南明离火
移动应用检测平台

ANDROID 静态分析报告

PornHub • v1.1.1

分析日期: 2024-09-27 16:46:03

应用概览

文件名称:	d8d8fa474476140ced503bf565c0b900657bda84f1b2c7842d90ba7aff41e584.apk
文件大小:	6.04MB
应用名称:	PornHub
软件包名:	com.zq.ph
主活动:	com.zq.ph.MainActivity
版本号:	1.1.1
最小SDK:	22
目标SDK:	30
加固信息:	未加壳
应用程序安全分数:	60/100 (低风险)
杀软检测:	5 个杀毒软件报毒
MD5:	7e747dafc64258062cc189c5bf5a0e42
SHA1:	cb7a4ae0139620ddb6548f8aa6d0c717f0930d5f
SHA256:	d8d8fa474476140ced503bf565c0b900657bda84f1b2c7842d90ba7aff41e584

分析结果严重性分布

高危	中危	信息	安全	关注
0	1	1	2	4

四大组件导出状态统计

Activity组件：1个，其中export的有：5个
Service组件：0个，其中export的有：0个
Receiver组件：2个，其中export的有：0个
Provider组件：2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

本报告由南明离火移动安全分析平台生成

v2 签名: True
v3 签名: False
v4 签名: False
主题: C=a, ST=a, L=a, O=a, OU=a, CN=a
签名算法: rsassa_pkcs1v15
有效期自: 2022-06-21 05:32:57+00:00
有效期至: 2049-11-06 05:32:57+00:00
发行人: C=a, ST=a, L=a, O=a, OU=a, CN=a
序列号: 0x41772888
哈希算法: sha256
证书MD5: d49d20229d9dab896e21574bc3232c24
证书SHA1: 97b79fd8c8827cda42e464328c46dfb462f81b1e
证书SHA256: ba05c89d57a24934d976a647b91f733d38eb6f32d0c254b52aaba0ac1cc13b4b
证书SHA512:
4cf78e142e057f170c4bab11acec9f775015ff9539379b930d33d62c7587815ea44a53570eaa9b1ac1d1c4688d43d0d0a45c[illegible]d86ddffcfff7caaac0389fb

公钥算法: rsa
密钥长度: 2048
指纹: a8622d5e2214871f8de1d32546543dce06b23472ccf6ef958be849992a5043d9
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.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.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.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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。

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: **7** | 信息: **0** | 屏蔽: **0**

本报告由南明离火移动安全分析平台生成

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。
4	Activity-Alias (com.zq.ph.MainActivity5) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
5	Activity-Alias (com.zq.ph.MainActivity4) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
6	Activity-Alias (com.zq.ph.MainActivity3) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
7	Activity-Alias (com.zq.ph.MainActivity2) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
8	Activity-Alias (com.zq.ph.MainActivity1) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

代码安全漏洞检测

高危: **0** | 警告: **4** | 信息: **1** | 安全: **1** | 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	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成

4	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
5	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
6	MD5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

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/libtoolChecker.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。		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	False warning 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	1/30	android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	5/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE

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
baq.fbafb.cn	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
dfe.hapha.cn	安全	否	No Geolocation information available.
api.h-gpro.com	安全	否	No Geolocation information available.

faw.douying8.com	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
douyin-api.ybunx.com	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.91076 **查看:** 高德地图
chen.ybunx.com	安全	是	**IP地址:** 61.160.148.90 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件

• https://img01.yzcdn.cn/vant/empty-image- • https://noembed.com/embed?url=https • https://cdn.plyr.io/static/blank.mp4 • https://axios-http.com • https://lf3-cdn-tos.bdxiguastatic.com/obj/ixigua-static/xigua_fe/xigua_video_web_pc/static/media/series.bd5583e1.gif • https://t.me/ • http://brianleroux.github.com/lawnchair/ • https://vimeo.com/api/oembed.json?url= • https://github.com/axios/axios.git • https://github.com/mathiasbynens/CSS.escape • https://dfe.hapha.cn/api/v1/ • https://baq.fbafb.cn/api/v1/ • https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE • https://i.ytimg.com/vi/ • https://html2canvas.hertzen.com • https://clipboardjs.com/ • http://feross.org • https://api.m-d.vip/api/v1/ • https://douying.uk • https://cdn.jsdelivr.net/npm/workbox-cdn • https://player.vimeo.com/video/ • https://api.hghub.vip/api/v1/ • https://img01.yzcdn.cn/vant/share-sheet- • https://github.com/surmon-china • https://go.aniview.com/api/adserver6/vast/ • https://player.vimeo.com/api/player.js • https://hertzen.com • https://api.h-gpro.com/api/v1/ • https://api.91yy.vip/api/v1/ • https://feross.org/opensource • https://www.youtube-nocookie.com • https://xkeshi.github.io/image-compressor • https://cdn.plyr.io/3.7.2/plyr.svg • https://faw.douying8.com/api/v1/ • http://jsperf.com/b64tests • https://github.com/axios/axios/issues	自研引擎-A
• https://chen.ybunx.com/apk/app-1.1.0-3.apk	com/zq/ph/Update.java
• https://dfe.hapha.cn • https://api.h-gpro.com • https://dfe.hapha.cn/api/v1/ • https://douyin-api.ybunx.com • https://faw.douyinga.com/ • https://douyin-api.ybunx.com/api/v1/ • https://baq.fbafb.cn	com/zq/ph/UpdateInfo.java
• https://dfe.hapha.cn • https://api.h-gpro.com • https://chen.ybunx.com/apk/app-1.1.0-3.apk • https://dfe.hapha.cn/api/v1/ • https://douyin-api.ybunx.com • https://faw.douying8.com/ • https://douyin-api.ybunx.com/api/v1/ • https://baq.fbafb.cn	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息

RootBeer	Scott Alexander-Bown	A tasty root checker library and sample app. We've scoured the internets for different methods of answering that age old question... Has this device got root?
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。

🔑 敏感凭证泄露检测

可能的密钥
82758dd12749c777ef579f1839ceea6a

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。