南明离火
移动应用检测平台

ANDROID 静态分析报告

myapp99 • v1.0

分析日期: 2025-04-03 18:42:47

应用概览

文件名称:	app-release_killer.apk
文件大小:	4.59MB
应用名称:	myapp99
软件包名:	com.example.myapp2
主活动:	com.example.myapp2.MainActivity2
版本号:	1.0
最小SDK:	24
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	55/100 (中风险)
杀软检测:	AI评估：安全
MD5:	2dcefa321b4180563631050a2684dbc7
SHA1:	78d542942c85596d9860a1779e1ef6bda485675b
SHA256:	d833b26471053d6086ead828ecb83a52ed1c91355dc36add5b8f369f9501ef51

分析结果严重性

高危	中危	信息	安全	关注
1	2	0	1	1

四大组件信息

Activity组件：2个，其中export的有：1个
Service组件：0个，其中export的有：0个
Receiver组件：0个，其中export的有：0个
Provider组件：1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: False
v3 签名: False
v4 签名: None
主题: C=cn, ST=ak, L=ak, O=androidkiller, OU=androidkiller, CN=androidkiller
签名算法: rsassa_pkcs1v15
有效期自: 2014-12-23 06:27:44+00:00
有效期至: 2069-09-25 06:27:44+00:00
发行人: C=cn, ST=ak, L=ak, O=androidkiller, OU=androidkiller, CN=androidkiller
序列号: 0x661d0629
哈希算法: sha256
证书MD5: 6230025aa9d683803c2bec499f6be89b
证书SHA1: ac4c35dbb80e320ac5e432f4991fd81798191c68
证书SHA256: 927d5aa90736d7b8d1b1f06978bb3697395caf14f794544158f37abd0f21df6d
证书SHA512:
50a756bf495b76d7583b0d1970eb4bfd7b7a7f4754bd57f486a2ba9996b7ccb8a4f88fdcf16189634909819b2b35e81654a4f687...9328cb3bdf27036a

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.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
com.example.myapp2.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

序号	范围	严重级别	描述

证书安全分析

高危: **1** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名
应用程序容易受到 Janus 漏洞的影响	高危	应用程序使用 v1 签名方案进行签名，如果仅使用 v1 签名方案进行签名，则在 Android 5.0-8.0 上容易受到 Janus 漏洞的影响。在使用 v1 和 v2/v3 方案签名的 Android 5.0-7.0 上运行的应用程序也容易受到攻击。

MANIFEST分析

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

序号	问题	严重程度	描述信息
1	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。
2	Activity (com.example.myapp2.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。

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	0/30	
其它常用权限	1/46	android.permission.INTERNET

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
i4t.com	安全	是	**IP地址:** 211.159.158.83 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图

URL链接分析

URL信息	源码文件
• https://i4t.com	com/example/myapp2/MainActivity2.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 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: