南明离火
移动应用检测平台

ANDROID 静态分析报告

App List • v1.4.1

分析日期: 2024-05-13 17:42:48

应用概览

文件名称:	应用列表.apk
文件大小:	4.75MB
应用名称:	App List
软件包名:	com.cvte.tv.appstore
主活动:	com.cvte.tv.appstore.AppStoreActivity
版本号:	1.4.1
最小SDK:	15
目标SDK:	23
加固信息:	未加壳
应用程序安全分数:	40/100 (中风险)
杀软检测:	3 个杀毒软件报毒
MD5:	83af4eccc4c2dbeaca363142fe3c4495
SHA1:	d924e0ed1031777bebfcd8ff7a1dfaa21dc8e74
SHA256:	91d5999bcc6ce491b4b89f4ec0035a283afe553bdd27dd1241b15ea9eec9d6

分析结果严重性分布

高危	中危	信息	安全	关注
5	13	1	1	2

四大组件导出状态统计

Activity组件：5个，其中export的有：3个
Service组件：2个，其中export的有：1个
Receiver组件：1个，其中export的有：1个
Provider组件：0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: False
v3 签名: False

本报告由南明离火移动安全分析平台生成

v4 签名: False
主题: C=CN, ST=GD, L=GZ, O=CVTE, OU=TV, CN=XRD
签名算法: rsassa_pkcs1v15
有效期自: 2016-07-07 09:38:02+00:00
有效期至: 2046-07-10 09:38:02+00:00
发行人: C=CN, ST=GD, L=GZ, O=CVTE, OU=TV, CN=XRD
序列号: 0xdbdf6221ff579746
哈希算法: sha1
证书MD5: 349c23576959233f70c580cb5c663d53
证书SHA1: 0e0a17620756275f8dbfa108d29e306d9d8634da
证书SHA256: 6d0d02eb08af38376b1d8c8dec09a17703307b43c5c3fef1475bb0d9bd6441c0
证书SHA512:
08916f4c390032d14ade9b4e3eedcbbc1016bf11f268201f0f61fef4b06332a98e5aaa5b773b15d2d5a3d303325371c845aefe761c8916ba25[illegible]56564d3da63

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.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_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.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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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.permission.READ_PHONE_STATE	危险	读取手机状态和标[illegible]	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.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.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_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.RESTART_PACKAGES	普通	重启进程	允许程序自己重启或重启其他程序
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
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。

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: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

高危: **4** | 警告: **7** | 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 4.0.3-4.0.4, [minSdk=15]	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。
3	Activity (com.cvte.tv.appstore.AppStoreActivity) 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 （com.cvte.tv.appstore.AppStoreActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (23) 更新到 28 或更高版本以在平台级别修复此问题。
5	Activity (com.cvte.tv.appstore.AppListActivity) 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 (com.cvte.tv.appstore.AppDetailActivity) 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 (com.cvte.tv.appstore.AppDetailActivity) 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。
8	Activity (com.cvte.tv.appstore.AppSelectActivity) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (23) 更新到 29 或更高版本以在平台级别修复此问题。

本报告由南明离火移动安全分析平台生成

9	Activity (com.cvte.tv.appstore.AppSelectActivity) 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。
10	Service (com.cvte.tv.appstore.modules.download.services.DownloadService) 未被保护。 [android:exported=true]	警告	发现 Service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。
11	Broadcast Receiver (com.cvte.tv.appstore.modules.webclient.NetWorkReceiver) 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。
12	高优先级的Intent (2147483647) [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

代码安全漏洞检测

高危: **0** | 警告: **5** | 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	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	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
5	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

6	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY (栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)
1	armeabi/libmengyou_bspatch.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会对溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限

恶意软件常用权限	7/30	android.permission.GET_TASKS android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.WRITE_SETTINGS android.permission.GET_ACCOUNTS android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.READ_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
myou.cvte.com	安全	是	**IP地址:** 42.192.255.173 **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
starkapp.cvte.com	安全	是	**IP地址:** 42.192.255.173 **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 链接安全分析

URL信息	源码文件
• http://myou.cvte.com/api/v1/monitor	com/cvte/a/f.java
• http://www.baidu.com • http://myou.cvte.com	com/cvte/a/g.java
• http://starkapp.cvte.com/ws/api/blacklist	com/cvte/tv/appstore/a/g.java
• http://starkapp.cvte.com/download/apk/ • http://starkapp.cvte.com/download/icon/	com/cvte/tv/appstore/c/a.java
• http://starkapp.cvte.com/	com/cvte/tv/appstore/modules/webclient/c.java
• http://starkapp.cvte.com/	com/cvte/tv/appstore/modules/webclient/impl/AppStoreApiImpl.java

• http://www.baidu.com • http://myou.cvte.com • http://starkapp.cvte.com/ws/apk/blacklist • http://starkapp.cvte.com/download/apk/ • http://myou.cvte.com/api/v1/monitor • http://starkapp.cvte.com/download/icon/ • http://starkapp.cvte.com/	自研引擎-S

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。

敏感凭证泄露检测

可能的密钥
凭证信息=> "MENGYOU_APPKEY" : "2aeafc622eb303fedab32c455231169a9e682733"
2aeafc622eb303fedab32c455231169a9e682733
bd0b79944bc47b663ffcc030db655c75cfd0eff7
5cc5aca6c6fca4842e86133c6ba2f564e447ad1d

免责声明及风险提示: