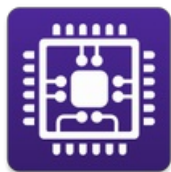




ANDROID 静态分析报告



CPU-Z • v1.51

分析日期: 2025-07-07 09:04:14

i应用概览

文件名称:	CPU-Z v1.51 专业版.apk
文件大小:	5.96MB
应用名称:	CPU-Z
软件包名:	com.cpuid.cpu_z
主活动:	com.cpuid.cpu_z.MainActivity
版本号:	1.51
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	42/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	9a8b5f12fcdac204d387966fbd6c1f14
SHA1:	88647aecd2606b3f2ee95e17ec215208e9f492ba
SHA256:	e7a1ce8a2c6f7f5878d9e3a6e2e4f08320e1126e6c8aefcfbab5e24c40157fb

分析结果严重性分布

高危	中危	信息	安全	关注
3	6	1	1	0

四大组件导出状态统计

Activity组件: 4个, 其中export的有: 0个
Service组件: 4个, 其中export的有: 1个
Receiver组件: 8个, 其中export的有: 1个

Provider组件: 1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: True

v3 签名: True

v4 签名: None

主题: C=IN

签名算法: rsassa_pkcs1v15

有效期自: 2020-11-01 10:49:08+00:00

有效期至: 2045-10-26 10:49:08+00:00

发行人: C=IN

序列号: 0x47723c30

哈希算法: sha1

证书MD5: 0ea9ea7bd967b60eff29ab7746d8bfbcb

证书SHA1: 2412f88ac73778c3d659d47a3112e27898f953b9

证书SHA256: 3b61c2a82aff9f7652ffe0b04be3c8f248b5e1aa7063f1a3846f0cf5c778628a

证书SHA512: 1c077d27a069939e563a8e959aeb767231a94eb6f2a9e7cbcb1538f095956000586ffab52ab2a990b447e34bfbfb8995f035eecd2430f99f16d1ce9160d275fa2

公钥算法: rsa

密钥长度: 1024

指纹: 74b4db306b8cd921cbfac0e876ef0a9a8574cb987da1221aa430bd56dc1d8301

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.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。
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。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）

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: 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: 3 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
2	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 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。
3	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.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: 3 | 警告: 1 | 信息: 1 | 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
2	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

3	默认情况下，调用Cipher.getInstance("AES")将返回AES ECB模式。众所周知，ECB模式很弱，因为它导致相同明文块的密文相同	高危	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-2	升级会员：解锁高级权限
4	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
5	该文件是World Writable。任何应用程序都可以写入文件	高危	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
6	该文件是World Readable。任何应用程序都可以读取文件	高危	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH (指定SO搜索路径)	RUNPATH (指定SO搜索路径)	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED (裁剪符号表)
----	-----	------------	-----	-------------------	-------	------------------	--------------------	-------------------	--------------------------

1	arm64-v8a/libcpuid.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 (ROP) 攻击更难可靠地执行。	False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项 -fstack-protector-all 来启用栈哨兵。这对于 Dart/Futter 库不适用，除非使用了 Dart FFI	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT (.got 和 .got.plt 两者) 被标记为只读。	N o n e i n f o 二进制文件没有设置运行时的搜索路径或 RPATH	N o n e i n f o 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数 (如 strcpy, gets 等) 的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Futter 库不适用	Tr u e i n f o 符号被剥离
---	-----------------------	---	--	---	--	--	---	---	--

应用行为分析

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
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
00036	从 res/raw 目录获取资源文件	反射	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
00013	读取文件并将其放入流中	文件	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
00012	读取数据并放入缓冲流	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	2/30	android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED
其它常用权限	3/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.FOREGROUND_SERVICE

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
valid.x86.fr	安全	否	IP地址: 195.154.28.169 国家: 法国 地区: 法兰西岛 城市: 巴黎 纬度: 48.859077 经度: 2.293486 查看: Google 地图
liteapks.com	安全	否	IP地址: 104.26.15.148 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
www.cpuid.com	安全	否	IP地址: 195.154.81.43 国家: 法国 地区: 法兰西岛 城市: 巴黎 纬度: 48.859077 经度: 2.293486 查看: Google 地图

🌐 URL 链接安全分析

URL信息	源码文件
https://liteapks.com/app.html	p000/p001/iab.java
- https://www.cpuid.com/ - https://valid.x86.fr/ - https://www.cpuid.com/software/cpu-z-android.html#faq	com/cpuid/cpu_z/Page_about.java
- https://valid.x86.fr/android.php - https://valid.x86.fr/a/	com/cpuid/cpu_z/Validation.java
https://valid.x86.fr/api/ainfo/	com/cpuid/cpuidsdk/JsonParser.java

• https://liteapks.com/app.html	p000/p001/iaw.java
---	--------------------

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
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。
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。开发人员 and 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 WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
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。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获得更强健的数据库访问机制。

✉ 邮箱地址敏感信息提取

EMAIL	源码文件
cpuz@cpuid.com	com/cpuid/cpu_z/MainActivity.java

第三方追踪器检测

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

🔑 敏感凭证泄露检测

可能的密钥
dR5Vx2mOx4GqCEi6Mx84jGeMEe5c38m7jWIajevG8I=
C+CgTFGA66yt4jXPEiIrxijxRU684sjgn/WncvVJPbMrHBQ+f0eE2Yjbl2IFh+z1GoVPWhNcQbF212Tdup4AeRX70kGPQJyuxeFb6Wtjzqs=
BHoKAJ0BAR2DLOvQkDvRcNLeeqqgqHLCqKMR1JfyXapo=
bKxCjRf2+J6gvv7C0fr4tYEBkjGR5dmbwzKykxOB8Fo=

Google Play 应用市场信息

标题: CPU-Z

评分: 3.8555093 安装: 100,000,000+ 价格: 0 **Android**版本支持: 分类: 工具 **Play Store URL:** [com.cpuidee.cpuspeedtest](https://play.google.com/store/apps/details?id=com.cpuidee.cpuspeedtest)

开发者信息: CPUID, CPUID, None, <https://www.cpuidee.com>, dev.cpuidee@gmail.com,

发布日期: 2013年6月13日 隐私政策: [Privacy link](#)

关于此应用:

流行的CPU识别工具，用于PC的Android版本，CPU-Z是一款免费的应用程序，报告有关设备的信息。 - 的SoC（片上系统）的名称，架构，时钟速度为每个核心; - 系统信息：设备品牌型号，屏幕分辨率，内存，存储; - 电池信息：等级，状态，温度，容量; - 传感器。要求： - Android 2.2及以上（版本1.03和+） 权限： - INTERNET许可，才能进行联机验证（见下面的注意事项了解更多详细的验证过程） - ACCESS_NETWORK_STATE统计。 注意事项：在线验证（1.04版和+） 验证允许存储你的Android设备的硬件规格在数据库中。确认后，程序会打开你的验证网址到您当前的互联网浏览器。如果您输入您的电子邮件地址（可选），电子邮件与你的验证链接将被发送到你作为一个提醒。 设置屏幕和调试（版本1.03和+） 如果CPU-Z异常关闭（在案件的bug），设置屏幕会出现在下次运行。您可以使用该屏幕来删除该应用程序的主要功能检测，并使其运行。 错误报告 在情况下的bug，请打开应用程序菜单，然后选择“发送调试的相关信息”发送报告通过电子邮件 常见问题和故障排除 <http://www.cpuidee.com/softwares/cpu-z-android.html#faq>: 您可以在该地址访问常见问题解答

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