南明离火
移动应用检测平台

ANDROID 静态分析报告

uToor • v1.0.4

分析日期: 2024-09-29 15:24:51

应用概览

文件名称:	utoor.torrent.search2 v1.0.4.apk
文件大小:	2.69MB
应用名称:	uToor
软件包名:	utoor.torrent.search2
主活动:	com.example.torrseartool.OpeningActivity
版本号:	1.0.4
最小SDK:	21
目标SDK:	33
加固信息:	未加壳
应用程序安全分数:	51/100 (中风险)
跟踪器检测:	1/432
杀软检测:	经检测，该文件安全
MD5:	50ce5695e6bb842d009d407eae875ce8
SHA1:	c6066c119c3dbcd7e5ddf03fe[illegible]253cfdd38
SHA256:	d6a83fb86d8842700e18e[illegible]34cdaa76cbe502[illegible]6426773c21d9fb360

分析结果严重性分布

高危	中危	信息	安全	关注
1	14	2	1	0

四大组件导出状态统计

Activity组件：6个，其中export的有：0个
Service组件：2个，其中export的有：0个
Receiver组件：1个，其中export的有：1个
Provider组件：2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: True
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: 2024-04-08 21:14:42+00:00
有效期至: 2054-04-08 21:14:42+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x24231d62510689d26a2f8984ec08899297c4af27
哈希算法: sha256
证书MD5: 9381230ac807f22da54f5bed1c62159b
证书SHA1: 44fac097a7decbced37a9fe7e609cd437454a7c2
证书SHA256: 8b0cbbe84b2fb510a995291f0ea3167ae2062e90ab21cdb7cec7e4f1bfeb015a
证书SHA512:
9368c4b1c0bcda366f1fe91e0574d822a8b90ee2b2cbdf66fb7062fff81aeb3acfd1a0828fa1bbb95dd51a1e379dcfe98be21c1fceaea8018cde7e0375a89f99

公钥算法: rsa
密钥长度: 4096
指纹: 6a1847a32ccee9b5aefa9ab5d172a18ec760884deb13cc1becb2bd87e0f16f2e
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_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.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.AD_ID	未知	未知权限	来自 android 引用的未知权限。
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.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。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
android.permission.ACCESS_ADSERVICES_TOPICS	普通	允许应用程序访问广告服务主题	这使应用程序能够检索与广告主题或兴趣相关的信息，这些信息可用于有针对性的广告目的。

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

本报告由南明离火移动安全分析平台生成

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: **0** | 警告: **3** | 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 5.0-5.0.2, [minSdk=21]	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。
3	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。
4	Broadcast Receiver (com.startapp.sdk.adsbase.remoteconfig.BootCompleteListener) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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。

代码安全漏洞检测

高危: **1** | 警告: **9** | 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	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
3	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	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	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
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	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
8	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
9	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
10	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
11	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
12	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

13	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	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	1/30	android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	5/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.ACCESS_WIFI_STATE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.gms.permission.AD_ID

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
adsmetadata.mobileadexchange.net	安全	否	**IP地址:** 213.35.117.150 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
infoevent.startappservice.com	安全	否	**IP地址:** 138.2.110.152 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
www.startapp.com	安全	否	**IP地址:** 138.2.110.152 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
geoip.api.p3insight.de	安全	否	No Geolocation information available.
d26xw8rpcmngfg.cloudfront.net	安全	否	**IP地址:** 18.154.207.110 **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

support.start.io	安全	否	**IP地址:** 152.195.62.69 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.773968 **经度:** -122.410446 **查看:** Google 地图
adsmetadata.startappservice.com	安全	否	**IP地址:** 138.2.110.152 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.85028 **查看:** Google 地图
daneden.me	安全	否	**IP地址:** 138.2.110.152 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 核桃 **纬度:** 34.015400 **经度:** -117.858223 **查看:** Google 地图
imp.startappservice.com	安全	否	**IP地址:** 152.195.62.69 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
lh6.ggpht.com	安全	否	**IP地址:** 172.217.14.97 **国家:** 美利坚合众国 **地区:** 华盛顿 **城市:** 西雅图 **纬度:** 47.604309 **经度:** -122.329842 **查看:** Google 地图
req.startappservice.com	安全	否	**IP地址:** 152.195.62.69 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
info.startappservice.com	安全	否	**IP地址:** 152.195.62.69 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 33.972069 **经度:** -118.430313 **查看:** Google 地图

d2to8y50b3n6dq.cloudfront.net	安全	否	**IP地址:** 18.154.207.110 **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
funnel-assets.startappservice.com	安全	否	**IP地址:** 152.195.62.69 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 33.972069 **经度:** -118.430315 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• javascript:startappbackpressed	com/startapp/sdk/adsbase/consent/ConsentActivity.java
• javascript:splash_fadeout • https://daneden.me/animate • https://lh6.ggpht.com/vo9wbfh89bbdbwfhuezqzogpkmfkjsatibvwk3qxnbyiwcr0r79evui0ab41a-je7x6=w200	com/startapp/sdk/ads/splash/SplashHtml.java
• http://0.0.0.0	com/startapp/kb.java
• https://info.startappservice.com/inapp/resources/info_l.png	com/startapp/sdk/adsbase/adinformation/AdInformationMetaData.java
• https://www.startapp.com • data:;base64,ivborw0kggo=	com/startapp/sdk/ads/video/vast/VASTResource.java
• http://134.209.240.60/toor/logica/logica/logica_ottieni_configurazione.php • http://adservice.google.com/getconfig/pubvendors	f1/u.java
• https://www.startapp.com/policy/privacy-policy/ • https://funnel-assets.startappservice.com/consent/index.html	com/startapp/sdk/adsbase/adinformation/AdInformationConfig.java
• https://play.google.com • http://play.google.com	com/startapp/sdk/adsbase/a.java
• 10.0.2.15	com/startapp/c2.java
• https://imp.startappservice.com/tracking/adimpression	com/startapp/q.java
• https://play.google.com/store/search?q=torrent	com/example/torrseartool/HomeActivity.java
• https://infoevent.startappservice.com/tracking/infoevent	com/startapp/sdk/adsbase/remoteconfig/AnalyticsConfig.java
• https://support.start.io/hc/en-us/articles/360014774799	com/startapp/sdk/adsbase/StartAppSDKInternal.java
• https://play.google.com/store/apps/details?id=utoor.torrent.search2	f1/w.java

本报告由南明离火移动安全分析平台生成

• https://adsmetadata.mobileadexchange.net/adsmetadata/api/v1.0/ • https://adsmetadata.startappservice.com/adsmetadata/api/v1.0/ • https://req.startappservice.com/1.5/ • https://d26xw8rp6mlgfg.cloudfront.net/adsmetadata/api/v1.0/	com/startapp/sdk/adsbase/remoteconfig/MetaData.java
• https://support.start.io/hc/en-us/articles/360014774799	com/startapp/r.java
• https://geoip.api.p3insight.de/geoip/ • https://d2to8y50b3n6dq.cloudfront.net/truststores/	com/startapp/sdk/insight/NetworkTestsMetaData.java
• https://www.startapp.com • 10.0.2.15 • https://www.startapp.com/policy/privacy-policy/ • http://play.google.com • https://info.startappservice.com/inapp/resources/info_l.png • https://lh6.ggpht.com/vo9wbfh89bbdbwfhuezqzogpkmfkjsatibvwk3qxpbvjwcr8i79evui0ab41a-je7x-6=w200 • javascript:splash_fadeout • https://d2to8y50b3n6dq.cloudfront.net/truststores/ • javascript:startappbackpressed • https://play.google.com/store/apps/details?id=utoor.torrent.search2 • http://134.209.240.60/toor/logica/logica/logica/ottieni_configurazione.php • https://play.google.com/store/search?q=torrent • https://geoip.api.p3insight.de/geoip/ • https://daneden.me/animate • http://0.0.0.0 • https://support.start.io/hc/en-us/articles/360014774799 • https://play.google.com • http://adservice.google.com/getconfig/pubvendors • data:;base64,ivborw0kggo=	查看引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。

第三方追踪器检测

名称	类别	网址
Startapp	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/195

敏感凭证泄露检测

可能的密钥
com/Vo9wbFH89BbDbWFhUezQZOGPKmfkJSAtIbVWk3QxPbvJwcR8I79EVuI0aB41a
2F73797374656D2F6C69622F6C69627265666572656E63652D72696C2E736F
3A757365722F72656C656173652D6B657973

Google Play 应用市场信息

标题: uToor - Torrent Search

评分: 0 **安装:** 1,000+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** utoor.torrent.search2

开发者信息: uToor Apps, uToor+Apps, None, None, uToorApp@outlook.com,

发布日期: 2024年4月8日 **隐私政策:** Privacy link

关于此应用:

uToor 是一个 torrent 搜索引擎，允许用户查找和发现磁力格式的 torrent 链接。您可以将此应用程序与您最喜欢的 torrent 下载器应用程序结合使用来搜索和下载视频、音频等。 特点： * 快速种子搜索 * 声音搜索 * 多个搜索提供商可用 * 复制并分享 torrent 磁力链接 * 按播种者、下载者、日期和大小对种子进行排序 * 按类别过滤种子 * 从搜索结果中删除没有播种器的种子

免责声明及风险提示: