南明离火
移动应用检测平台

ANDROID 静态分析报告

Neko Slots • v1.76

分析日期: 2024-06-12 16:33:11

应用概览

文件名称:	Neko-Slots_apkr6slo20_major_336.apk
文件大小:	7.7MB
应用名称:	Neko Slots
软件包名:	com.neko.slots.apk
主活动:	com.game.intsdk.StartActivity
版本号:	1.76
最小SDK:	24
目标SDK:	34
加固信息:	未加壳
应用程序安全分数:	35/100 (高风险)
杀软检测:	AI评估：安全
MD5:	57c74e51662b07820a12ae8432e248d9
SHA1:	e0f531cdec394b3dd1e736a984e314cdf93ca54c
SHA256:	89aa011b6cda388ef9064aaa2[illegible]ee448a286c3838a[illegible]65be63f18d1a7

分析结果严重性分布

高危	中危	信息	安全	关注
4	4	10	1	0

四大组件导出状态统计

Activity组件：4个，其中export的有：0个
Service组件：0个，其中export的有：0个
Receiver组件：2个，其中export的有：1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: False
v2 签名: True

v3 签名: False
v4 签名: False
主题: C=SI, ST=Amapá, L=Monteiro de Costa, O=da Mota - EI, OU=Barros, CN=Sr. João Felipe Pinto
签名算法: rsassa_pkcs1v15
有效期自: 2017-02-23 11:23:00+00:00
有效期至: 2117-01-30 11:23:00+00:00
发行人: C=SI, ST=Amapá, L=Monteiro de Costa, O=da Mota - EI, OU=Barros, CN=Sr. João Felipe Pinto
序列号: 0xbc242cd84cbe90c2
哈希算法: sha256
证书MD5: 8ecd50345b978a2cf1b5e368c1a77bf6
证书SHA1: 9fed60d314fc14fe7d9b728d2113e4c4de9b5b3b
证书SHA256: 281728cf1d274b9cbd09a083cef9bf52c728fc60933f08646038a010fb897c0a
证书SHA512:
18253c2f7515aeeb5426dd1c138306a3ea60c7c5be91c557112ff0f0a0628cb3bed6343430015df596a1409dba0b19b32dbcf250054aeb9a96f9900aa2c2a33

公钥算法: rsa
密钥长度: 2048
指纹: 7604320b3ca4946ba7b8d38de5fff3ebb89301b312f6a5ccf2f2dceb69fb7509
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_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.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.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。
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。
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.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
com.neko.slots.apk.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.game.intsdk.StartActivity	Schemes: intscheme://, Hosts: int.game,

网络通信安全风险分析

高危: **3** | 警告: **1** | 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。
2	*	警告	基本配置配置为信任系统证书。
3	*	高危	基本配置配置为信任用户安装的证书。
4	43.132.55.55	高危	域配置不安全地配置为允许明文流量到达范围内的这些域。

证书安全合规分析

高危: **0** | 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 7.0, [minSdk=24]	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:networkSecurityConfig=@xml/network_security_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。
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	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.DUMP [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。

代码安全漏洞检测

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

序号	问题	等级	参考标准	文件位置
1	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

2	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

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.VIBRATE
其它常用权限	7/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.gms.permission.AD_ID

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。

第三方 SDK 组件分析

SDK名称	开发者	描述信息
MMKV	Tencent	MMKV 是基于 mmap 内存映射的 key-value 组件，底层序列化/反序列化使用 protobuf 实现，性能高，稳定性强。
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。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。

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。