南明离火
移动应用检测平台

ANDROID 静态分析报告

PITS • v6.4

分析日期: 2024-07-19 10:58:38

应用概览

文件名称:	MCSS_HN-universal-release.apk
文件大小:	23.06MB
应用名称:	PITS
软件包名:	com.ailk.appclientCloud
主活动:	com.ailk.appclientCloud.admin.Login_welcome
版本号:	6.4
最小SDK:	7
目标SDK:	7
加固信息:	未加壳
应用程序安全分数:	45/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：很危险，请谨慎安装
MD5:	4e30e5d88f2582cc00956dd6cb6a65f0
SHA1:	d3ebb499b1c716b66bc56a7341[illegible]0b1ef36
SHA256:	7437f82dd9ebba401d58a3c[illegible]ac090b536fd54acc912[illegible]b23a4d807d0b163b8

分析结果严重性分布

高危	中危	信息	安全	关注
2	20	1	0	1

四大组件导出状态统计

Activity组件：142个，其中export的有：8个
Service组件：3个，其中export的有：2个
Receiver组件：1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

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=6, ST=5, L=4, O=3, OU=2, CN=1
签名算法: rsassa_pkcs1v15
有效期自: 2022-09-26 09:53:47+00:00
有效期至: 2047-09-20 09:53:47+00:00
发行人: C=6, ST=5, L=4, O=3, OU=2, CN=1
序列号: 0x4b5e6ba3
哈希算法: sha256
证书MD5: 8a69f227da8cd11a066377c2ed7e10d6
证书SHA1: 3ae45904a85b2976f18cbb1fa05532ec24bad392
证书SHA256: c9e077b3c0c20e993a9970c1613c1f04cb7edc7495ed3cb4950ba4ec5e007288
证书SHA512:
d26c9e8f09e0d7a43697515340376d4a49c5e43fcf03c0a65e71a0b5e4066386ab4b1a49086da28d7839c5227d899a34d0e87ec5[illegible]df1b5558dce2180da449861

公钥算法: rsa
密钥长度: 2048
指纹: 56b451824c4c197329bb70e508483a3122b4988ff48cb9e16fe983bb89fbf518
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.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.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。
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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi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.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.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.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.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.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。

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_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
android.permission.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.ailk.appclientCloud.admin.Login_welcome	Schemes: com.ailkCloud://, Hosts: service.welcome,
com.ailk.appclientCloud.admin.LoginActivity	Schemes: jtmcss-mobile://,

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: **1** | 警告: **12** | 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 XX, [minSdk=7]	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	Service (com.ailk.appclientCloud.service.MessageService) 未被保护。 存在一个intent-filter。	警告	发现 Service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Service是显式导出的。
4	Activity (com.ailk.appclientCloud.admin.Login_welcome) is vulnerable to StrandHogg 2.0	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (7) 更新到 29 或更高版本以在平台级别修复此问题。
5	Activity (com.ailk.appclientCloud.admin.LoginActivity) 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。
6	Activity (com.ailk.appclientCloud.admin.MainHomeActivity) 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。
7	Activity (com.ailk.appclientCloud.admin.MainMenuActivity) 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。
8	Activity (com.ailk.appclientCloud.admin.Main_more) 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。
9	Activity (com.ailk.appclientCloud.admin.SearchActivity) 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。
10	Activity (com.ailk.appclientCloud.activity.home.QueryCommonActivity) 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。
11	Activity (com.ailk.appclientCloud.activity.grid.GridMsgMainActivity) 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。
12	Activity (com.ailk.appclientCloud.activity.home.ManagerMainActivity) 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。
13	Service (com.ailk.appclientCloud.service.NotificationService) 未被保护。 存在一个intent-filter。	警告	发现 Service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Service是显式导出的。
14	Broadcast Receiver (com.ailk.appclientCloud.broadcast.UpdateMessageBroad) 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。

本报告由南明离火移动安全分析平台生成

代码安全漏洞检测

高危: **1** | 警告: **7** | 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	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
3	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
4	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	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
5	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-312: 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
6	使用弱加密算法	高危	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
7	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
8	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

9	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

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/libmmkvmapv320.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 库不适用	False warning 符号可用

2	armeabi/libmp3lame.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	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 库不适用	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	13/30	android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.READ_PHONE_STATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.CAMERA android.permission.VIBRATE android.permission.RECEIVE_SMS android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.CALL_PHONE android.permission.SEND_SMS
其它常用权限	6/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS

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

lame.sf.net	安全	否	**IP地址:** 104.18.20.237 **国家:** 美利坚合众国 **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
it.telecomjs.com	安全	是	**IP地址:** 61.147.19.61 **国家:** 中国 **地区:** 江苏 **城市:** 徐州 **纬度:** 34.266666 **经度:** 117.166664 **查看:** 高德地图
www.418log.org	安全	否	No Geolocation information available.

URL 链接安全分析

URL信息	源码文件

• http://dbushell.com/ • http://trirand.com/blog/ • http://php.net/manual/en/function.date.php • http://www.SuperSlide2.com/TouchSlide/ • http://datatables.net/license_bsd • https://bugzilla.mozilla.org/show_bug.cgi?id=649285 • http://omnipotent.net/jquery.sparkline/ • https://github.com/jzaefferer/jquery-validation • http://datatables.net/plug-ins/pagination • https://support.microsoft.com/kb/2856746 • https://github.com/vitalets/x-editable/issues/37 • http://twitter.github.com/bootstrap/javascript.html • http://jsperf.com/getall-vs-sizzle/2 • http://jdewit.github.com/bootstrap-timepicker • http://rocha.la • http://lihongxun945.github.io/jquery-weui/ • http://www.eyecon.ro/bootstrap-colorpicker • http://jqueryui.com • http://www.jacklmoore.com/autosize • http://benalman.com/projects/jquery-resize-plugin/ • https://github.com/jrburke/requirejs/wiki/Updating-existing-libraries • https://github.com/harvesthq/chosen/blob/master/LICENSE.md • http://bootboxjs.com/license.txt • http://benalman.com/about/license/ • http://github.com/vitalets/x-editable • http://datatables.net/license_gpl2 • http://www.SuperSlide2.com/ • http://hammerjs.github.io/ • http://www.malot.fr/bootstrap-datetimepicker • http://jsperf.com/thor-indexof-vs-for/5 • http://it.telecomjs.com:8080/app/uploadHttpServlet • https://bugzilla.mozilla.org/show_bug.cgi?id=491668 • http://blindsignals.com/index.php/2009/07/jquery-delay/ • http://www.iana.org/assignments/character-sets • http://sizzlejs.com/ • http://digitalbush.com/projects/masked-input-plugin/ • http://www.baidu.com • http://sam.zoy.org/wtfpl/ • http://arshaw.com/fullcalendar/ • http://jsperf.com/b64tests • http://www.jacklmoore.com/colorbox • http://unicode.org/reports/tr35/tr35-4.html	自研引擎-A
• http://137.32.180.175:30432/odsmsportlet/ • 132.228.97.47 • http://137.32.180.175:30432/odsmsportal/ • http://137.32.180.175:30431/ • http://222.85.126.177/ • http://202.102.116.51:8080/mcss/	com/ailk/appclientCloud/tools/JsonAConUtil.java
• http://202.102.116.51:8080/appupload/	com/ailk/appclientCloud/activity/archive/MyWorkViewActivity.java
• http://202.102.116.51:8080/appupload/	com/ailk/appclientCloud/activity/archive/MarketingCaseViewActivity.java
• javascript:wade.mobile.event.menu • javascript:wade.mobile.event.search	com/wade/wademobile/basic/WadeMobileActivity.java
• 192.168.1.245	com/wade/wademobile/basic/MobileThread.java
• http://202.102.116.51/app/soft/android/v0.9.6/gis.apk • http://202.102.116.51/app/soft/android/v0.9.6/css-m.apk	com/ailk/appclientCloud/activity/download/SoftManagerActivity.java

• http://202.102.116.51:8080/mcss/soft/maplocation/v1.0/maplocation.apk	com/ailk/appclientCloud/tools/MoveProject.java
• http://www.google.com/loc/json	com/wade/wademobile/tools/GoogleApi.java
• http://www.google.com/loc/json	com/wade/wademobile/func/MobilePositionHelp.java
• http://it.telecomjs.com:8080/	com/ailk/appclientCloud/activity/WadeActivity.java
• http://202.102.116.51/app/soft/android/v0.9.6/	com/ailk/appclientCloud/activity/download/DownLoadManagerActivity.java
• http://www.418log.org/	com/ab/http/AbHttpClient.java
• http://137.32.180.175:30432/odsmsportlet/ • http://www.418log.org/ • 192.168.112.45 • http://137.32.180.175:30432/odsmsportal/ • 10.0.0.172 • http://202.102.116.51:8080/appup/upload/ • http://www.google.com/loc/json • http://202.102.116.51:8080/mcss/soft/maplocation/v1.0/maplocation.apk • 10.0.0.200 • javascript:wade.mobile.event.menu • http://202.102.116.51/app/soft/android/v0.9.6/css-m.apk • http://222.85.126.177/ • http://202.102.116.51/app/soft/android/v0.9.6/gis.apk • http://it.telecomjs.com:8080/ • 132.228.97.47 • http://cdv_exec/ • javascript:wade.mobile.event.search • http://137.32.180.175:30431/ • http://202.102.116.51/app/soft/android/v0.9.6/ • http://202.102.116.51:8080/mcss/	自研引擎-S
• http://lame.sf.net	lib/armeabi/libmp3lame.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
LAME	The LAME Project	LAME is a high quality MPEG Audio Layer III (MP3) encoder licensed under the LGPL.
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。

第三方追踪器检测

名称	类别	网址
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97

免责声明及风险提示:

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隐患。