南明离火
移动应用检测平台

ANDROID 静态分析报告

The King Of Fighters '97 • v1.5

分析日期: 2024-05-19 20:43:41

应用概览

文件名称:	The King Of Fighters '97_1.5.apk
文件大小:	58.32MB
应用名称:	The King Of Fighters '97
软件包名:	com.snkplaymore.android001
主活动:	com.dotemu.neogeo.kof97.KOF97InstallerActivity
版本号:	1.5
最小SDK:	14
目标SDK:	30
加固信息:	未加壳
应用程序安全分数:	39/100 (高风险)
跟踪器检测:	6/432
杀软检测:	AI评估：安全
MD5:	b5591ed994d4f8c457ed7081b713a622
SHA1:	9e108f46c2a915674f02f6363e9b049b9be5aa0f
SHA256:	31f87f6e53a21410b296c[illegible]e2394031ca3bb6b1cc461[illegible]bcdabdc3332e8dec5c

分析结果严重性分布

高危	中危	信息	安全	关注
5	1	1	1	3

四大组件导出状态统计

Activity组件：6个，其中export的有：1个
Service组件：2个，其中export的有：0个
Receiver组件：2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=sign, ST=sign, L=sign, O=sign, OU=sign, CN=sign.keystore
签名算法: rsassa_pkcs1v15
有效期自: 2016-03-30 13:22:39+00:00
有效期至: 2153-02-20 13:22:39+00:00
发行人: C=sign, ST=sign, L=sign, O=sign, OU=sign, CN=sign.keystore
序列号: 0x15f28a3
哈希算法: sha256
证书MD5: 1b8eafb7e9eda3176eb7b614f2176c0b
证书SHA1: ad19e3e2290382ae01020fedbe90495e4b9d8057
证书SHA256: d9ea86d285c97dab1fd2a42b7f625ab4bae6b4bddbc433f11035ad3e1d0a07d5
证书SHA512:
e00f9aac7d817abbbfc0b55cfaa2770b9f436b78744e79e078051c956b03031b842c8cbddc026d1a8985490a06892d57224b25d3[illegible]6cfe074b5b66eb6c5949030

公钥算法: rsa
密钥长度: 1024
指纹: 50ccf75d1355776e1aa08c5c63961581ce56fbc131e76487fddaf2f58528275f
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.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.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
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.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.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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
com.android.vending.CHECK_LICENSE	未知	未知权限	来自 android 引用的未知权限。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
android.permission.BLUETOOTH_SCAN	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够发现和配对附近的蓝牙设备。
android.permission.BLUETOOTH_ADVERTISE	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够向附近的蓝牙设备进行广告。
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: **3** | 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 4.0-4.0.2, [minSdk=14]	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	应用程序可以使用明文网络流量，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。
4	Activity (com.dotemu.neogeo.kof97.KOF97MainActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity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是显式导出的。

代码安全漏洞检测

高危: **4** | 警告: **7** | 信息: **1** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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

3	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
4	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	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	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
8	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
9	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
10	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

11	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
12	默认情况下，调用Cipher.getInstance("AES")将返回AES ECB模式。众所周知，ECB模式很弱，因为它导致相同明文块的密文相同	高危	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-2	升级会员：解锁高级权限
13	WebView域控制不严格漏洞	高危	CWE: CWE-73: 外部控制文件名或路径	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/libEmulator.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	3/30	android.permission.ACCESS_FINE_LOCATION android.permission.GET_TASKS android.permission.WAKE_LOCK
其它常用权限	7/46	android.permission.WRITE_EXTERNAL_STORAGE android.permission.BLUETOOTH_ADMIN android.permission.BLUETOOTH android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET 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
corporate.dotemu.com	安全	否	**IP地址:** 51.91.73.21 **国家:** 法国 **地区:** 上法兰西岛 **城市:** 鲁拜克斯 **纬度:** 50.693710 **经度:** 3.174439 **查看:** Google 地图

applab-sdk.amazon.com	安全	否	**IP地址:** 72.21.194.171 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
goo.gl	安全	否	**IP地址:** 172.217.161.206 **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
ags-ext.amazon.com	安全	否	**IP地址:** 54.215.230.51 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
cortana-gateway.amazon.com	安全	否	**IP地址:** 52.46.130.13 **国家:** 美利坚合众国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
market.android.com	安全	否	**IP地址:** 173.194.174.118 **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
data.flurry.com	安全	否	**IP地址:** 106.10.248.147 **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
www.apple.com	安全	是	**IP地址:** 180.163.150.169 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.061668 **经度:** 118.777992 **查看:** 高德地图
www.amazon.com	安全	否	**IP地址:** 104.76.30.12 **国家:** 大韩民国 **地区:** 首尔teukbyeolsi **城市:** 首尔 **纬度:** 37.566311 **经度:** 126.977203 **查看:** Google 地图

www.livinggames.jp	安全	否	**IP地址:** 59.106.13.207 **国家:** 日本 **地区:** 东京 **城市:** 东京 **纬度:** 35.689499 **经度:** 139.692322 **查看:** Google 地图
www.googletagmanager.com	安全	是	**IP地址:** 180.163.150.38 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
www.chartboost.com	安全	否	**IP地址:** 13.226.210.27 **国家:** 美利坚合众国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
googleads.g.doubleclick.net	安全	是	**IP地址:** 180.163.150.38 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
pass.auone.jp	安全	否	**IP地址:** 18.64.8.112 **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
live.chartboost.com	安全	否	**IP地址:** 34.107.157.36 **国家:** 美利坚合众国 **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

URL 链接安全分析

URL信息	源码文件
• https://cortana-gateway.amazon.com/cortana/gateway/getsigneddownloadurl	com/amazon/ags/client/whispersync/migration/MigrationHttpClient.java
• https://kes-ext.amazon.com/service/gamedata/whisperdata	com/amazon/ags/client/whispersync/network/WhispersyncHttpClientImpl.java
• javascript:handleoverlaydata	com/amazon/ags/html5/overlay/GameCircleAlertUserInterface.java

• javascript:handleoverlaydata	com/amazon/ags/html5/overlay/GameCircleUserInterface.java
• javascript:handlemessage	com/amazon/ags/html5/service/WebViewServiceHelper.java
• https://applab-sdk.amazon.com/1.0	com/amazon/insights/abtest/DefaultABTestClient.java
• https://applab-sdk.amazon.com/1.0	com/amazon/insights/core/configuration/HttpCachingConfiguration.java
• https://applab-sdk.amazon.com/1.0	com/amazon/insights/delivery/ERSRequestBuilder.java
• https://www.chartboost.com/support/sdk_download/?os=ios	com/chartboost/sdk/Chartboost.java
• file:///android_res/	com/chartboost/sdk/impl/at.java
• https://live.chartboost.com	com/chartboost/sdk/impl/ba.java
• http://market.android.com/	com/chartboost/sdk/impl/bb.java
• http://corporate.dotemu.com/assets/%s/%s	com/dotemu/neogeo/kof97/KOF97InstallerActivity.java
• http://www.amazon.com/gp/mas/dl/android?p=%s&showall=1	com/dotemu/_3rdParty/impls/store/_3rdPartyStore_Amazon.java
• https://play.google.com/store/apps/developer?id=dotemu&referrer=utm_source%3ddotmoregames%26utm_medium%3dcpc%26utm_campaign%3d	com/dotemu/_3rdParty/impls/store/_3rdPartyStore_GooglePlay.java
• http://pass.auone.jp/app/detail?app_id=%s • http://www.livinggames.jp/sp/#toiawase?app=%s	com/dotemu/_3rdParty/impls/store/_3rdPartyStore_WorkerBee.java

• https://www.chartboost.com/support/sdk_download/?os=ios • https://live.chartboost.com • http://pass.auone.jp/app/detail?app_id=%s • http://corporate.dotemu.com/assets/%s/%s • http://www.amazon.com/gp/mas/dl/android?p=%s&showall=1 • https://cortana-gateway.amazon.com/cortana/gateway/getsigneddownloadurl • http://hostname/? • http://www.google.com • http://www.livinggames.jp/sp/#toiawase?app=%s • http://data.flurry.com/aap.do • javascript:handlemessage • javascript:handleoverlaydata • http://plus.google.com/ • https://applab-sdk.amazon.com/1.0 • https://data.flurry.com/aap.do • https://ags-ext.amazon.com/service/gamedata/whisperdata • 127.0.0.1 • http://market.android.com/ • file:///android_res/ • https://www.googletagmanager.com • http://goo.gl/nafqqk • https://play.google.com/store/apps/developer?id=dotemu&referrer=utm_source%3ddotmoregames%26utm_medium%3dcpc%26utm_campaign%3d	自研引擎-S
• ftp://%s:%s@%s • 127.0.0.1 • 1.2.0.4 • http://www.facebook.com/snk.kofworld/	lib/arm64-v8a/libEmulator.so

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。

邮箱地址敏感信息提取

EMAIL	源码文件
support@dotemu.com	com/dotemu/game/base/activities/DEMainActivity.java
support@dotemu.com	com/dotemu/installer/activities/DEInstallerActivity.java
support@dotemu.com	com/dotemu/_3rdParty/_3rdParty.java
support@dotemu.com	自研引擎-S

第三方追踪器检测

名称	类别	网址
Amazon Analytics (Amazon insights)	Analytics	https://reports.exodus-privacy.eu.org/trackers/95
ChartBoost		https://reports.exodus-privacy.eu.org/trackers/53
Flurry	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/25
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

敏感凭证泄露检测

可能的密钥
凭证信息=> "com.google.android.gms.games.APP_ID" : "@string/app_id_dotemu"
2e0b46f8d04a06ac187a2eb0429558fe
a25ff919-ed9e-4e80-b06d-f0d53f5a367b
62466ae0-95ca-11e1-b0c4-0800200c9a68
Y29tLmFuZHJvaWQudmVuZGluZy5saWNlbnNpbmcuSUxpY2Vuc2luZ1NlcnZpY2U=
97e83c003bded24445aefd4c72dc4b85
jqyngW96w5vk9a3gLSPP0srNdRpFkRi2+FjI6qMoPrg=

Google Play 应用市场信息

标题: THE KING OF FIGHTERS '97

评分: 3.5888524 **安装:** 100,000+ **价格:** 16.704889 **Android版本支持:** **分类:** 街机 **Play Store URL:** com.snkplaymore.android001

开发者信息: SNK CORPORATION, 5156685669113307397, Osaka No.2 NK Building 3rd Floor, 4-5-41, Miyahara, Yodogawa-ku, Osaka, 532-0003, JAPAN, https://www.snk-corp.co.jp/game/, info@snk-corp.co.jp

发布日期: None **隐私政策:** Privacy link

关于此应用:

本作加入了由玩家投票产生的新角色，以及通过编辑队伍组合达成不同的结局等众多崭新要素。 草薙京与八神庵的宿命对决，众人与大蛇一族壮绝的战斗最终将走向何方？ 燃烧吧，不灭的激情！ 特色■多达35人的参战角色！ 除了「草薙京」「特瑞 博加德」等玩家耳熟能详的名字外、来自饿狼传说系列的「布鲁 玛丽」、「山崎龙二」、KOF原创角色「七枷社」等新面孔也将率队参战！！同时，玩家一开始就可以使用NEOGEO版中的隐藏角色[暴走八神庵]和[觉醒莉安娜]！当然，作为KOF的特色之一，信息量巨大的替换内容让任何角色之间的对战都不会冷场！ ■2种操作模式让游戏系统更加深奥！ 本作融合了ADVANCED MODE与EXTRA MODE两种操作模式。玩家可以选择适合自己的模式展开激战！ ＜ADVANCED MODE的特点＞ 前冲，后撤及丰富的跳跃方式使玩家能够迅速接近或远离对手，是一种富于攻击性的模式。 通过储存能量槽，玩家可以在任意时间发动[MAX模式]或者[超必杀技]等需要消费能量槽的操作。 如果目前使用的角色输掉比赛，接下来出场的角色的能量槽的存储量会因为他与目前使用角色之间的关系而变化。队伍的编成以及出场顺序的选择变得更为重要。 ＜EXTRA MODE的特点＞ 通过利用灵巧快速的前后移动，可以将对手玩弄于鼓掌之间。 可以在任意时间主动积蓄能量槽，积满后自动进入POWER MAX状态。 角色体力所剩不多时，体力槽会闪烁，此时可以无限制使用超必杀技。 ■不仅仅是NEOGEO版的完全移植！ 除了完全再现街机版的4键操作方式外，也可以设置包含[紧急回避]和[吹飞攻击]专用按钮的6键模式或者一键即可使出必杀技的SP按钮！ ■通过蓝牙功能展开热血对战！ 除了单人游戏外，更可以利用蓝牙功能展开双人对战。新老玩家皆可享受PVP快感！ 官方新浪微博：SNK CORPORATION 官方腾讯微博：SNK官方 ©SNK CORPORATION ALL RIGHTS RESERVED.

免责声明及风险提示: