



ANDROID 静态分析报告



FFH4X • v1.0

分析日期: 2024-07-10 10:57:18

i应用概览

文件名称:	FFH4X_1.0.apk
文件大小:	9.61MB
应用名称:	FFH4X
软件包名:	com.damonmodder
主活动:	.MainActivity
版本号:	1.0
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	64/100 (低风险)
杀软检测:	5 个杀毒软件报毒
MD5:	890038dafd9397e8f61e09774e835cf9
SHA1:	026b10c861ca04f85e84918730e1ea310aab5468
SHA256:	c572610a17e2bccd06e67631c4171e65183d5765b621d95fdc937153fad07546

分析结果严重性分布

高危	中危	信息	安全	关注
0	4	0	1	0

四大组件导出状态统计

Activity组件: 2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: True

v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccb6b34ec4233f5f640703581053abfea303977272d17958704d89b1711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
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.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.RECEIVE_WIFI_CREDENTIAL_CHANGE	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_WIFI_CREDENTIAL	未知	未知权限	来自 android 引用的未知权限。
android.permission.CHANGE_WIFI_MULTICAST_STATE	危险	允许接收WLAN多播	允许应用程序接收并非直接向您的设备发送的数据包。这样在查找附近提供的服务时很有用。这种操作所耗电量大于非多播模式。
android.permission.OVERRIDE_WIFI_CONFIG	普通	允许修改任何 Wi-Fi 配置	允许应用程序修改任何 wifi 配置，即使是由另一个应用程序创建的。
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。

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: 2 | 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	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
3	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过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。

</> 代码安全漏洞检测

高危: 0 | 警告: 2 | 信息: 0 | 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
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

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.SYSTEM_ALERT_WINDOW
其它常用权限	2/46	android.permission.CHANGE_WIFI_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。

URL 链接安全分析

URL信息	源码文件
127.0.0.1	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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 App Startup	Google	App Startup 库提供了一种直接，高效的方法在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。

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