



ANDROID 静态分析报告



Android • v6.2.71

分析日期: 2025-04-26 08:04:48

i应用概览

文件名称:	□□□□ v6.2.71.apk
文件大小:	14.21MB
应用名称:	□□□□
软件包名:	com.dsbttoh96mrc4pgttcqfijlco8bvqjwl23wh.s3pl3ulo
主活动:	com.dsbttoh96mrc4pgttcqfijlco8bvqjwl23wh.s3pl3ulo.my.phone.ui.main.KeyPadActivity
版本号:	6.2.71
最小SDK:	23
目标SDK:	29
加固信息:	自定义加固
开发框架:	Java/Kotlin
应用程序安全分数:	56/100 (中风险)
杀软检测:	21 个杀毒软件报毒
MD5:	e826e7ac4635c584221cc87de96270b8
SHA1:	432212f674b080de17c7d367128601417630d921
SHA256:	f4c7ee99fceed5904b9d2b66dc360a0c9b910dfe1ceaa7b14285a14dd86513d0

分析结果严重性

🚨 高危	⚠️ 中危	i 信息	✓ 安全	🔍 关注
0	1	0	1	0

四大组件信息

Activity组件: 12个, 其中export的有: 2个
Service组件: 12个, 其中export的有: 2个
Receiver组件: 2个, 其中export的有: 1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: True

v2 签名: True
v3 签名: False
v4 签名: False
主题: C=h0, ST=mLXe, L=kxDHx, O=jxdMJT.tkpb, OU=lZz.fcmO7c, CN=cD6HitC4SIz7YX
签名算法: rsassa_pkcs1v15
有效期自: 2023-05-14 07:14:53+00:00
有效期至: 2050-09-29 07:14:53+00:00
发行人: C=h0, ST=mLXe, L=kxDHx, O=jxdMJT.tkpb, OU=lZz.fcmO7c, CN=cD6HitC4SIz7YX
序列号: 0x35087000
哈希算法: sha256
证书MD5: 0bf81ba49da5480e638cf0cd906a298e
证书SHA1: a81f9ad0650a25af164adf8cdfcd510c4711b76f
证书SHA256: 4360e619ae7fe3b4d1d7a0eb322332f009f4b9059c68d161e19e85a15519a846
证书SHA512:
7a3f0fb5f9357688b076e871df56acccb03e17e9b31b499d1d4f041709a9516dee49a9de6d0b9ef19f540f3116ad65c16d13d657b40706caa50a45d68d9c99b0

公钥算法: rsa
密钥长度: 2048
指纹: 93ea4cd78e49fd5f55607a80b78f505f5ec01e3e944b73c491a2438d97c493bc
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.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。恶意应用程序可能借此将您的数据发送给其他人。
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.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.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.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_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
android.permission.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.ARTIFACTMANAGE_OVERLAY_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
android.permission.ANSWER_PHONE_CALLS	危险	允许应用程序接听来电	一个用于以编程方式应答来电的运行时权限。
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.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。

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.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.PROCESS_OUTGOING_CALLS	危险	拦截外拨电话	允许应用程序处理外拨电话或更改要拨打的号码。恶意应用程序可能会借此监视、另行转接甚至阻止外拨电话。
android.permission.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。
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.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.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
android.permission.RECEIVE_LAUNCH_BROADCASTS	未知	未知权限	来自 android 引用的未知权限。
android.permission.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
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.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.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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
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.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.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_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.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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。

可浏览的Activity组件

ACTIVITY	INTENT
com.dsbtoh96mrc4pgttcqfijlco8bvqjwl23wh.s3pl3ulo.my.phone.ui.calling.PhoneCallActivity	Scheme: tel://,

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: 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分析

高危: 0 | 警告: 9 | 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=@7F141002]	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	Activity设置了TaskAffinity属性 (com.dsbtoh96mrc4pgttcqfijlco8bvqjwl23wh.s3pl3ulo.my.phone.ui.calling.PhoneCallActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名

5	Activity (com.dsbtoh96mrc4pgttcqfijlco8bvqjwl23wh.s3pl3ulo.my.phone.ui.calling.PhoneCallActivity) 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	Activity (com.dsbtoh96mrc4pgttcqfijlco8bvqjwl23wh.s3pl3ulo.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。
7	Service (com.dsbtoh96mrc4pgttcqfijlco8bvqjwl23wh.s3pl3ulo.services.AccessServ) 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。
8	Service (com.dsbtoh96mrc4pgttcqfijlco8bvqjwl23wh.s3pl3ulo.NotificationReceiver Service) 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	Broadcast Receiver (com.dsbtoh96mrc4pgttcqfijlco8bvqjwl23wh.s3pl3ulo.cast.CallMyListener) 受权限保护,但是应该检查权限的保护级别。 Permission: android.permission.RECEIVE_BOOT_COMPLETED [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。
10	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	18/30	android.permission.READ_CONTACTS android.permission.ACCESS_FINE_LOCATION android.permission.READ_CALL_LOG android.permission.WAKE_LOCK android.permission.CALL_PHONE android.permission.CAMERA android.permission.PROCESS_OUTGOING_CALLS android.permission.READ_PHONE_STATE android.permission.SYSTEM_ALERT_WINDOW android.permission.MODIFY_AUDIO_SETTINGS android.permission.WRITE_CALL_LOG android.permission.READ_SMS android.permission.RECEIVE_SMS android.permission.ACCESS_COARSE_LOCATION android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.WRITE_CONTACTS android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	11/46	android.permission.BLUETOOTH android.permission.INTERNET android.permission.ACCESS_BACKGROUND_LOCATION android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.BLUETOOTH_ADMIN android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_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。

第三方SDK

SDK名称	开发者	描述信息
Sentry	Sentry	Sentry 是一个实时事件日志记录和聚合平台，它专门用于监视错误和提取执行适当的事后操作所需的所有信息。

密钥凭证

可能的密钥
QmBvb251VwJob2UhbGBqZEVkeURkGk3VylWxkdWluZQ
YG9lc25oZS9gcXEvQGJ1aHdodXhvdXNkYGU

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。

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