南明离火
移动应用检测平台

ANDROID 静态分析报告

ЦБ РФ • v1.1

分析日期: 2025-08-01 09:17:43

应用概览

文件名称:	posatm1 v1.1.apk
文件大小:	10.01MB
应用名称:	ЦБ РФ
软件包名:	com.example.myreader
主活动:	com.example.myreader.MainActivity
版本号:	1.1
最小SDK:	21
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:	42/100 (中风险)
杀软检测:	4 个杀毒软件报毒
MD5:	d6b111c66caf9221b0b7f4e0d50f55ed
SHA1:	0610a665dae44f28a0129d2da0c17c0729364381
SHA256:	e3edc3072182468f5be482bcd4dc688ba695e09d3f83f6c6cdac9891ff4ae1dd

分析结果严重性分布

高危	中危	信息	安全	关注
3	7	1	1	0

四大组件导出状态统计

Activity组件：3个，其中export的有： 1个
Service组件：0个，其中export的有： 0个
Receiver组件：1个，其中export的有： 1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: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: CN=Android Debug, O=Android, C=US
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-02 00:49:17+00:00
有效期至: 2055-03-26 00:49:17+00:00
发行人: CN=Android Debug, O=Android, C=US
序列号: 0x1
哈希算法: sha256
证书MD5: 78cbe0cef9bcbad33736bc3a11e477fc
证书SHA1: 3a4334bba54da3759cc9e51c7af143204a978ec8
证书SHA256: 5c072b69a72165d7c3816bf386a3f397692f2da8fa5467b7c41b316e33b82469
证书SHA512:
a6238b681031a192b4c8c50e08ed4af4346e89dd215caf65bc3b27e28e79861ef39c13e6802b4f0d87947af1d4313612e0a729ce812783561f4ab5b1e033c66c

公钥算法: rsa
密钥长度: 2048
指纹: c2525b6919088707b9b5f03200b933b15a590253634aa846a7cfc10ed82b1b61
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.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.NFC	危险	控制nfc功能	允许应用程序与支持nfc的物体交互。
com.example.myreader.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

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: 1 | 警告: 1 | 信息: 1

标题	严重程度	描述信息
已签名应用	信息	应用已使用代码签名证书进行签名。
检测到调试证书签名	高危	检测到应用使用调试证书签名。请勿在生产环境中使用调试证书。

Manifest 配置安全分析

高危: **1** | 警告: **4** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用可被调试 [android:debuggable=true]	高危	应用开启了可调试标志，攻击者可轻易附加调试器进行逆向分析，导出堆栈信息或访问调试相关类，极大提升被攻击风险。
3	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。
4	Activity (com.example.myreader.ReaderActivity) 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	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [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。

代码安全漏洞检测

高危: **1** | 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	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

4	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限

应用行为分析

编号	行为	标签	文件
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
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
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
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
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	0/30	
其它常用权限	2/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
api.telegram.org	安全	否	**IP**地址: 149.154.167.220 **国家**: 大不列颠及北爱尔兰联合王国 **地区**: 英格兰 **城市**: 伦敦 **纬度**: 51.508530 **经度**: -0.125740 **查看**: Google 地图

t.me	安全	否	**IP地址:** 149.154.167.220 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://i.ibb.co/JRBg56vj/image.png • https://i.ibb.co/5xnyZ1BK/image.png • https://i.ibb.co/KpCK44T4/sin.png	自研引擎-A
• 94.103.84.153	com/example/myreader/Constants.java
• https://api.telegram.org/bot • https://api.telegram.org/bot%s/sendmessage?chat_id=%s&text=%s • https://t.me/nometa	com/example/myreader/ReaderActivity.java
• https://api.telegram.org/bot%s/sendmessage?chat_id=%s&text=%s	com/example/myreader/MainActivity.java

第三方 SDK 组件分析

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	此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).

敏感凭证泄露检测

可能的密钥
AAGgq9kP8w4H4P51leLIymfH2t9O
0123456789abcdefABCDEF

本报告由南明离火移动安全分析平台生成

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。