南明离火
移动应用检测平台

ANDROID 静态分析报告

深圳天气 • v6.2.1

分析日期: 2024-06-15 18:52:28

应用概览

文件名称:	com.sz.china.weather_6.2.1.apk
文件大小:	14.67MB
应用名称:	深圳天气
软件包名:	com.sz.china.weather
主活动:	com.sz.china.mycityweather.ui.activity.WelcomeActivity
版本号:	6.2.1
最小SDK:	24
目标SDK:	33
加固信息:	未加壳
应用程序安全分数:	55/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	743699dc9f310c4b239754c5147b3119
SHA1:	d2938747fad7d5c00810fe8a848a7410f5ae9058
SHA256:	719928b8283585a2768f1b45133d1cf1c54022a0f0a8c4207a64f1ff78c9efab

分析结果严重性分布

高危	中危	信息	安全	关注
1	2	10	1	0

四大组件导出状态统计

Activity组件：25个，其中export的有：0个
Service组件：3个，其中export的有：0个
Receiver组件：0个，其中export的有：0个
Provider组件：2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: True

本报告由南明离火移动安全分析平台生成

v3 签名: True
v4 签名: False
主题: C=86, ST=yby, L=shenzhen, O=Shenzhen China meteorological, OU=Shenzhen China meteorological, CN=chs
签名算法: rsassa_pkcs1v15
有效期自: 2011-08-05 07:01:17+00:00
有效期至: 2036-07-29 07:01:17+00:00
发行人: C=86, ST=yby, L=shenzhen, O=Shenzhen China meteorological, OU=Shenzhen China meteorological, CN=chs
序列号: 0x4e3b953d
哈希算法: sha1
证书MD5: 1116c0fbb17bea368f395cd8aff2e960
证书SHA1: 0581f9579624c77d32814d09aafa025a901af788
证书SHA256: 74f0564088ed3e1635c1134667111fd126fca077652951a8cca6d5e0dc48badf
证书SHA512:
9459149c5ba6656fff43a2f817b4da707b0c38e18be577e99cf62b64c792c2569888d0f6273b5e50ef00b30c57f5f64abe5d7e59142c707012d0979a1332aa1b

公钥算法: rsa
密钥长度: 1024
指纹: 10424fa3ebcd029c41a07a24b0ce75fa8a20d622daeaa6e217520868f700b5b1
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.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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
com.android.launcher.permission.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
android.permission.BROADCAST_STICKY	普通	发送置顶广播	允许应用程序发送顽固广播，这些广播在结束后仍会保留。恶意应用程序可能会借此使手机耗用太多内存，从而降低其速度或稳定性。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
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错略的经纬度信息，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.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
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.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
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_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
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）

android.permission.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
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。

网络通信安全风险分析

高危: **1** | 警告: **0** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

证书安全合规分析

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 配置安全分析

高危: **0** | 警告: **1** | 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 7.0, [minSdk=24]	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	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
3	高优先级的Intent (1000) [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

代码安全漏洞检测

序号	问题	等级	参考标准	文件位置

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/libobjectbox-jni.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。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk', '__memcpy_chk', '__read_chk', '__vsnprintf_chk', '__memmove_chk', '__vsprintf_chk']	False warning 符号可用
2	arm64-v8a/libsecidea2.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。		True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	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。	None info 二进制文件没有设置运行时搜索路径或RPATH	None info 二进制文件没有设置RUNPATH	True info 二进制文件有以下加固函数: ['old_read_chk']	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限

恶意软件常用权限	7/30	android.permission.WAKE_LOCK android.permission.RECEIVE_BOOT_COMPLETED android.permission.GET_TASKS android.permission.REQUEST_INSTALL_PACKAGES android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.READ_PHONE_STATE
其它常用权限	7/46	android.permission.BROADCAST_STICKY android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.INTERNET android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.FOREGROUND_SERVICE android.permission.ACCESS_BACKGROUND_LOCATION

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
objectbox.io	安全	否	**IP地址:** 85.13.163.69 **国家:** 德国 **地区:** 图林根 **城市:** 弗里德斯多夫 **纬度:** 50.604919 **经度:** 11.035770 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://api.weibo.com/oauth2/authorize	自研引擎-A
• https://objectbox.io/sync/	lib/arm64-v8a/libobjectbox-jni.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
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。

本报告由南明离火移动安全分析平台生成

敏感凭证泄露检测

可能的密钥
高德地图的=> "com.amap.api.v2.apikey" : "299bcd6327f523aae0e02d97be729a42"
凭证信息=> "TA_APPKEY" : "AB8VCJEF333J"

免责声明及风险提示: