南明离火
移动应用检测平台

ANDROID 静态分析报告

无线可控水浴锅自动加水及温度调节系统 • v7.0

分析日期: 2024-04-01 17:55:38

应用概览

文件名称:	无线可控水浴锅加水系统.apk
文件大小:	0.73MB
应用名称:	无线可控水浴锅自动加水及温度调节系统
软件包名:	com.ESP8266
主活动:	com.e4a.runtime.android.StartActivity
版本号:	1.0
最小SDK:	17
目标SDK:	26
加固信息:	未加壳
应用程序安全分数:	45/100 (中风险)
杀软检测:	AI评估：安全
MD5:	6c72abaf1cc258cbc285f80a40774c18
SHA1:	d76c2721648b491bf1ad37fbd1ea6be402cbb490
SHA256:	d3fc713a1b270f97781abc1ac3e64b5256f02df46402897d2f17050a6c49aaf0

分析结果严重性分布

高危	中危	信息	安全	关注
2	4	10	1	2

四大组件导出状态统计

Activity组件：2个，其中export的有：1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

应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: False

本报告由南明离火移动安全分析平台生成

v3 签名: False
v4 签名: False
主题: C=US, O=Android, CN=Android Debug
签名算法: rsassa_pkcs1v15
有效期自: 2023-02-08 15:33:09+00:00
有效期至: 2024-02-08 15:33:09+00:00
发行人: C=US, O=Android, CN=Android Debug
序列号: 0x7c90bc80
哈希算法: sha256
证书MD5: d9295f646b6f80e2238f2b4675a4fe50
证书SHA1: 49c524a6a49052dcc45de9180f8997bda6be52d5
证书SHA256: d9893603290e468fc458b8792b8fbc56632878e5a2665714db9e0d41b2119d17
证书SHA512:
718d9ba4e30e77b5e3ea58132a2f03467f874f13a73605c86995b3c366d802084a620eaf75fd3ad61cc80612f97d232b50429d9674dc5faa73c106df453c696d

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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
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。恶意应用程序可能会发现有关其他应用程序的保密信息。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android 8.0 以上系统允许安装未知来源应用程序权限。
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.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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
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.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
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.SYSTEM_OVERLAY_WINDOW	未知	未知权限	来自 android 引用的未知权限。
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）
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.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.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。

本报告由南明离火移动安全分析平台生成

android.permission.CHANGE_CONFIGURATION	危险	改变UI设置	允许应用程序 允许应用程序更改当前配置，例如语言区域或整体的字体大小。

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: **2** | 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v1/v3签名方案的应用程序也同样存在漏洞。
应用程序使用了调试证书进行签名	高危	应用程序使用了调试证书进行签名。生产环境的应用程序不能使用调试证书发布。

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	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 4.2-4.2.2, [minSdk=17]	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	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false。默认情况下它被设置为true，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。
3	Activity (com.e4a.runtime.android.mainActivity) 未被保护。 存在一个 intent-filter。	警告	发现 Activity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是显式导出的。

代码安全漏洞检测

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

序号	问题	等级	参考标准	文件位置
1	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	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	5/30	android.permission.GET_TASKS android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_PHONE_STATE android.permission.SYSTEM_ALERT_WINDOW android.permission.WAKE_LOCK
其它常用权限	7/46	android.permission.READ_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_WIFI_STATE android.permission.INTERNET android.permission.FOREGROUND_SERVICE 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
bbs.e4asoft.com	安全	是	**IP地址:** 43.248.189.45 **国家:** China **地区:** Jiangsu **城市:** Suqian **纬度:** 33.933334 **经度:** 118.283333 **查看:** 高德地图
www.123cha.com	安全	是	**IP地址:** 61.147.211.30 **国家:** China **地区:** Jiangsu **城市:** Nantong **纬度:** 32.030281 **经度:** 120.874718 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• 192.168.4.1	com/ESP8266/C0001.java
• http://www.123cha.com/ • 192.168.4.1 • http://bbs.e4asoft.com/openapi_unsafe.php • http://api.fanyi.baidu.com/api/trans/vip/translate?q= • http://bbs.e4asoft.com	自研引擎分析结果

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。

免责声明及风险提示: