南明离火
移动应用检测平台

ANDROID 静态分析报告

639.CC

全民乐 VII • v1.0

分析日期: 2024-03-15 17:49:46

应用概览

文件名称:	全民乐 VII.apk
文件大小:	3.27MB
应用名称:	全民乐 VII
软件包名:	com.ghqmaebppv.qkllwedyhn
主活动:	com.ghqmaebppv.qkllwedyhn.MainActivity
版本号:	1.0
最小SDK:	21
目标SDK:	27
加固信息:	未加壳
应用程序安全分数:	67/100 (低风险)
杀软检测:	3 个杀毒软件报毒
MD5:	33dd0a77cd4b8e16b3031f5482c4f022
SHA1:	e5bbcdb6a77a847d383b4a3e8524708c87f223cf
SHA256:	af5edbe06c334531b532e57f8[illegible]2a8792384be15072fc59[illegible]2bb780198f8b

分析结果严重性分布

高危	中危	信息	安全	关注
0	3	1	1	0

四大组件导出状态统计

Activity组件：1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: False
v2 签名: False

本报告由南明离火移动安全分析平台生成

v3 签名: False
v4 签名: False
主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
签名算法: rsassa_pkcs1v15
有效期自: 2023-11-09 16:47:45+00:00
有效期至: 2078-08-12 16:47:45+00:00
发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
序列号: 0x34169a46
哈希算法: sha256
证书MD5: 0d3c9fdd3ef5cc228f29d65a47fea2f9
证书SHA1: b572b3918f9453288a39e3d4a31835051116c814
证书SHA256: 016d82827a88246e77d8aa8f45fc33ae9754ebfc279b74ea14b089d267781e0e
证书SHA512:
6efef6d72516c8b9fe513cf205d1ee30529c56e5389dab78f83802882c46a5b33e9d901be4dbdd13e55fa2e7e83c66fccbab31fb7461c46df7f928f265dd4320

公钥算法: rsa
密钥长度: 2048
指纹: eed148ba5abe89ee1695ef80f273d9e77c9a0d36b841800aa83523ef5d068511
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.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.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。

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: **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: **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 5.0-5.0.2, [minSdk=21]	警告	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: **0** | 信息: **1** | 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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	0/30	
其它常用权限	3/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_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。

免责声明及风险提示: