南明离火
移动应用检测平台

ANDROID 静态分析报告

Emtu Lugar • v7.9

分析日期: 2024-09-27 16:32:07

应用概览

文件名称:	ar.com.alltrack.santarosacolectivos v7.9.apk
文件大小:	2.98MB
应用名称:	Emtu Lugar
软件包名:	ar.com.alltrack.santarosacolectivos
主活动:	ar.com.alltrack.santarosacolectivos.WelcomeActivity
版本号:	7.9
最小SDK:	21
目标SDK:	31
加固信息:	未加壳
应用程序安全分数:	64/100 (低风险)
杀软检测:	经检测，该文件安全
MD5:	9c46e3ef4f2a69744e16bafb257ce3be
SHA1:	bc6231a0b6c979a30ee39fca77f0fc26db263d60
SHA256:	18ae415218a4f9e3db50ea20375[illegible]75ecc1ea1f23add713[illegible]ba4b8836b82b

分析结果严重性

高危	中危	信息	安全	关注
0	4	1	1	0

四大组件信息

Activity组件：1个，其中export的有：0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: 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: 2020-07-23 10:45:57+00:00
有效期至: 2050-07-23 10:45:57+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xcbc12e53cbb3a6de566b5190b124c1798805720d
哈希算法: sha256
证书MD5: f7167a7830870a1da170de7b2ce037a5
证书SHA1: 0dfdfb9dfb1aa6e44f781c841bb963ed737bd9b2
证书SHA256: 41e4410f7db13edc23499cd343e92ac9014b0c1db52490c153a2252e8ca86895
证书SHA512:
7482a368c67977beed2a3ca81ec47db42c753089a4885a2759e522c2ccbaefafffb427dde7d7adf52727e245d534e1d6f3b90a55875fac74197797814b690ce04

公钥算法: rsa
密钥长度: 4096
指纹: f506ee5db535c1900b5c23a86c656bcf4800ea42b72dd3128cb85f0c0c4b67aa
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。
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.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.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。
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.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.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。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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。

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	应用程序已使用代码签名证书进行签名

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。

安全漏洞检测

高危: 0 | 警告: 1 | 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: MST G-STORAGE-3	升级会员：解锁高级权限
2	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: MST G-STORAGE-2	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	4/30	android.permission.ACCESS_COARSE_LOCATION android.permission.READ_PHONE_STATE android.permission.CAMERA android.permission.RECORD_AUDIO
其它常用权限	6/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE com.google.android.gms.permission.AD_ID android.permission.FLASHLIGHT android.permission.ACCESS_NETWORK_STATE

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
sistema1.alltrack.com.ar	安全	否	**IP地址:** 34.134.16.27 **国家:** 美利坚合众国 **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
www.santarosa.gob.ar	安全	否	**IP地址:** 181.14.207.101 **国家:** 阿根廷 **地区:** 拉潘帕 **城市:** 圣罗莎 **纬度:** -36.616734 **经度:** -64.283424 **查看:** Google 地图
www.alltrack.com.ar	安全	否	**IP地址:** 34.134.16.27 **国家:** 美利坚合众国 **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

URL链接分析

URL信息	源码文件
• https://www.santarosa.gob.ar/	ar/com/alltrack/santarosacolectivos/BaseActivity.java
• https://plus.google.com/ • https://sistema1.alltrack.com.ar/ • https://www.santarosa.gob.ar/ • http://www.alltrack.com.ar/app/terminos_condiciones_santa_rosa.html	自研引擎-S

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。
Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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 Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

密钥凭证

可能的密钥
凭证信息=> "com.google.android.geo.API_KEY" : "@string/google_maps_key"
"google_maps_key" : "AIzaSyDJBa22nhRjLNN5RSfHPxKa-lCPfcGnmxA"

GooglePlay应用信息

标题: Emtu Lugar

评分: 3.29 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 地图和导航 **Play Store URL:** ar.com.alltrack.santarosa.colectivos

开发者信息: Alltrack, Alltrack, None, http://www.alltrack.com.ar, info@alltrack.com.ar,

发布日期: None **隐私政策:** Privacy link

关于此应用:

Transporte Urbano Santa Rosa是该市公共交通的官方应用程序，可以帮助您更轻松，更可靠地移动。 它具有有关公共汽车路线，线路和公共汽车站以及每辆公共汽车实时位置的最新信息。

免责声明及风险提示: