南明离火
移动应用检测平台

ANDROID 静态分析报告

Smart Notify • v6.3.866

分析日期: 2025-05-16 17:24:36

应用概览

文件名称:	Smart Notify v6.3.866.apk
文件大小:	1.6MB
应用名称:	Smart Notify
软件包名:	com.kuma.smartnotify
主活动:	com.kuma.smartnotify.SmartNotifyMain
版本号:	6.3.866
最小SDK:	26
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	47/100 (中风险)
杀软检测:	1 个杀毒软件报毒
MD5:	d5e5b29093df31689dcdc3c05ac46e89
SHA1:	c20e605e7121852b71cf9aa97c6a0f23f4e89f42
SHA256:	b5a713739a46970a13781500bbecc51282b9d1a7be828959d7ba2937b92e734

分析结果严重性分布

高危	中危	信息	安全	关注
3	3	2	1	0

四大组件导出状态统计

Activity组件：22个，其中export的有： 14个
Service组件：5个，其中export的有： 3个
Receiver组件：8个，其中export的有： 9个
Provider组件：1个，其中export的有： 0个

应用签名证书信息

APK已签名

v1 签名: False
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=IN
签名算法: rsassa_pkcs1v15
有效期自: 2020-11-01 10:49:08+00:00
有效期至: 2045-10-26 10:49:08+00:00
发行人: C=IN
序列号: 0x47723c30
哈希算法: sha1
证书MD5: 0ea9ea7bd967b60eff29ab7746d8bfbc
证书SHA1: 2412f88ac73778c3d659d47a3112e27898f953b9
证书SHA256: 3b61c2a82aff9f7652ffe0b04be3c8f248b5e1aa7063f1a3846f0cf5c778628a
证书SHA512:
1c077d27a069939e563a8e959aeb767231a94eb6f2a9e7cbc1538f095956000586ffab52ab2a9908447e54bfbfb8995f035eecc243c99f16d1ce9160d275fa2

公钥算法: rsa
密钥长度: 1024
指纹: 74b4db306b8cd921cbfac0e876ef0a9a8574cb987da1221aa430bd56dc1d83df
共检测到 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.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.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.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
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.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入手机或 SIM 卡中存储的短信。恶意应用程序可借此删除您的信息。
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.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.RECEIVE_WAP_PUSH	危险	接收WAP	允许应用程序接收和处理 WAP 信息。恶意应用程序可借此监视您的信息，或者将信息删除而不向您显示。
android.permission.RECEIVE_MMS	危险	接收彩信	允许应用程序接收和处理彩信。恶意应用程序可借此监视您的信息，或者将信息删除而不向您显示。
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.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.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.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.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_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.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.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.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.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_CALENDAR	危险	添加或修改日历活动以及向邀请对象发送电子邮件	允许应用程序添加或更改日历中的活动，这可能会向邀请对象发送电子邮件。恶意应用程序可能会借此清除或修改您的日历活动，或者向邀请对象发送电子邮件。
android.permission.READ_CALENDAR	危险	读取日历活动	允许应用程序读取您手机上存储的所有日历活动。恶意应用程序可借此将您的日历活动发送给其他人。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.hardware.sensor.proximity	未知	未知权限	来自 android 引用的未知权限。
android.permission.MODIFY_PHONE_STATE	签名(系统)	修改手机状态	允许应用程序控制设备的电话功能。拥有此权限的应用程序可自行切换网络、打开和关闭无线通信等，而不会通知您。
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.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。
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。
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.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.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.FOREGROUND_SERVICE_SPECIAL_USE	普通	启用特殊用途的前台服务	允许常规应用程序使用类型为“specialUse”的 Service.startForeground。

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.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.kuma.smartnotify.SmartNotifyMain	Schemes: tel://,
com.kuma.smartnotify.SmartNotifySMS	Schemes: sms://, smsto://, Mime Types: text/plain,

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: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用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: **28** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
2	Activity (com.kuma.smartnotify.CallActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
3	Activity (com.kuma.smartnotify.SmartNotifyPermissions) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
4	Activity (com.kuma.smartnotify.SmartNotifyMessages) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

5	Activity (com.kuma.smartnotify.SmartNotifyDialer) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
6	Service (com.kuma.smartnotify.NLService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
7	Service (com.kuma.smartnotify.dialer.services.CallService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_INCALL_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
8	Activity (com.kuma.smartnotify.SmartNotifyNumberDetail) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
9	Activity (com.kuma.smartnotify.SMSorCallDialog) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
10	Activity (com.kuma.smartnotify.SmartNotifyDateTimePicker) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
11	Activity (com.kuma.smartnotify.SmartNotifyNote) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
12	Activity (com.kuma.smartnotify.AddNumber) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
13	Activity (com.kuma.smartnotify.Preferences) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
14	Activity (com.kuma.smartnotify.TextActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
15	Activity (com.kuma.smartnotify.SmartNotifyPopup) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

16	Broadcast Receiver (com.kuma.smartnotify.smsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BROADCAST_SMS [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
17	Broadcast Receiver (com.kuma.smartnotify.mmsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BROADCAST_WAP_PUSH [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
18	Service (com.kuma.smartnotify.HeadlessSmsSendService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.SEND_RESPOND_VIA_MESSAGE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
19	Activity (com.kuma.smartnotify.ContactPicker) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
20	Activity (com.kuma.smartnotify.SmartNotifySMS) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
21	Broadcast Receiver (com.kuma.smartnotify.CarmodeWidgetProvider) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
22	Broadcast Receiver (com.kuma.smartnotify.SMSWidgetProvider) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
23	Broadcast Receiver (com.kuma.smartnotify.CallsWidgetProvider) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
24	Broadcast Receiver (com.kuma.smartnotify.SpeakWidgetProvider) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
25	Broadcast Receiver (com.kuma.smartnotify.SNWidgetProvider) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。

本报告由南明离火移动安全分析平台生成

26	Broadcast Receiver (com.kuma.smartnotify.SNBroadcastReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
27	Broadcast Receiver (com.kuma.smartnotify.dialer.receivers.ActionReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
28	高优先级 Intent（999） - {1} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

高危: **3** | 警告: **3** | 信息: **2** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	该文件是World Writable。任何应用程序都可以写入文件	高危	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
2	该文件是World Readable。任何应用程序都可以读取文件	高危	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
3	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
4	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
5	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限

6	默认情况下，调用Cipher.getInstance("AES")将返回AES ECB模式。众所周知，ECB模式很弱，因为它导致相同明文块的密文相同	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
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	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

应用行为分析

编号	行为	标签	文件
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
00189	获取短信内容	短信	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00126	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
00188	获取短信地址	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
00064	监控来电状态	控制	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
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
00191	获取短信收件箱中的消息	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
00095	将设备的ICCID写入文件	信息收集 电话服务	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
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
00036	从 res/raw 目录获取资源文件	反射	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
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	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
00038	查询电话号码	信息收集	升级会员：解锁高级权限
00102	将手机扬声器设置为打开	命令	升级会员：解锁高级权限
00112	获取日历事件的日期	信息收集 日历	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	19/30	android.permission.READ_SMS android.permission.WRITE_SMS android.permission.SEND_SMS android.permission.RECEIVE_SMS android.permission.RECEIVE_MMS android.permission.READ_CALL_LOG android.permission.WRITE_CALL_LOG android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.READ_PHONE_STATE android.permission.CALL_PHONE android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED android.permission.VIBRATE android.permission.WRITE_CALENDAR android.permission.READ_CALENDAR android.permission.CAMERA android.permission.MODIFY_AUDIO_SETTINGS android.permission.SYSTEM_ALERT_WINDOW

其它常用权限	7/46	android.permission.FLASHLIGHT android.permission.READ_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE com.android.launcher.permission.INSTALL_SHORTCUT android.permission.FOREGROUND_SERVICE android.permission.BLUETOOTH android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

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
www.kuma.cz	安全	否	**IP地址:** 185.59.211.210 **国家:** 捷克 **地区:** 布拉格 **城市:** 布拉格 **纬度:** 50.087915 **经度:** 14.421798 **查看:** Google 地图
liteapks.com	安全	否	**IP地址:** 172.67.73.174 **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

URL 链接安全分析

URL信息	源码文件
• http://www.kuma.cz/download/en-privacy.htm	com/kuma/smartnotify/ViewOnClickListenerC0000a.java
• https://liteapks.com/xxx.html	p000/p001/iab.java
• https://liteapks.com/app.html	p000/p001/iaw.java
• http://www.google.com/search?q=%s	自研引擎-S

敏感凭证泄露检测

可能的密钥
C+CgTFGA6Cyt4jXtFIlrxijxRU684sjgn/WncvVJPbMrHBQ+f0eE2YJbl2lFh+z1GoVPWhNcQbF212Tdup4AeRX70kGPQJyuxeFb6WtJzqs=
dR5Vx2mCx4GqCE6I6Mx84jGeMEe5c38m7jWIajevG8I=
BHoKAJ0BAR2DLOvQkDvRcNLeeqgqHLCqKMR1JfyXapo=

bKxCJRf2+J6gvv7C0fr4tYEBkjGR5dmbwzKykxOB8Fo=

Google Play 应用市场信息

标题: Smart Notify - Dialer & SMS

评分: 4.128655 **安装:** 1,000,000+ **价格:** 0 **Android版本支持:** **分类:** 通讯 **Play Store URL:** com.kuma.smartnotify

开发者信息: Milan Vyšata, Milan+Vy%C5%A1ata, Jungmannova 2241 347 01 Tachov Czech Republic , None, info@kuma.cz,

发布日期: 2013年1月29日 **隐私政策:** Privacy link

关于此应用:

具有内置拨号和短信功能的呼叫和短信处理和调度应用程序（默认消息应用程序）。 要删除短信，需要将应用程序设置为默认消息，否则不需要 - 双 SIM 卡支持 - 智能手表支持（提醒、电池充电通知） - 在选定的时间发送短信 - 显示待接电话和短信 - 当充电断开时，通过声音通知 GSM (Wi) 信号丢失或恢复，包括显示电池状态和温度，或可调节重复次数的已充电电池的声音信号 - 有来电或短信且静音模式开启时相机闪光灯闪烁 - 未接来电响铃时长 - 阻止来自选定号码的电话和短信 - 删除传出短信中的变音符号的选项 - 自动添加短信或未接来电到选定的日历 - 主屏幕上的一个小部件，其中包含未读短信、未接来电或我们未拨打的联系人（积压呼叫）以及用于新消息、电话拨号器或联系人概述的按钮 - 自动拒绝来自隐藏号码的呼叫的选项 如何在Android 8及以上版本中隐藏服务通知：https://youtu.be/sSdMUba763Y

免责声明及风险提示: