南明离火
移动应用检测平台

ANDROID 静态分析报告

NShare • v1.4.0

分析日期: 2024-09-28 10:09:32

应用概览

文件名称:	best.share.machin v1.4.0.apk
文件大小:	4.52MB
应用名称:	NShare
软件包名:	best.share.machin
主活动:	best.share.machin.activity.Main2Activity
版本号:	1.4.0
最小SDK:	14
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	52/100 (中风险)
杀软检测:	2 个杀毒软件报毒
MD5:	8aab63964245d09289bf3e7c48a6dcf1
SHA1:	953c4198aa57cc32342892eb2bdc2c1df753c44bd
SHA256:	54acf5200f63e153155433019d61ee91122ef2fd3b879a4f491a675d3795d9e7

分析结果严重性分布

高危	中危	信息	安全	关注
2	4	2	2	0

四大组件导出状态统计

Activity组件：20个，其中export的有：4个
Service组件：5个，其中export的有：3个
Receiver组件：2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

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=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2020-07-12 15:35:38+00:00
有效期至: 2050-07-12 15:35:38+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x2ba89ec0cc56a871537c0e865aba698434f8d039
哈希算法: sha256
证书MD5: 7045946529cb0ec35290e9e0b73ebc69
证书SHA1: 50f5e3391d162921e849c426906696bf80542b98
证书SHA256: cd9ab4427cf52078b2fa0d1fceb61291d04711a0b6dc25051505449ef1aaa064
证书SHA512:
c7604f467f616a8c0ad98118985621b27c62084bf99c732fe3ba559879e1ffa3e3be5ab0e95cb9e22560f136b3f4de9dcbf3376acdb7c2f8ae6278d1fc54a8cd

公钥算法: rsa
密钥长度: 4096
指纹: 2496ebe7db1c4f0fe269d772424f9013a1935cb3e8d53230871c0fa757f114a6
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_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_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.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.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
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.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.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
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.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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
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粗略的经纬度信息，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.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.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.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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
best.share.machin.activity.ViewTransferActivity	Schemes: file://, content://, Hosts: *, Mime Types: */*, Path Patterns: .*\\.tshare, .*\\..*\\.tshare,

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: **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: **2** | 警告: **9** | 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 4.0-4.0.2, [minSdk=14]	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。
3	Activity (best.share.machin.activity.HomeActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
4	Activity (best.share.machin.activity.HomeActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity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Activity是显式导出的。
5	Activity (best.share.machin.activity.ShareActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity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Activity是显式导出的。

6	Activity (best.share.machin.activity.ContentSharingActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
7	Activity (best.share.machin.activity.ViewTransferActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity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Activity是显式导出的。
8	Activity (best.share.machin.activity.ChangeStoragePathActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity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Activity是显式导出的。
9	Broadcast Receiver (best.share.machin.receiver.NetworkStatusReceiver) 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。
10	Service (best.share.machin.service.DeviceChooserService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_CHOOSER_TARGET_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。
11	Service (best.share.machin.service.DeviceScannerService) 未被保护。 存在一个intent-filter。	警告	发现 Service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Service是显式导出的。
12	Service (best.share.machin.service.CommunicationToggleTile) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_QUICK_SETTINGS_TILE [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。

代码安全漏洞检测

高危: **0** | 警告: **5** | 信息: **2** | 安全: **1** | 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	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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
3	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
4	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
5	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
6	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
7	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
8	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	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	8/30	android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.SYSTEM_ALERT_WINDOW android.permission.WRITE_SETTINGS android.permission.ACCESS_COARSE_LOCATION android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.CAMERA

其它常用权限	7/46	android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.INTERNET android.permission.FOREGROUND_SERVICE 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
mylivetvforyou.blogspot.com	安全	否	**IP地址:** 142.250.68.1 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
www.ubuntu.com	安全	否	**IP地址:** 185.125.190.21 **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://mylivetvforyou.blogspot.com/2020/07/trebleshot-and-nshare.html	best/share/machin/activity/Main2Activity.java
• https://mylivetvforyou.blogspot.com/2020/07/nshare-fun.html	best/share/machin/activity/MainActivity.java
• 1.0.2.8	com/genonbeta/android/framework/BuildConfig.java
• 127.0.0.1	fi/iki/elonen/NanoHTTPD.java
• http://%s:%d/ • 127.0.0.1 • https://www.ubuntu.com/legal/font-licence • https://mylivetvforyou.blogspot.com/2020/07/trebleshot-and-nshare.html • 192.168.1.2 • https://github.com/velitasali/ubuntufontforandroid • https://mylivetvforyou.blogspot.com/2020/07/nshare-fun.html • 1.0.2.8	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
ZXing Android Embedded	JourneyApps	Barcode scanning library for Android, using ZXing for decoding.
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。

免责声明及风险提示: