南明离火
移动应用检测平台

ANDROID 静态分析报告

消防实操模拟软件 - v1.0.9

分析日期: 2024-05-08 10:49:36

应用概览

文件名称:	com.yaota.subjob_1.6.9_liqucn.com.apk
文件大小:	48.31MB
应用名称:	消防实操模拟软件
软件包名:	com.yaota.subjob
主活动:	com.yaota.firecontrol.fire_control_learning.MainActivity
版本号:	1.6.9
最小SDK:	21
目标SDK:	31
加固信息:	Flutter/Dart 加固
应用程序安全分数:	52/100 (中风险)
跟踪器检测:	1/432
杀软检测:	AI评估：安全
MD5:	e635330631e48e09998daf2053b76857
SHA1:	a76987dbbb85732f1add9fc2da8122074581d9c9
SHA256:	e1439375023a423b031f77ee46af456a2257425dbe2c7f48bf800ff03b635510

分析结果严重性分布

高危	中危	信息	安全	关注
2	1	2	2	2

四大组件导出状态统计

Activity组件：10个，其中export的有：2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=中国, ST=上海, L=上海, O=彩住科技, OU= 彩住, CN= Lei Liu
签名算法: rsassa_pkcs1v15
有效期自: 2021-08-03 08:58:18+00:00
有效期至: 2120-02-26 08:58:18+00:00
发行人: C=中国, ST=上海, L=上海, O=彩住科技, OU= 彩住, CN= Lei Liu
序列号: 0x5e717b7c
哈希算法: sha256
证书MD5: aab844c2325fbe700470d65b1fa7c54c
证书SHA1: 4eb78366ac56585365443265b2b460746b6c9977
证书SHA256: 91647f651b42d037e7f904b09d54477d5afc198324faeb6dddb3339d694521c8
证书SHA512:
709b36d285cfbaa220a704d9940abb033baa63643edee14181122472d4b7e6642d91db3d97044106f179c786726dce93165399f9de782102651f9b79a15906bf

公钥算法: rsa
密钥长度: 2048
指纹: 405c4c52b92ba5d327a22fe8a5737da0bd7e8b102ea603f9cd011464d73dce33
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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取、修改或删除外部存储内容	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.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.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
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.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_MEDIA_LOCATION	危险	获取照片的地址信息	更换头像，聊天图片等图片的地址信息被读取。
com.yaota.subjob.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。

可浏览 Activity 组件分析

ACTIVITY	INTENT

本报告由南明离火移动安全分析平台生成

com.yaota.firecontrol.fire_control_learning.MainActivity	Schemes: yaotafireapp://, Hosts: firepal.cn, Paths: /id,

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: **5** | 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 5.0-5.0.2, [minSdk=21]	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	Activity设置了TaskAffinity属性 (com.jarvan.fluwx.wxapi.FluwxWXEntryActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
4	Activity设置了TaskAffinity属性 (com.yaota.sub.job.wxapi.WXEntryActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
5	Activity-Alias (com.yaota.sub.job.wxapi.WXEntryActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias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-Alias是显式导出的。
6	Activity-Alias (com.yaota.sub.job.wxapi.WXPayEntryActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity-Alias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-Alias是显式导出的。

代码安全漏洞检测

高危: **2** | 警告: **8** | 信息: **2** | 安全: **2** | 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	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
3	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
4	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
5	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
6	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
7	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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
8	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
9	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
10	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限

11	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
12	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
13	SHA-1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
14	该文件是World Writable。任何应用程序都可以写入文件	高危	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

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/libapp.so	True info 二进制文件设置了NX位，这标记着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	True info	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	Not Applicable info RELRO 检查不适用于 Flutter/Dart 二进制文件	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 info 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	3/30	android.permission.READ_PHONE_STATE android.permission.REQUEST_INSTALL_PACKAGES android.permission.VIBRATE
其它常用权限	5/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_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
astat.bugly.cros.wr.pvp.net	安全	否	**IP地址:** 170.106.118.26 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图
mobilegw.aaa.alipay.net	安全	否	No Geolocation information available.
schemas.microsoft.com	安全	否	**IP地址:** 119.28.121.133 **国家:** 美利坚合众国 **地区:** 华盛顿 **城市:** 雷德蒙 **纬度:** 47.682899 **经度:** -122.120903 **查看:** Google 地图
mobilegw-1-64.test.alipay.net	安全	否	No Geolocation information available.
h5.m.taobao.com	安全	是	**IP地址:** 119.28.121.133 **国家:** 中国 **地区:** 江苏 **城市:** 镇江 **纬度:** 32.209366 **经度:** 119.434372 **查看:** 高德地图
api.flutter.dev	安全	否	**IP地址:** 199.36.158.100 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
default.url	安全	否	No Geolocation information available.

www.amazon.com	安全	否	**IP地址:** 54.230.62.214 **国家:** 大韩民国 **地区:** 京畿道 **城市:** Icheon **纬度:** 37.279179 **经度:** 127.442421 **查看:** Google 地图
astat.bugly.qcloud.com	安全	否	**IP地址:** 119.28.121.133 **国家:** 新加坡 **地区:** 新加坡 **城市:** 新加坡 **纬度:** 1.289987 **经度:** 103.850281 **查看:** Google 地图
mobilegw.stable.alipay.net	安全	否	No Geolocation information available.
mobilegw.alipaydev.com	安全	是	**IP地址:** 110.75.132.131 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161423 **查看:** 高德地图
dashif.org	安全	否	**IP地址:** 185.199.110.153 **国家:** 美利坚合众国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图
aomedia.org	安全	否	**IP地址:** 185.199.110.153 **国家:** 美利坚合众国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• 2.0.76.4	g4/b.java
• 127.0.0.	h9/e.java
• https://render.alipay.com/p/s/i?scheme=%s	i3/b.java
• http://www.amazon.com/gp/mas/get-appstore/android/ref=mas_mx_mba_iap_dl	j4/a.java
• 4.1.9.3	ja/b.java
• https://astat.bugly.qcloud.com/rqd/async • https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	ja/d.java
• https://h.trace.qq.com/kv	ja/e.java

• 4.1.9.3	ja/h1.java
• https://mobilegw.alipay.com/mgw.htm • https://mobilegw.alipaydev.com/mgw.htm • https://mcgw.alipay.com/sdklog.do • https://loggw-exsdk.alipay.com/loggw/logupload.do • http://m.alipay.com/?action=h5quit • https://wappaygw.alipay.com/home/exterfaceassign.htm? • https://mclient.alipay.com/home/exterfaceassign.htm?	k3/a.java
• https://h5.m.taobao.com/mlapp/olist.html	l3/a.java
• https://play.google.com/store/apps/details?id=	o9/b.java
• http://dashif.org/guidelines/last-segment-number • data:cs:audiopurposecs:2007 • http://dashif.org/guidelines/trickmode • http://dashif.org/thumbnail_tile • http://dashif.org/guidelines/thumbnail_tile • file:dvb-dash:	t7/d.java
• https://github.com/baseflow/flutter-permission-handler/issues	z4/p.java
• https://mclient.alipay.com/home/exterfaceassign.htm? • http://dashif.org/thumbnail_tile • 2.0.76.4 • http://wappaygw.alipay.com/service/rest.htm • https://github.com/baseflow/flutter-permission-handler/issues • https://render.alipay.com/p/s/i?scheme=%s • file:dvb-dash: • https://h.trace.qq.com/kv • https://loggw-exsdk.alipay.com/loggw/logupload.do • http://mobilegw.stable.alipay.net/mgw.htm • http://mobilegw.aaa.alipay.net/mgw.htm • https://astat.bugly.qcloud.com/rqd/async • http://mobilegw-1-64.test.alipay.net/mgw.htm • https://mobilegw.alipaydev.com/mgw.htm • https://wappaygw.alipay.com/service/rest.htm • http://www.amazon.com/gp/mas/get-appstore/android/ref=mas_mx_mba_iap_dl • https://mclient.alipay.com/service/rest.htm • https://mclient.alipay.com/cashier/mobilepay.htm • https://developer.apple.com/streaming/emsg-id3 • http://dashif.org/guidelines/thumbnail_tile • https://mclient.alipay.com/home/exterfaceassign.htm • https://mcgw.alipay.com/sdklog.do • http://mclient.alipay.com/service/rest.htm • https://play.google.com/store/apps/details?id= • https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async • 127.0.0.1 • http://mclient.alipay.com/home/exterfaceassign.htm • https://default.url • http://dashif.org/guidelines/last-segment-number • https://mobilegw.alipay.com/mgw.htm • data:cs:audiopurposecs:2007 • http://m.alipay.com/?action=h5quit • https://aomedia.org/emsg/id3 • https://wappaygw.alipay.com/home/exterfaceassign.htm? • https://h5.m.taobao.com/mlapp/olist.html • http://mclient.alipay.com/cashier/mobilepay.htm • 4.1.9.3 • http://dashif.org/guidelines/trickmode	自研引擎-S
• https://api.flutter.dev/flutter/material/scaffold/of.html	lib/arm64-v8a/libapp.so

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Flutter	Google	Flutter 是谷歌的移动 UI 框架，可以快速在 iOS 和 Android 上构建高质量的原生用户界面。
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。
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
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。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

第三方追踪器检测

名称	类别	网址
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

敏感凭证泄露检测

可能的密钥
e6b1bdcb890370f2f2419fe06d0fdf7628ad0083a52da1efe991164711bbf9297e753b3de96f1740695d07610567b1240549af9cbd87d06919ac31c859ad37ab6907c311b4756e1e208775989a4f691bff4b0bc81744d2a96b1d0d970a051140d7ee57dfc33b1bafaf6e0d820e838427018b6435f903df04ba7fd34d73f843df9434b164e0220baabb10c8978c3f4c6b7da79d8220a968356d15090da107a9606f665cbec14d218dd3d691cce2866a58840971b6a57b76af88b1a65ffdffd2c080281a6ab20be5879e0330eb7f70871de684e7174ada5dc3166461975a0796b17ce7beca83cf34f65976d237aee993db48d34a4e344f4d8b7e99119168bdd7
b6cbad6cbd5ed0d209afc69ad3b7a617efaae9b3c47eabe0be4d024936fa78c8001b1fd74b079e5ff9690061dacfa4768e981a526b9ca77156ca36251cf2f906d105481374998a7e6e6e18f7bca98b8ed2eaf86ff402c874ccaa263053f22237858206867d210020daa38c48b20cc9dfd82b44a51aeb5db459b22794e2d649
16a09e667f3bcc908b2fb1366ea957d3e3ade1751275099da2f590b0667322a
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
e2719d58-a985-b3c9-781a-b030af78d3e
9a04f079-9840-4286-ab92-e65be0885f95
0136024004378801593602505

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隐患。