



ANDROID 静态分析报告



📱 SportSmart • v0.1.13

分析日期: 2025-11-21 19:51:54

i应用概览

文件名称:	SportSmart v0.113.apk
文件大小:	13.27MB
应用名称:	SportSmart
软件包名:	org.podiumanalytics.podium
主活动:	org.podiumanalytics.podium.MainActivity
版本号:	0.113
最小SDK:	28
目标SDK:	35
加固信息:	未加壳
开发框架:	Cordova
应用程序安全分数:	60/100 (低风险)
杀软检测:	2 个杀毒软件报毒
MD5:	d276acc08754faeb71778e265973832e
SHA1:	1846915372c8c73adfeb2f424e6c41b2607d4578
SHA256:	ee5353757e1e2da477b5f52ff6e0b12a1d8c8b82eba4f655a571f57aa7bc2851

📊分析结果严重性分布

🚨 高危	⚠️ 中危	🔍 低危	✅ 安全	🔔 关注
0	6	1	1	0

📦四大组件导出状态统计

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: 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

APK已签名
v1 签名: False
v2 签名: False

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: 2021-03-15 12:44:41+00:00
有效期至: 2051-03-15 12:44:41+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0x20aa79da095b182262e7f4cfb69746a17cd8d13d
哈希算法: sha256
证书MD5: a03be5c477e4643984155874fa5c70ac
证书SHA1: 1ec82fccd3ce3ed978da7147fc1771c8a48aa2d9
证书SHA256: 1841e3ad3f50cadcd6864cb07c364110899aafa0a2a1f37ecc1e8ba31c405b35
证书SHA512:
7b725e50c95f4d4fb56a938e7d36d3af642cd023d979020ef26a0e48703e22e1b53d46446b7a198a54286478722c6a82a8d1ab6a1aebb2683db9d5b6a16e2cd6

公钥算法: rsa
密钥长度: 4096
指纹: 9d0addf159c13d5625f9d92ec17e587582d1194713d2fd3ea4a5a461570dda89
共检测到 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_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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.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.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.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.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。
org.podiumanalytics.podium.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
org.podiumanalytics.podium.MainActivity	Schemes: org.podiumanalytics.podium://, Hosts: podiumanalytics.outsystemsenterprise.com,

网络通信安全风险分析

序号	范围	严重级别	描述
----	----	------	----

证书安全分析

高危: 0 | 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: 2 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用已配置网络安全策略 [android:networkSecurityCo nfig=@7F100004]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。 可针对特定域名或应用范围进行灵活配置。
2	应用数据存在泄露风险 未设置[android:allowBackup] 标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。
3	Broadcast Receiver (android x.profileinstaller.ProfileInstal lReceiver) 受权限保护，但应 检查权限保护级别。 Permission: android.permis sion.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义 处检查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互； 若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: 0 | 警告: 4 | 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	应用程序创建临时文件。敏感信息永远不应该被写入临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: In secure 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

5	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: In sufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
---	----------------------------------	----	--	-----------------------------

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频	升级会员：解锁高级权限
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
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
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00028	从assets目录中读取文件	文件	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	4/30	android.permission.RECORD_AUDIO android.permission.VIBRATE android.permission.CAMERA android.permission.MODIFY_AUDIO_SETTINGS
其它常用权限	4/4	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE 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。

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。
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。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

► Google Play 应用市场信息

标题: SportSmart

评分: None 安装: 100+ 价格: 0 Android版本支持: 分类: 体育 Play Store URL: [org.podiumanalytics.podium](https://play.google.com/store/apps/details?id=com.podiumanalytics.sportsmart)

开发者信息: Podium Analytics, Podium+Analytics, None, <https://podiumanalytics.org/>, info@podiumanalytics.org.

发布日期: None 隐私政策: [Privacy link](#)

关于此应用:

SportSmart 是一款报告受伤情况的应用程序，由慈善机构 Podium Analytics 免费提供给所有学校和俱乐部。

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成