MoGua

消防报警一体机 1.1.0.APK 分析报告

APP名称: 消防报警一体机

包名:	com.afl.machine.alarm
域名线索:	8条
URL线索:	7条
邮箱线索:	0条
分析日期:	2025年8月14日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: alarm_uat_release_1.1.0_2022_06_29_14_45.apk
文件大小: 2.68MB
MD5值: d2255ae4c94781e8857370fccb4a5987
SHA1值: a373906bfa29ed3febe6a506444c4d84297f579a
SHA256值: 84af7b7e7e9476b48de228d3c981a9c7941a2c92264502d7479b00e3b42d7138

APP 信息

App名称: 消防报警一体机
包名: com.afl.machine.alarm
主活动Activity: com.afl.lego.smoke.app.LauncherActivity
安卓版本名称: 1.1.0
安卓版本: 2

域名线索

域名	服务器信息
uat-afl-device-api.aihuishou.com	**IP**: 114.55.105.179 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
github.com	**IP**: 20.205.243.166 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
dev-afl-portal-api.aihuishou.com	**IP**: 10.193.96.4 **所属国家**: - **地区**: -

	城市: - **纬度**: 0.000000 **经度**: 0.000000
android.bugly.qq.com	**IP**: 109.244.244.35 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
astat.bugly.cros.wr.pvp.net	**IP**: 170.106.135.32 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
afl-device-api.aihuishou.com	**IP**: 223.4.222.157 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
astat.bugly.qcloud.com	**IP**: 150.109.27.253 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289670 **经度**: 103.850067
schemas.android.com	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/c.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/c.java
http://dev-afl-portal-api.aihuishou.com/	c2/b.java
http://schemas.android.com/apk/res/android	a0/h.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	w3/b.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	w3/d.java
https://afl-device-api.aihuishou.com/	o1/a.java
http://dev-afl-portal-api.aihuishou.com/	o1/a.java
https://uat-afl-device-api.aihuishou.com/	o1/a.java

邮箱线索

手机线索

签名证书

APK is signed
v1 signature: True
v2 signature: False

v3 signature: False
Found 1 unique certificates
Subject: C=021, ST=shanghai, L=shanghai, O=china, OU=ai, CN=aifenlei
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-06-02 11:04:25+00:00
Valid To: 2122-05-09 11:04:25+00:00
Issuer: C=021, ST=shanghai, L=shanghai, O=china, OU=ai, CN=aifenlei
Serial Number: 0x7b4bc1db
Hash Algorithm: sha256
md5: 51f736e88ec0d60c9cece56d9a2d3bab
sha1: 8f40f10e463f83649758fe056942b42d9c8c0483
sha256: 7e1a21d648cbbca23c83508aa3de9d386ae25781a9c44193373bcdf70de82335
sha512: 46405c551163d50dc851318ba334124dab902d7434c05b3a60c9275d1bc9f3f55278987343494e7ecd41d6f0e3c2ceb78f43ca945c192648fdb5a580e1407ef3

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.bbk.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.bbk.launcher2.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference

android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.ACCESS_WIFI_STATE	正常	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.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
com.afl.machine.alarm.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.ACCESS_NOTIFICATION_POLICY	正常		希望访问通知策略的应用程序的标记权限。
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
		允许应用程序请	

android.permission.REQUEST_INSTALL_PACKAGES	危险	求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序

应用内通信
