南明离火
移动应用检测平台

ANDROID 静态分析报告

班班通 • v1.0.1.3432

分析日期: 2024-06-04 15:40:06

应用概览

文件名称:	app_board_v1.0.1.3432.apk
文件大小:	2.42MB
应用名称:	班班通
软件包名:	com.wmzz.board
主活动:	com.wmzz.board.MainActivity
版本号:	1.0.1.3432
最小SDK:	19
目标SDK:	27
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：可能有安全隐患
MD5:	5e53ba7a554c370fdf228f0fc741564c
SHA1:	2154d61a213a9726fc184d740a7c4246b477f1d7
SHA256:	3300595a78935d8266e0c80fd[illegible]c30a963b0b17ce5f2722059e6684d5337f9fe

分析结果严重性分布

高危	中危	信息	安全	关注
2	4	1	1	0

四大组件导出状态统计

Activity组件：3个，其中export的有：0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: True
v3 签名: False
v4 签名: False
主题: C=CN, ST=guangdong, L=guangzhou, O=gzwmzz, OU=gzwmzz, CN=brook.tran
签名算法: rsassa_pkcs1v15
有效期自: 2015-09-08 09:14:55+00:00
有效期至: 2043-01-24 09:14:55+00:00
发行人: C=CN, ST=guangdong, L=guangzhou, O=gzwmzz, OU=gzwmzz, CN=brook.tran
序列号: 0xcfbeb9c
哈希算法: sha256
证书MD5: 6adad9a6076e08fd6ad62972ddc5c9aa
证书SHA1: 337b139fcbfa24a6910bbda0ebac12d7c4ae23a0
证书SHA256: 7851967427dc5cfbe78a158cbb2ed909c16b295f6d6edda44a9b0e098cca4ea3
证书SHA512:
918a7f537318e3dcf4879799f1f8a8716286c247b0e7ff24132f966a8c7b1dc0727df6eefe80024f46ca8cffefa14ccb9a1c3...28fd507f8d2a24c4278212ed7a

公钥算法: rsa
密钥长度: 2048
指纹: aed36b9b2a3edb29c09dec47515a082d6df335ba96aa1580fa23af4f094a573e
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.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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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。
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

序号	范围	严重级别	描述

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: **2** | 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 4.4-4.4.4, [minSdk=19]	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	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
3	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。

代码安全漏洞检测

高危: **2** | 警告: **2** | 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	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
3	确保用户控制的URL永远不会到达Web视图。在WebView中启用从URL访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成

4	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
5	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	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	armeabi/liblbs.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	No RELRO high 此共享对象未启用 RELRO。整个 GOT（.got 和 .got.plt）都是可写的。如果没有此编译器标志，全局变量上的缓冲区溢出可能会覆盖 GOT 条目。使用选项 -z,relro,-z,now 启用完整 RELRO，仅使用 -z,relro 启用部分 RELRO。	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	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/Flutter 不适用	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	6/30	android.permission.VIBRATE android.permission.CAMERA android.permission.REQUEST_INSTALL_PACKAGES android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.READ_PHONE_STATE
其它常用权限	3/46	android.permission.INTERNET android.permission.FLASHLIGHT 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。

URL 链接安全分析

URL信息	源码文件

• http://banbantong.wm3dao.com • http://shop.wmketang.com/?r=shop/app/update • https://gist.github.com/triceam/4658021 • https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE • http://jsperf.com/b64tests • http://brianleroux.github.com/lawnchair/ • https://bbt.gdedu.gov.cn • http://sizzlejs.com/ • http://www.iana.org/assignments/character-sets	自研引擎-A

第三方 SDK 组件分析

SDK名称	开发者	描述信息
腾讯浏览服务（TBS）	Tencent	腾讯浏览服务，依托 X5 内核强大的能力，致力于提供优化移动端浏览体验的整套解决方案。
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:

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。