



ANDROID 静态分析报告



Fluent图标包 · v23.3

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2024-05-13 14:24:58

i应用概览

文件名称:	fluent_v2.3.3_downyi.com.apk
文件大小:	15.15MB
应用名称:	Fluent图标包
软件包名:	com.fluent.iconpack
主活动:	cn.ommiao.iconpacktemplate.MainActivity
版本号:	2.3.3
最小SDK:	22
目标SDK:	29
加固信息:	未加壳
应用程序安全分数:	60/100 (低风险)
杀软检测:	2 个杀毒软件报毒
MD5:	c9b23334463a85980d050c9d00b5cba8
SHA1:	55ae1089fecbba29187519a5cae394d7b5e65891
SHA256:	7b3157c9170c20ac1d00718671ba71c274f2e3fc8eab07a1d9bc5185e0dd7e04

📊 分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✓ 安全	🔍 关注
1	0	0	1	0

📦 四大组件导出状态统计

Activity组件: 7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: 0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=86, ST=ShaanXi, L=China, O=Personal, OU=Personal, CN=oMMiao
 签名算法: rsassa_pkcs1v15
 有效期自: 2019-12-10 06:24:28+00:00
 有效期至: 2044-12-03 06:24:28+00:00
 发行人: C=86, ST=ShaanXi, L=China, O=Personal, OU=Personal, CN=oMMiao
 序列号: 0x24eb04aa
 哈希算法: sha256
 证书MD5: b7a1c6386d8097fba8362e3280d5a714
 证书SHA1: 931d6d726383f768cdfc0b2def104e855c1987e7
 证书SHA256: c51a0cec2ab728ff7a162c4022604655ef30f0c498e860100e86890e98c448f6
 证书SHA512:
 fb8476d797d513328f2fedce97efb13b95dda4cd872e64fb7ebd4c7d69f5e50a758cae1477247ad36e3cdae6ba49ddd72e929f10245051be1fb59eac2b16fb

公钥算法: rsa
 密钥长度: 2048
 指纹: bc0664a03580772c26d5c904ed975110167cb0056b3714d316c997f0b0edba4e
 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.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
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	危险	完全互联网访问	允许应用程序创建网络套接字。

网络通信安全风险分析

高危: 1 | 警告: 0 | 信息: 0 | 安全: 0

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

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: 0 | 信息: 1 | 未知: 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 5.1-5.1.1, [minSdk=22]	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	应用程序具有网络安全配置 [android:networkSecurityCo nfig=@xml/network_securit y_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
---	--	----	---

</> 代码安全漏洞检测

序号	问题	等级	参考标准	文件位置
----	----	----	------	------

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	1/30	android.permission.SET_WALLPAPER
其它常用权限	2/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET

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
<ul style="list-style-type: none"> http://zhuti.xiaomi.com/detail/21beec10-13d7-4738-a77e-c951efaa746e https://fluenticonpack.carrd.co/assets/images/carrd.jpg?v=3e04bef3 https://themes.cloud.huawei.com/m/detailShare.html?ver=2.1&mp https://fluenticonpack.carrd.co/assets/images/gallery02/97148db9_original.jpg?v=3e04bef3 https://jq.qq.com/?_wv=1027&mp https://url.cloud.huawei.com/bsZYCYOng8 http://www.coolapk.com/u/2200896 https://fluenticonpack.carrd.co https://fluenticonpack.carrd.co/assets/images/gallery01/5056f33_original.jpg?v=3e04bef3 https://cdofs.oppomobile.com/cdo-activity/static/theme/detail/index.html?masterId=2156511&mp https://fluenticonpack.carrd.co 	自研引擎-A

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火移动安全分析平台自动生成