



ANDROID 静态分析报告



Downloader • 1.10.2

分析日期: 2024-02-19 22:00:12

i应用概览

文件名称:	a2e29b8987ec0874f336594163d92bd34f673c79ea8a1586c9bc6e4393cb7ea6.apk
文件大小:	0.58MB
应用名称:	Downloader
软件包名:	com.tuneonn.Ayurveda
主活动:	not_found_main_activity!!
版本号:	10.2
最小SDK:	11
目标SDK:	22
加固信息:	未加壳
应用程序安全分数:	47/100 (中风险)
跟踪器检测:	1/432
杀软检测:	31 个杀毒软件报毒
MD5:	ca439671e13f0db3c99b568d3f7eab26
SHA1:	35d2e78de68b89843091b9547126b797fffacacf
SHA256:	a2e29b8987ec0874f336594163d92bd34f673c79ea8a1586c9bc6e4393cb7ea6

📊分析结果严重性分布

🔴 高危	🟡 中危	📘 信息	🟢 安全	🔍 关注
2	1	0	1	0

📦四大组件导出状态统计

Activity组件: 52个, 其中export的有: 1个
Service组件: 4个, 其中export的有: 0个
Receiver组件: 4个, 其中export的有: 4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
v4 签名: False
主题: C=Unknown, ST=XC, L=CX, O=Unknown, OU=Unknown, CN=Unknown
签名算法: dsa
有效期自: 2016-10-06 10:52:33+00:00
有效期至: 2044-02-22 10:52:33+00:00
发行人: C=Unknown, ST=XC, L=CX, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x5cf4ed2
哈希算法: sha1
证书MD5: 1a9cf3a6c7d1ae7f9df6ac4b61c4f5f7
证书SHA1: c1efdb6367d79c15fcfe8452a0d341991076552a
证书SHA256: 1432936f6dff74de250cffcaefbdf0563e145f4b6786c2a112b2419f4fbb8dc1
证书SHA512:
94b1cfccc0f1ffb39e20779a9a48d9096401c66d0508f3c079610b5c13f818c7a44c89be538c10030681e03216060b9ae52d0c31d60d48513689e6f30f293e

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_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.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。

网络通信安全风险分析

序号	范围	严重程度	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: 1 | 警告: 6 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
----	----	------	------

1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 3.0, [minSdk=11]	警告	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	Activity (am.xtrack.SoloActivity) 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。
3	Activity-Alias (am.xtrack.LolalaActivity\$a) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias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-Alias是显式导出的。
4	Broadcast Receiver (am.xtrack.StereoReceiver) 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, 因此使其对设备上的任何其他应用程序都可访问。
5	Broadcast Receiver (am.xtrack.Metrica) 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, 因此使其对设备上的任何其他应用程序都可访问。
6	Broadcast Receiver (am.xtrack.Analytics) 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, 因此使其对设备上的任何其他应用程序都可访问。
7	Broadcast Receiver (com.startapp.android.publish.common.metaData.BootCompleteListener) 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Broadcast Receiver是显式导出的。

代码安全漏洞检测

高危: 0 | 警告: 3 | 信息: 0 | 安全: 1 | 屏蔽: 0

序号	问题	等级	参考标准	文件位置
1	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-112: 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
2	此应用没有使用SSL Pinning 来检测或防止发生在通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
3	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

4	SHA-1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: In sufficient Cryptograp hy OWASP MASVS: MSTG -CRYPTO-4	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	0/30	
其它常用权限	3/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_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
bbsec.enconfhz.com	安全	否	IP地址: 5.149.249.226 国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980 查看: Google 地图
googl p μ.com	安全	否	No Geolocation information available.
api.mobengine.xyz	安全	否	IP地址: 213.196.46.117 国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980 查看: Google 地图

URL 链接安全分析

URL信息	源码文件
• http://bbsec.enconfhz.com/	am/xtrack/BuildConfig.java
• http://googl P μ.com	model_/networking/Common.java
• http://api.mobengine.xyz	model_/networking/Static.java

- file:///android_asset - http://localhost/ - http://googleplay.com - http://bbsec.enconfhz.com/ - javascript:window.HTMLLOUT.processHTML(document.getElementsByTagName('body')) - http://api.mobengine.xyz	自研引擎分析结果
---	----------

第三方追踪器检测

名称	类别	网址
MobFox	Analytics, Profiling, Advertisement	https://reports.exodus-privacy.eu.org/trackers/185

Google Play 应用市场信息

标题: Ayurvedic Treatments(Ayurveda)

评分: 4.15873 安装: 1,000,000+ 价格: 0 Android版本支持: 分类: 健康与健身 Play Store URL: [com.tuneonn.Ayurveda](https://play.google.com/store/apps/details?id=com.tuneonn.Ayurveda)

开发者信息: Tuneonn Inc., Tuneonn+Inc., None, <http://appstoday.in>, tuneonn@gmail.com,

发布日期: 2014年9月16日 隐私政策: [Privacy link](#)

关于此应用:

The ayurvedic way is the best way to heal. This application contains several ayurvedic therapy, tips, treatment and medicine in hindi. So, all of you who trust in the power of nature, install the app right now. More than a mere system of treating illness, Ayurveda is a science of life (Ayur = life, Veda = science or knowledge). It offers a body of wisdom designed to help people stay vital while realizing their full human potential. 'Ayurveda' is generally understood as 'Science of life' translating 'Ayuh (r)' as life and 'Veda' as science. Ayurveda is an ancient system of life and also the oldest surviving medical system in the world The Ayurvedic Healing Village provides an overview of the Ayurvedic Treatments, Medicinal Massage, Ayurvedic spa and Herbal Remedies. Ayurvedic treatment is one of the most popular and ancient way of treating your body. Know these 16 natural treatments to get rid of various body disorders. It is best if you opt for natural methods. In this article, we have listed a few effective diet tips and a diet plan that can help you gain weight. Consume foods that help you gain weight: There are natural foods which make you gain weight in a healthy manner. Including foods rich in healthy fat content is a must. You can include fish like tuna and salmon, natural fruit juices, whole wheat breads and Indian flat breads. Weight Loss Tips That Are Actually Evidence-Based. Drink Water, Especially Before Meals. It is often claimed that drinking water can help with weight loss, and this is true. Eat Eggs For Breakfast. Drink Coffee (Preferably Black) Drink Green Tea. Cook With Coconut Oil. When it comes to losing weight, we have been told time and again to eat right and exercise regularly. Experts have come up with some simple yet effective weight loss tips which can help you shed those extra pounds the healthy way. 10 Simple All Natural Beauty Tips. Banana and Egg Hair Treatment. Looking for a little more shine in your hair? Moisturizing Nail Treatment. Simple Honey Face Mask. Apple Cider Vinegar Clarifying Shampoo. Elbow and Knee Exfoliate and Skin Brightener. Gentle Body Scrub. Easy Deep Conditioning Hair Treatment. All Natural Beauty Tips For Any Skin Type. Eliminate Tired Puffy Eyes With Chilled Tea Bags. Use Raspberries And Coconut Oil For Brighter Lips. Get A Natural Face Lift With Simple Yoga Poses. Get Soft, Kissable Skin With A Natural Pomegranate, Raspberry, and Sweet Almond Oil Blend. Alternative ayurvedic treatment of cancer, tumours, multiple sclerosis, infantile paralysis and psoriasis. Ayurveda treatment cope with all diseases. Read more about disease management in Ayurveda, Ayurvedic treatment and Herbs. this app in hindi gives you all information on Ayurvedic Diseases which is a wholistic system of medicine from India. App includes - ■■■■ ■■■■ ■■■■ | Diseases treatments from ayurveda therapy ■■■■ ■■■■ ■■■■ | healthy lifestyle by ayurved ■■■■ ■■■■ ■■■■ | Ayurvedic medicine ■■■■ ■■■■ ■■■■ | beauty tips by a ayurved ■■■■ ■■■■ ■■■■ | Sexual disorders and issues ■■■■ ■■■■ | Sugar ■■■■ | kidney stone treatment A-Z ■■■■ ■■■■ | all diseases caused and treatments ■■■■ ■■■■ | constipation treatments ■■■■ (■■■■■■■■■■) ■■■■ | gas acidity treatment ■■■■ ■■■■ (■■■■■■■■■■) | foot orthosis ■■■■ ■■■■ ■■■■ | hormones therapy ■■■■ ■■■■ ■■■■ | vitamin therapy in hindi. ■■■■ ■■■■ | weight gain tips ■■■■ ■■■■ | weight loss tips in hindi ■■■■ ■■■■ | Thyroid disease in hindi Disease and ayurvedic treatment. Healthy life. Ayurvedic medicine. Natural beauty therapy. Ayurved Living and stay healthy.

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