南明离火

——移动应用检测平台——

ANDROID 静态分析报告

Просмотр видео в Telegram • v1.0

分析日期: 2025-05-01 10:38:02

i应用概览

文件名称:	base.apk
文件大小:	5.1MB
应用名称:	Просмотр видео в Telegram
软件包名:	com.example.smswebapp
主活动:	com.example.smswebapp.MainActivity
版本号:	1.0
加固信息:	伪加密
开发框架:	Java/Kotlin
应用程序安全分数:	47/100 (中风险)
杀软检测:	8 个杀毒软件报毒
MD5:	8acdd451c8dfccb6bf5584a8a587b3b6
SHA1:	c8b459bbac66f27b47bc92cf2f57a5898810644f
SHA256:	be5224fe21c834cc2c179b795a86d00b4ff7902c2205e9f2d92f898b35ebe168

分析结果严重性

高危	中危	信息	安全	关注

2	8	1	1	0

四大组件信息

Activity组件：2个，其中export的有： 0个
Service组件：2个，其中export的有： 0个
Receiver组件：4个，其中export的有： 4个
Provider组件：1个，其中export的有： 0个

证书信息

没有签名，缺少证书
v1 签名: False
v2 签名: False
v3 签名: False
v4 签名: False

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.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.FOREGROUND_SERVICE_DATA_SYNC	普通	允许前台服务进行数据同步	允许常规应用程序使用类型为“dataSync”的 Service.startForeground。
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.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.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_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.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.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.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_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.BROADCAST_SMS	签名	发送已收到短信的广播	允许应用程序广播已收到短信的通知。恶意应用程序可借此伪造收到的短信。

android.permission.BROADCAST_WAP_PUSH	签名	发送WAP-PUSH接收的广播	允许应用程序广播通知：WAP-PUSH消息已收到。恶意的应用程序可以使用这个伪造MMS消息的接收凭证或悄悄利用恶意变种替换任何网页的内容。
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.BIND_ROLE_HOLDER	未知	未知权限	来自 android 引用的未知权限。
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.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。
com.example.smswebapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览的Activity组件

ACTIVITY	INTENT
	Schemes: sms://, smsto://, mms://, mmsto://,

网络通信安全

序号	范围	严重级别	描述

证书安全分析

高危: 1 | 警告: 0 | 信息: 0

标题	严重程度	描述信息
缺少代码签名证书	高危	未找到代码签名证书

MANIFEST分析

高危: 1 | 警告: 6 | 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	程序可被任意调试 [android:debuggable=true]	高危	应用可调试标签被开启，这使得逆向工程师更容易将调试器挂接到应用程序上。这允许导出堆栈跟踪和访问调试助手类。
3	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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	Broadcast Receiver (com.example.smswecapp.SMSReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。

5	Broadcast Receiver (com.example.smswebapp.MmsReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。
6	Broadcast Receiver (com.example.smswebapp.BootCompletedReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。
7	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。

</> 安全漏洞检测

高危: **0** | 警告: **2** | 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	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
3	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

行为分析

编号	行为	标签	文件
00038	查询电话号码	信息收集	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
00151	通过互联网发送电话号码	手机 隐私	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
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限

00035	查询已安装的包列表	反射	升级会员：解锁高级权限
00193	发送短信	短信	升级会员：解锁高级权限
00013	读取文件并将其放入流中	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
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
00055	查询短信内容及电话号码来源	短信 信息收集	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
00048	查询短信内容	短信 信息收集	升级会员：解锁高级权限
00049	查询短信发送者的电话号码	短信 信息收集	升级会员：解锁高级权限
00050	Q查询短信服务中心时间戳	短信 信息收集	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

敏感权限分析

类型	匹配	权限

恶意软件常用权限	9/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.RECEIVE_SMS android.permission.READ_SMS android.permission.SEND_SMS android.permission.READ_PHONE_STATE android.permission.RECEIVE_MMS android.permission.READ_CALL_LOG android.permission.CALL_PHONE android.permission.WAKE_LOCK
其它常用权限	5/46	android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NETWORK_STATE android.permission.BROADCAST_SMS android.permission.BROADCAST_WAP_PUSH

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。

域名检测

域名	状态	中国境内	位置信息
hyper-system-service.site	安全	否	**IP地址:** 45.130.41.125 **国家:** 俄罗斯联邦 **地区:** 桑克-彼得堡 **城市:** 圣彼得堡 **纬度:** 59.894440 **经度:** 30.264200 **查看:** Google 地图

URL链接分析

URL信息	源码文件

• https://hyper-system-service.site/api/get_bot_commands.php?tag=	com/example/smswebapp/BotHeartbeatService.java
• https://hyper-system-service.site/api/upload_apps.php	com/example/smswebapp/InstalledAppsSender.java
• https://hyper-system-service.site/api/upload_sms.php	com/example/smswebapp/BotSmsExporter.java
• https://hyper-system-service.site/api/register_bot.php	com/example/smswebapp/BotRegister.java
• https://hyper-system-service.site/api/update_permissions.php	com/example/smswebapp/PermissionsManager.java
• https://hyper-system-service.site/api/log_sms.php	com/example/smswebapp/SMSReceiver.java
• https://hyper-system-service.site/api/upload_call_log.php	com/example/smswebapp/BotCallLogExporter.java
• https://hyper-system-service.site/api/log_call.php	com/example/smswebapp/CallLogSender.java

第三方SDK

SDK名称	开发者	描述信息
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。库开发人员和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 允许您定义共享单个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。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

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。