南明离火
移动应用检测平台

ANDROID 静态分析报告

[redacted] v8.3.0

分析日期: 2025-04-01 21:18:55

应用概览

文件名称:	■■■■■■■ v8.3.0.apk
文件大小:	62.51MB
应用名称:	■■■■■■■
软件包名:	jp.konami.pesar
主活动:	com.epicgames.ue4.SplashActivity
版本号:	8.3.0
最小SDK:	24
目标SDK:	27
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	36/100 (高风险)
跟踪器检测:	2/432
杀软检测:	6 个杀毒软件报毒
MD5:	07d028e43510a60bc7f0c6a2a10f9a5e
SHA1:	ffa6e867fcdfd9ee6dbf140f41654b6cc87e2421
SHA256:	114caba16f30fdcd9da4dc11c0ad183aecde0bfab95a7942e3c0825ca59e797

分析结果严重性分布

高危	中危	信息	安全	关注
10	22	4	1	1

四大组件导出状态统计

Activity组件：16个，其中export的有： 2个
Service组件：12个，其中export的有： 5个
Receiver组件：10个，其中export的有： 4个
Provider组件：3个，其中export的有： 1个

应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: False
v3 签名: False
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:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea30397727d17958704d89b7711292a4569

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.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.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.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_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.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.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
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.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.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
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.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。

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。
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。
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，在手机屏幕关闭后后台进程仍然运行。
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。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
com.android.vending.CHECK_LICENSE	未知	未知权限	来自 android 引用的未知权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
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。
jp.konami.pesar.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
net.dinglisch.android.tasker.PERMISSION_RUN_TASKS	未知	未知权限	来自 android 引用的未知权限。
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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	申请用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
android.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。

可视觉 Activity 组件分析

ACTIVITY	INTENT

com.epicgames.ue4.GameActivity	Schemes: pesactionmobile://,

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: **1** | 警告: **0** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名
应用程序容易受到 Janus 漏洞的影响	高危	应用程序使用 v1 签名方案进行签名，如果仅使用 v1 签名方案进行签名，则在 Android 5.0-8.0 上容易受到 Janus 漏洞的影响。在使用 v1 和 v2/v3 方案签名的 Android 5.0-7.0 上运行的应用程序也容易受到攻击。

Manifest 配置安全分析

高危: **5** | 警告: **12** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Activity （com.epicgames.ue4.SplashActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (27) 更新到 28 或更高版本以在平台级别修复此问题。
2	Activity (com.epicgames.ue4.SplashActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (27) 更新到 29 或更高版本以在平台级别修复此问题。
3	Activity （com.epicgames.ue4.GameActivity） 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。 然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。 这使应用程序成为网络钓鱼攻击的易受攻击目标。 可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity="") 属性来修复此漏洞。 您还可以将应用的目标 SDK 版本 (27) 更新到 28 或更高版本以在平台级别修复此问题。
4	Activity (com.epicgames.ue4.GameActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (27) 更新到 29 或更高版本以在平台级别修复此问题。
5	Activity (com.epicgames.ue4.GameActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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	Broadcast Receiver (com.epicgames.ue4.MulticastBroadcastReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver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	Service (jp.konami.android.common.FirebaseMessagingServiceDerived) 未被保护。 [android:exported=true]	警告	发现 Service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	Service (jp.konami.android.common.FirebaseInstanceIdServiceDerived) 未被保护。 [android:exported=true]	警告	发现 Service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。
9	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
10	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
11	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 未被保护。 [android:exported=true]	警告	发现 Service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。
12	Content Provider (com.applisto.appcloner.classes.DefaultProvider) 未被保护。 [android:exported=true]	警告	发现 Content Provider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。
13	Service (com.applisto.appcloner.service.RemoteService) 未被保护。 [android:exported=true]	警告	发现 Service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。
14	Broadcast Receiver (com.applisto.appcloner.classes.DefaultProvider$DefaultReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
15	Activity (com.applisto.appcloner.classes.DefaultProvider$MyActivity) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (27) 更新到 29 或更高版本以在平台级别修复此问题。
16	Activity (com.applisto.appcloner.classes.DefaultProvider$MyActivity) 未被保护。 [android:exported=true]	警告	发现 Activity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。

17	Broadcast Receiver (com.applisto.appcloner.classes.FakeCamera$FakeCameraReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver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Broadcast Receiver是显式导出的。

代码安全漏洞检测

高危: **4** | 警告: **8** | 信息: **3** | 安全: **0** | 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	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
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	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
6	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
7	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

8	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
9	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
10	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: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	升级会员：解锁高级权限
11	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
12	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
13	此应用侦听剪贴板更改。一些恶意软件也会监听剪贴板更改	信息	OWASP MASVS: MSTG-PLATFORM-4	升级会员：解锁高级权限
14	应用程序创建临时文件。敏感信息永远不应被写进临时文件	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
15	应用程序在加密算法中使用ECB模式。ECB模式是已知的弱模式，因为它对相同的明文块[UNK]产生相同的密文	高危	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-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/libappcloner.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	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	True info 符号被剥离

2	arm64-v8a/libtry-alloc-lib.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。	False high 这个二进制文件没有在栈上添加栈哨兵值。栈哨兵是用于检测和防止攻击者覆盖返回地址的一种技术。使用选项-fstack-protector-all来启用栈哨兵。这对于Dart/Flutter库不适用，除非使用了Dart FFI	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	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
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	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
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
00172	检查管理员权限以（可能）获取它们	admin	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
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
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	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

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
00175	获取通知管理器并取消通知	通知	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	升级会员：解锁高级权限
00026	方法反射	反射	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	升级会员：解锁高级权限
00028	从assets目录中读取文件	文件	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	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
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00121	创建目录	文件 命令	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	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	6/30	android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.SYSTEM_ALERT_WINDOW android.permission.CAMERA android.permission.WRITE_SETTINGS

其它常用权限	15/46	android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.CHANGE_NETWORK_STATE android.permission.CHANGE_WIFI_STATE android.permission.FOREGROUND_SERVICE android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE com.google.android.gms.permission.AD_ID com.google.android.c2dm.permission.RECEIVE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.FLASHLIGHT android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

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
google.com	安全	否	**IP地址:** 142.250.189.14 **国家:** 美国 **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
www.samsung.com	安全	是	**IP地址:** 61.147.219.216 **国家:** 中国 **地区:** 江苏 **城市:** 南通 **纬度:** 32.030296 **经度:** 120.874779 **查看:** 高德地图
pes-action-mobile-57853607.firebaseio.com	安全	否	**IP地址:** 34.120.160.131 **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
www.applilink.jp	安全	否	**IP地址:** 18.154.144.112 **国家:** 美国 **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

www.konami.jp	安全	否	**IP地址:** 23.206.229.81 **国家:** 美国 **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
whois.domaintools.com	安全	否	**IP地址:** 199.30.228.13 **国家:** 美国 **地区:** 华盛顿 **城市:** 西雅图 **纬度:** 47.615700 **经度:** -122.344438 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• http://play.google.com/store/apps/details?id=	jp/konami/android/common/AppStore.java
• https://google.com/ • https://www.samsung.com/	com/epicgames/ue4/network/NetworkChangedManager.java
• www.applilink.jp	jp/applilink/sdk/common/ApplilinkConsts.java
• http://www.konami.jp	jp/konami/android/common/KWebDialog.java
• http://whois.domaintools.com/ • 127.0.0.1	com/applisto/appcloner/classes/HostsBlocker.java
• https://pes-action-mobile-57868607.firebaseio.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://pes-action-mobile-57868607.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/306442212056/namespaces/firebase:fetch?key=AIzaSyAWLh32Pgw6ga12CTmcO-TLgq-1t7fUCA8 ）已禁用。响应内容如下所示：
		
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

本报告由南明离火移动安全分析平台生成

SDK名称	开发者	描述信息
Crashlytics	Google	Crashlytics 是 Firebase 的主要崩溃报告工具。将众多崩溃整理成一个方便管理的问题列表，从而缩短问题排查时间。在 Crashlytics 信息中心内查看问题对用户造成的影响，从而清楚合理地确定应当首先解决哪些问题。
Sandhook	asLody	SandHook 是作用在 Android ART 虚拟机上的 Java 层 Hook 框架，作用于进程内是不需要 Root 的。
Unreal Engine	Epic Games	虚幻引擎是一款由 Epic Games 开发的游戏引擎。该引擎主要是为了开发第一人称射击游戏而设计，但现在已经被成功地应用于开发潜行类游戏、格斗游戏、角色扮演游戏等多种不同类型的游戏。
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
Google Sign-In	Google	提供使用 Google 登录的 API。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图，Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
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，高效的方法来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。
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。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

第三方追踪器检测

名称	类别	网址
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

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"
"google_app_id" : "1:206442212056:android:5f015d05ae825eab"
"firebase_database_url" : "https://pes-action-mobile-57868607.firebaseio.com"
"google_api_key" : "AIzaSyAWLh32Pgw6ga12CTmcO-TLgq-1t7fUCA8"
"google_crash_reporting_api_key" : "AIzaSyAWLh32Pgw6ga12CTmcO-TLgq-1t7fUCA8"

"app_id" : "306442212056"
n4EPbNtXMNgNzgO0pJjfLc54Q9QnnUoOaUIYAPh3VtjxGkQhzM+wXdSDCxzgR/iipbLkIXQNuy2sY
Y29tLmFuZHJvaWQudmVuZGluZy5saWNlbnNpbmcuSUxpY2Vuc2luZ1NlcnZpY2U=
n5cgy1k4ASf3A5cAFuJXKKaF9KpBPgDvM7KP4g1oIIGkCMADcBJwb2p8KOMvMPoUaCCBpALgfmBba
n+ZGkpzrId6ak3RlpLm1xz5kePn0QOrZ5A3H9GIMf80wHeZ+l7OZo6Qh7HwFWh45t3iCsKEiATkXo
Y29tLmFwcGxpc3RvLmFwcGNsb25lci5jbGFzc2VzLnNlY29uZGFyeQ==
njY7OJr0mLOpwiHpt4BgUi6Q3PCZi8h1SSjpR0vaM9LxEkHSMh69dMRHz7agGfUSIhqhzKG50dHiJ
nJBUhcameExFCkEhow4NEJCIST32oW4TEg3ogbg+NkIAaSl1KFG2lNGlJimqU0/P3sGZ0nLNn9qx9
n+AxcP7sT90e4wsx2lRLoVkh6KOeOs1Z8IekeSce3yWOWpL9T0tgIaWGb+w/x8OmdyoJXQPCPkDTc
nnEP6ewBXAAflTa7oYJUhwJEetmtGlXCvCL+m3LNYblk7NznmCXnpivcDfARoGWQz+wH3PlZaTRjs
n78C8qoIPewXwOcK9V1kHzIi2qlRGLEB3LDSVx3KgP3rEWSlxHzAZt8OgIjPjEvkcWGJmr4dyoA/A
nYfAXeebVnyGCJC3JuHeGh1/vFx2nMjvh++m8iTvax9jMPgHOBv5OMXlE0tICyhR86SYXchted46h
49DBDDA1F6D2617B78C7F70DEF494BF6
nbmhoaGhoaMig8M5S0hTgENxxYMk8kg9v+nAPg34ys79CB6GnkDt8Q5KGon97[illegible]LWU8UsbB
nZWtL6D4gxIeEjTgRsiZreZ8nNC9qRwx6BC0WIWuyNpCzY/YJalfUgLEw4L[illegible]umNuJ4BOD
876293D0801C6FF99A4FC4A4F4C885CD
n2olwU2SXZdN1AtzmEfwtI+49oSQRspqj1yT9EUqAMoahx3r[illegible]W8MLONwFzglxT7WyQ9[illegible]mX0M
noCasBeYxdhEKpQwBfJ50pb7yY2abgNmki7C4F0Q[illegible]sII[illegible]Fm4VchWLJb0nG[illegible]9QicidEUf
nd7qkHRn2vssMU5VdE3xYVka86jITBsDMNu[illegible]mjD[illegible]9Ihqhj7ifnqmsb[illegible]0PGDUkNXMvqV4
nJ2k5MBi65DXhQ6iwE5b0BHBP6FLX[illegible]Wa2u5ImSNKdNMFP[illegible]Ka0CkmcDa0CWuCVuBu8zs
nCXBIWXMAAC4jAAAuIwF4pT92A[illegible]EQVR42u2dW6wd[illegible]f98pirqUREIc6tIihKZOL0rqLiEI
nzHYAd4WORoWsA241sx[illegible]SHgPuC+lQifwM[illegible]ZGav[illegible]nYmptVM+CLc4RUzgEm42eiehP2E
nsw0NDQ0NDQ0[illegible]IesnY[illegible]BE4BTsKt2ewLT[illegible]CfK[illegible]feUYzYO8ROjmQsca3o2IrYFJm2AXuAL81s
0A78FEBE1D4E2[illegible]98BBD19FBAC49[illegible]0949E9120E411C0E9EE9F8C945860C07105FFB90A5AE8CD5310C13C800BFBDD65C2F65076D05B4 3F923FE[illegible]83D197DB4F1A1AA4D18[illegible]67F6A8CD401745818217165C43292CE44034CA16A39FAD3184FF463E2787183461C0936EE29974FB57B 61F6323F0E[illegible]B3E1049D16051E97D[illegible]027987BB3B1151AB132
nEWYD347Bz/VmtmYM96cS[illegible]CLMJVsE38naNXQ+k30gdExyI+kVj3Z1fpu0Jssdnp1GWxEkHSTp
nlwr5ETjezBRsKULS6Z[illegible]U8[illegible]oIPcBxwGQRaC5I0iNvycX7oSARkPgQQQNKjwHJgQugIBGYiVLwY
n6ILXhSq+P2A[illegible]V0REDDQ314F/QQmVQhaYmuwAAAABJRU5ErkJggg==
nxtAB6[illegible]5W9DaF97Fkkv5BBgPHxbUjgkvZgS+F2SbgztX10o9cGJpAXA1cB03BOr94DlZvZT
nbz2PpFXK5obQPvYskh5WPqaG9rXnkDRR0q6cAjxZdP59oQNQA84ADshpO6vozBsB4DAP2/2KzrwR
nAP7xsB0qOvNGAL+5kIrOvBGghKD60AgQmEYAONDD9oSiM98ndOIrwNdAPL4fjn7G/UKyedoX+C60

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。