南明离火
移动应用检测平台

ANDROID 静态分析报告

FMG • v6.0

分析日期: 2025-08-26 17:02:42

应用概览

文件名称:	FMG v6.0.apk
文件大小:	23.84MB
应用名称:	FMG
软件包名:	it.icontact.android.pdf2ipad.irisfmg
主活动:	it.icontact.android.pdf2ipad.irisfmg.view.main.MainActivity
版本号:	6.0
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	60/100 (低风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	e147f086f77c804ad677d439457e16d9
SHA1:	3686929be8348fa9d0adcff600d81ee15e0d680
SHA256:	fe457b48d787a64e92eecf8500ca7780bde136ae3ca50308625c9bb4a0c5681

分析结果严重性分布

高危	中危	信息	安全	关注
0	6	2	1	0

四大组件导出状态统计

Activity组件：4个，其中export的有： 0个
Service组件：8个，其中export的有： 0个
Receiver组件：3个，其中export的有： 1个
Provider组件：3个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: CN=Graniti Fiandre
签名算法: rsassa_pkcs1v15
有效期自: 2016-07-06 14:55:44+00:00
有效期至: 2046-06-29 14:55:44+00:00
发行人: CN=Graniti Fiandre
序列号: 0x461cb519
哈希算法: sha256
证书MD5: 6fd50d4ba8b51de277e6068cecf30e7d
证书SHA1: 87eadf45bd2f69ccc57ee2ce80eb1ed494cbffd2
证书SHA256: a5e7c0d378f6b62099fc6a9b017b0190f6b9bb7af2c7c5c9105042989b4c256c
证书SHA512:
35d74daf474804029151b7574a5316e74f8cdcb98a8140be8986b3010b7127cb050d3f56bb186fda6a21c94bd0da71d609b088cf8f10a259074bc026abd08d4b

公钥算法: rsa
密钥长度: 2048
指纹: 983f3c9d3d6ac3247511d3866f9c0492e3317e4260c6322d9a02e47289e354cc
共检测到 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.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.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.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后台进程仍然运行。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。

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: 3 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
3	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: 0 | 警告: 1 | 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

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/libmodft2.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。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行	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	True info 二进制文件有以下加固函数: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限

00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	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	2/30	android.permission.VIBRATE android.permission.WAKE_LOCK
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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
pdfapp.xcer.it	安全	否	**IP地址:** 88.44.227.30 **国家:** 意大利 **地区:** 伦巴第大区 **城市:** 米兰 **纬度:** 45.464336 **经度:** 9.188547 **查看:** Google 地图
www.irisreg.com	安全	否	**IP地址:** 104.110.240.89 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图

granitifiandre-a5043.firebaseio.com	安全	否	**IP地址:** 35.190.39.113 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
finderapp.iris-group.it	安全	否	**IP地址:** 88.44.227.30 **国家:** 意大利 **地区:** 伦巴第大区 **城市:** 米兰 **纬度:** 45.464336 **经度:** 9.188547 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://granitifiandre-a5043.firebaseio.com • https://finderapp.iris-group.it/? • http://pdfapp.xcer.it/ • http://www.irisfmg.com • www.irisfmg.com/pdfapp • www.irisfmg.com	自研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://granitifiandre-a5043.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	Firebase远程配置URL（https://firebaseremoteconfig.googleapis.com/v1/projects/407894425822/namespaces/firebase:fetch?key=AIzaSyBTOqCX5bkXb8FxZsMcw0Krj9T6anKidzQ ） 已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
C++ 共享库	Android	在 Android 应用中运行原生代码。
Pdfium	Google	Pdfium Android binding.
Dexter	Karumi	Dexter 是一个 Android 库，它简化了运行时请求权限的过程。

Jetpack Lifecycle	Google	生命周期感知型组件可执行操作来响应另一个组件（如 Activity 和 Fragment）的生命周期状态的变化。这些组件有助于您写出更有条理且往往更精简的代码，这样的代码更易于维护。
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。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

邮箱地址敏感信息提取

EMAIL	源码文件
info@irisfmg.com	自研引擎-S

第三方追踪器检测

名称	类别	网址
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
凭证信息=> "io.fabric.ApiKey" : "0af6ffee706237c6a7a85c23b0a5b7f2499053a1"
"google_app_id" : "1:407894425822:android:cf9289f4a8f20bf8"
"google_crash_reporting_api_key" : "AIzaSyBTOqCX5bkXb8FxZsMcw0Krj9T6anKidzQ"
"google_api_key" : "AIzaSyBTOqCX5bkXb8FxZsMcw0Krj9T6anKidzQ"
"D1_APP_ID" : "3"
"firebase_database_url" : "https://granitifiandre-a5043.firebaseio.com"
5c5359a0c58e79c54800a163caec994e
03c944ca8e8743bd911bacbc0a500c1b

Google Play 应用市场信息

标题: FMG Newsstand

评分: 3.8 **安装:** 1,000+ **价格:** 0 **Android版本支持:** **分类:** 家居装修 **Play Store URL:** it.icontact.android.pdf2ipad.irisfmg

开发者信息: Floornature.com, Floornature.com, None, http://www.irisfmg.com, app@floornature.com,

发布日期: 2016年7月18日 **隐私政策:** Privacy link

关于此应用:

欢迎使用 FMG Fabbrica Marmi e Graniti 应用程序：高品质陶瓷表面的宇宙。 您是一名建筑师或设计师，正在为您的项目寻找创新、高品质的表面吗？探索 FMG Fabbrica Marmi e Graniti 应用程序，这是专为您量身定制的资源。 FMG Fabbrica Marmi e Graniti 是 Iris Ceramica 集团旗下品牌，是优质瓷器表面生产的全球领导者。该品牌的使命是在工厂环境中重新创造最稀有、最珍贵的大理石、石头和花岗岩，同时充分尊重环境。 FMG 与自然之间的深厚关系是有意识和负责任的设计的非凡灵感和反思源泉。这个应用程序是一个旨在支持和促进您的项目实现的工具，甚至可以随时离线。您可以在此应用程序中找到什么： 目录、产品和设置图像：浏览、下载和分享我们的目录和图像，以激发灵感并随时了解最新新闻和创新。 创新的搜索功能，具有实用的过滤器，可搜索、咨询和索取有关 FMG Fabbrica Marmi e Graniti 产品的信息。 我们新展览空间的虚拟游览：在我们的展厅体验身临其境的旅程，让您可以通过设备舒适地探索每一个细节。 立即下载 FMG Fabbrica Marmi e Graniti 应用程序，开始使用我们的高端陶瓷板创造非凡的项目。

免责声明及风险提示: