com/omarea/vtools/dialogs/g3.java
helloklf@outlook.com	com/omarea/net/SceneMagisk.java
helloklf@outlook.com	com/omarea/vtools/fragments/x1.java
helloklf@outlook.com 1191634433@qq.com	com/omarea/vtools/dialogs/c4.java

🔑 敏感凭证泄露检测

可能的密钥
"app_user" : "User"
"user_pwd_input" : "password"
"dialog_addin_wlan_pwd" : "Password:"
"source_author" : "Source/Author:"
"REQUEST_PASSWORD_COMPLEXITY" : "REQUEST_PASSWORD_COMPLEXITY"
FNt6SyjNPzndLXNgAzGpmXEPI4T4haU1
34ea0e93b18c7df94decd663857bb3bf

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