南明离火
移动应用检测平台

ANDROID 静态分析报告

Volume Booster Pro • v1.8

分析日期: 2025-03-11 09:50:51

应用概览

文件名称:	Volume_Booster_Pro_1.8-pro_8_dae06c.apk
文件大小:	3.85MB
应用名称:	Volume Booster Pro
软件包名:	com.soundapps.volumebooster.pro
主活动:	com.jojoy.delegate.JojoyInstallerActivity
版本号:	1.8
最小SDK:	19
目标SDK:	25
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	45/100 (中风险)
跟踪器检测:	5/432
杀软检测:	7 个杀毒软件报毒
MD5:	98e9fb94cfe9164c86d4eab6499c8712
SHA1:	d315913e817318143523da1cbdec0fb51ed4cd6e
SHA256:	dae06c189667473dc753781c952ca5206fbb220ffb3543f22f9fbfd3b536128a

分析结果严重性

高危	中危	信息	安全	关注
3	14	2	1	1

四大组件信息

Activity组件：7个，其中export的有： 1个
Service组件：5个，其中export的有： 1个
Receiver组件：5个，其中export的有： 3个
Provider组件：3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: True
v3 签名: True
v4 签名: False
主题: O=jojoy.mod
签名算法: rsassa_pkcs1v15
有效期自: 2021-11-11 02:56:52+00:00
有效期至: 2120-10-18 02:56:52+00:00
发行人: O=jojoy.mod
序列号: 0x3b8e0f2a
哈希算法: sha256
证书MD5: 082eebeb1b8af3326b42c241e7c6de94
证书SHA1: dfa1bcc9f927744eff6a24bddf1feadcb632e37c
证书SHA256: c104e57fa7aea4ac9fc5f050e9639d4b3ace4ab23b68348998902088776ed58d
证书SHA512:
7ab82c172fb5d28e83ec2dd74f0304fcc682ea75ebac49026a9783e8954cb57424cd320fcf4b7a4df94fbed0a4d881e3383a759c03cac82f1c6a879b867198d6

公钥算法: rsa
密钥长度: 2048
指纹: fc2256a38aef0878e6689017c99505499dc18a2bce8b2cb2a3f4f4da6a8b6253
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.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
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.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。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
com.soundapps.volumebooster.pro.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。

网络通信安全

序号	范围	严重级别	描述

证书安全分析

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	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **1** | 警告: **6** | 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.soundapps.volumebooster.MainActivity) 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。
3	Broadcast Receiver (com.appbrain.ReferrerReceiver) 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。
4	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	警告	发现一个 Broadcast Receiver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。
5	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver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。
6	Service (com.google.firebase.iid.FirebaseInstanceIdService) 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。
7	Activity (com.jojoy.delegate.JojoyInstallerActivity) 容易受到StrandHogg 2.0的攻击	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 (25) 更新到 29 或更高版本以在平台级别修复此问题。

安全漏洞检测

高危: **1** | 警告: **7** | 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	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	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	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
6	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
7	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
8	应用程序使用SQLite数据库执行原始SQL查询。原始SQL查询中处理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
9	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

行为分析

编号	行为	标签	文件
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
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
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	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
00153	通过 HTTP 发送二进制数据	http	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00083	查询IMEI号	信息收集 电话服务	升级会员：解锁高级权限
00016	获取设备的位置信息并将其放入 JSON 对象	位置 信息收集	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	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
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	升级会员：解锁高级权限
00065	获取SIM卡提供商的国家代码	信息收集	升级会员：解锁高级权限
00132	查询ISO国家代码	电话服务 信息收集	升级会员：解锁高级权限
00146	获取网络运营商名称和IMSI	电话服务 信息收集	升级会员：解锁高级权限
00038	查询电话号码	信息收集	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00117	获取 IMSI 和网络运营商名称	电话服务 信息收集	升级会员：解锁高级权限
00067	查询IMSI号码	信息收集	升级会员：解锁高级权限

00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 控制	升级会员：解锁高级权限
00035	查询已安装的包列表	反射	升级会员：解锁高级权限
00062	查询WiFi信息和WiFi Mac地址	WiFi 信息收集	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00116	获取当前WiFi MAC地址并放入JSON中	WiFi 信息收集	升级会员：解锁高级权限
00076	获取当前WiFi信息并放入JSON中	信息收集 WiFi	升级会员：解锁高级权限
00082	获取当前WiFi MAC地址	信息收集 WiFi	升级会员：解锁高级权限
00003	将压缩后的位图数据放入JSON对象中	相机	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	2/30	android.permission.MODIFY_AUDIO_SETTINGS android.permission.WAKE_LOCK
其它常用权限	3/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE com.google.android.c2dm.permission.RECEIVE

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

plugin.moddroid.co	安全	否	**IP地址:** 34.231.89.55 **国家:** 美国 **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
bit.ly	安全	否	**IP地址:** 35.225.17.101 **国家:** 美国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.750134 **经度:** -73.997009 **查看:** Google 地图
mediation1.apptornado.com	安全	否	**IP地址:** 35.225.17.101 **国家:** 美国 **地区:** 爱荷华州 **城市:** 康瑟尔布拉夫斯 **纬度:** 41.261940 **经度:** -95.860832 **查看:** Google 地图
apps-3d7d2.firebaseio.com	安全	否	**IP地址:** 34.120.160.131 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
market.android.com	安全	否	**IP地址:** 142.250.72.174 **国家:** 美国 **地区:** 科罗拉多州 **城市:** 丹佛 **纬度:** 39.739361 **经度:** -104.983597 **查看:** Google 地图
api.topstrawberry.com	安全	否	**IP地址:** 172.67.135.225 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
sdk.appbrain.comhttps	安全	否	No Geolocation information available.
applift-a.apptornado.comhttps	安全	否	No Geolocation information available.
applift-a.apptornado.com	安全	否	**IP地址:** 172.67.135.225 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

manual.sensorsdata.cn	安全	是	**IP地址:** 61.160.227.233 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
etpr-game.jojoy.mobi	安全	否	**IP地址:** 43.134.152.57 **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

URL链接分析

URL信息	源码文件
• https://api.topstrawberry.com/api/ad/game/get/config • https://api.topstrawberry.com	com/advertisement/waterfall/sdk/config/AdConfigManager.java
• https://plugin.moddroid.co • https://bit.ly/3avsljk • https://bit.ly/3g3fxm2	com/jojoy/core/Constants.java
• javascript:window.sensorsdata_app_call_js	etp/com/sensorsdata/analytics/android/sdk/visual/bridge/JSBridgeHelper.java
• http://market.android.com • http://play.google.com • https://play.google.com • https://market.android.com	com/appbrain/a/af.java
• https://applift-a.apptornado.com,https://applift-b.apptornado.com • http://mediation1.apptornado.com • https://sdk.appbrain.com,https://sdk-b.apptornado.com • https://applift-a.apptornado.com	com/appbrain/a/k.java
• https://manual.sensorsdata.cn/sa/latest/tech_sdk_client_web_use-7545346.html	etp/com/sensorsdata/analytics/android/sdk/visual/ViewSnapshot.java
• 10.0.2.15	a/a/a/d.java
• https://plugin.moddroid.co/plugin/channel?id= • https://plugin.moddroid.co/plugin/keywords • https://plugin.moddroid.co/plugin/config?id= • https://plugin.moddroid.co/plugin/pop_up?id=	com/jojoy/core/model/MainRepository.java
• 10.0.2.15	etp/a/a/a/d.java
• https://www.google.com/search?q=	com/jojoy/core/main/JojoyContainer.java
• https://etpr-game.jojoy.mobi	com/jojoy/core/log/LogManager.java
• https://play.google.com/store/apps/details?id=com.soundapps.volumebooster.pro • https://apps-3d7d2.firebaseio.com	自研引擎-S

FIREBASE数据库分析

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://apps-3d7d2.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	Firebase远程配置URL （https://firebaseremoteconfig.googleapis.com/v1/projects/1016904315817/namespaces/firebase:fetch?key=AIzaSyB7_xWiBdjAnVQAPsOQvAfXG0RBszpmlKA ）已禁用。响应内容如下所示:
		{
		"state": "NO_TEMPLATE"
		}

第三方SDK

SDK名称	开发者	描述信息
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用测量解决方案，可提供关于应用使用情况和用户互动度的分析数据。

追踪器

名称	类别	网址
AppBrain		https://reports.exodus-privacy.eu.org/trackers/136
Flurry	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/25
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sensors Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/248

密钥凭证

可能的密钥
凭证信息=> "ETP_KEY" : "20378"
凭证信息=> "FLURRY_KEY" : "7MN7MSM85GDW3J7P6Z23"
"firebase_database_url" : "https://apps-3d7d2.firebaseio.com"

"google_api_key" : "AIzaSyB7_xWiBdjAnVQAPsOQvAfXG0RBszpmlKA"
"google_app_id" : "1:1016904315817:android:2ca258397365feeb"
"google_crash_reporting_api_key" : "AIzaSyB7_xWiBdjAnVQAPsOQvAfXG0RBszpmlKA"
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

免责声明及风险提示: