南明离火
移动应用检测平台

ANDROID 静态分析报告

• v6.7.5

分析日期: 2024-07-31 17:15:39

应用概览

文件名称:	bbe4e2d3d34235debeca33b0d9204141cbb73e4ffc3f3bac45fbd2d7d10efc2d.apk
文件大小:	8.73MB
应用名称:	
软件包名:	com.x2ttgcsgyasmnuwnzsa646t4enwmcfkjiuszgvezystl6r9newtoluuygx1i.ripzhk
主活动:	com.x2ttgcsgyasmnuwnzsa646t4enwmcfkjiuszgvezystl6r9newtoluuygx1i.ripzhk.my.phone.ui.main.KeyPadActivity
版本号:	6.7.3
最小SDK:	23
目标SDK:	29
加固信息:	深盾安全(Virbox) 加固
应用程序安全分数:	52/100 (中风险)
杀软检测:	19 个杀毒软件报毒
MD5:	0361f9c601cc48c330b93174ae801984
SHA1:	09938e923a7dc134f5b02dd119a019c84976751a
SHA256:	bbe4e2d3d34235debeca33b0d9204141cbb73e4ffc3f3bac45fbd2d7d10efc2d

分析结果严重性分布

高危	中危	信息	安全	关注
1	7	1	1	0

四大组件导出状态统计

Activity组件：12个，其中export的有：2个
Service组件：11个，其中export的有：1个
Receiver组件：1个，其中export的有： 0个
Provider组件：2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=lO, ST=p0qE, L=r1vUo, O=jdJsXF.nV0r, OU=gLZ.snrHV3, CN=jUF9SrXQ6dKiJ8
签名算法: rsassa_pkcs1v15
有效期自: 2024-06-30 01:38:49+00:00
有效期至: 2051-11-16 01:38:49+00:00
发行人: C=lO, ST=p0qE, L=r1vUo, O=jdJsXF.nV0r, OU=gLZ.snrHV3, CN=jUF9SrXQ6dKiJ8
序列号: 0x3c820af7
哈希算法: sha256
证书MD5: 7f3c0e58c0968a22d40d8a04d0c94a22
证书SHA1: 021b916349667577467a453a769a1822c0b6377d
证书SHA256: d5245ced327cb32a5be3b98c38af8516de3d7bda7d13f717efac6055ed0c616f
证书SHA512:
cdceddcd99fdbc55a57873ac77981b1153cf3fbc0926f6a4a0b150588fb1486d37123a66256a297087cb8103b9e712887817150404600c073d3d76fd6a59b085

公钥算法: rsa
密钥长度: 2048
指纹: 73bd69aab3a04223c0bd0691b0e0ee81d43ea5e443a9e59f400a46931c1f88ba
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.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.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.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错略的经纬度信息，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.ACTION_MANAGE_OVERLAY_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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.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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
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.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.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.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.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.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.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.READ_CONTACTS	危险	读取联系人信息	允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.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_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.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.RECEIVE_LAUNCH_BROADCASTS	未知	未知权限	来自 android 引用的未知权限。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.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.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.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.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.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.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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.x2ttgcsgyasmnuwnzsa646t4enwmcfkjiuszgvezystl6r9newtoluuygx1i.ripzhk.my.phone.ui.calling.PhoneCallActivity	Schemes: tel://,

网络通信安全风险分析

高危: **1** | 警告: **0** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

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	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 6.0-6.0.1, [minSdk=23]	信息	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	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。
3	应用程序具有网络安全配置 [android:networkSecurityConfig=@0x7F140002]	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。
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	Activity (com.x2ttgcsgyasmnuwnzsa646t4enwmcfkjiuszgvezystl6r9newtoluuygx1i.ripzhk.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。

6	Service (com.x2ttgcsgyasmnuwnzsa646t4enwmcfkjiuszgvezystl6r9newtoluuygx1i.ripzhk.NotificationReServ) 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。
7	Activity设置了TaskAffinity属性 (com.x2ttgcsgyasmnuwnzsa646t4enwmcfkjiuszgvezystl6r9newtoluuygx1i.ripzhk.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
8	Activity (com.x2ttgcsgyasmnuwnzsa646t4enwmcfkjiuszgvezystl6r9newtoluuygx1i.ripzhk.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。
9	Content Provider (com.x2ttgcsgyasmnuwnzsa646t4enwmcfkjiuszgvezystl6r9newtoluuygx1i.ripzhk.db.PackageContentProvider) 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。

代码安全漏洞检测

高危: **0** | 警告: **0** | 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

敏感权限滥用分析

类型	匹配	权限

恶意软件常用权限	18/30	android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.CALL_PHONE android.permission.CAMERA android.permission.MODIFY_AUDIO_SETTINGS android.permission.PROCESS_OUTGOING_CALLS android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_CALL_LOG android.permission.READ_CONTACTS android.permission.READ_PHONE_STATE android.permission.READ_SMS android.permission.RECEIVE_BOOT_COMPLETED android.permission.RECEIVE_SMS android.permission.RECORD_AUDIO android.permission.WAKE_LOCK android.permission.WRITE_CALL_LOG android.permission.WRITE_CONTACTS android.permission.VIBRATE
其它常用权限	11/46	android.permission.ACCESS_BACKGROUND_LOCATION android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.CHANGE_WIFI_STATE android.permission.FOREGROUND_SERVICE android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 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。

免责声明及风险提示: