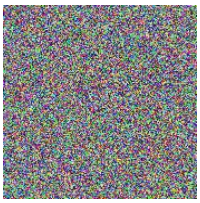
南明离火
移动应用检测平台

ANDROID 静态分析报告



pakgamerz • v1.1.12

分析日期: 2024-02-19 21:53:15

应用概览

文件名称:	Sharpahooter_Bgmi_64_Fixed.apk
文件大小:	9.39MB
应用名称:	pakgamerz
软件包名:	com.cheat.ninja
主活动:	com.cheat.ninja.loaderactivity
版本号:	13.12
最小SDK:	23
目标SDK:	29
加固信息:	未加壳
应用程序安全分数:	55/100 (中风险)
杀软检测:	26 个杀毒软件报毒
MD5:	576856798655ac3ed2220f49900fbd23
SHA1:	5fbde7a4a9950b87de5eace94d9699e8111e2371
SHA256:	3d592870fb50a93e8e44b007067[illegible]df63579a7a6d53f6[illegible]7a39b68d19504

分析结果严重性分布

高危	中危	信息	安全	关注
1	2	0	1	0

四大组件导出状态统计

Activity组件：7个，其中export的有：0个
Service组件：3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: True
v2 签名: False

v3 签名: False
v4 签名: False
主题: C=8609, ST=Surigao Del Norte, L=Caraga, OU=anon.org, O=zph-mph, CN=Jx Clarynx
签名算法: rsassa_pkcs1v15
有效期自: 2018-09-15 18:25:01+00:00
有效期至: 2118-08-22 18:25:01+00:00
发行人: C=8609, ST=Surigao Del Norte, L=Caraga, OU=anon.org, O=zph-mph, CN=Jx Clarynx
序列号: 0x1
哈希算法: sha256
证书MD5: 555c716f43950ea9c0dba29a5260e644
证书SHA1: 7d64f9c253c7ef35a0720f6f8a802bd4b920aa3a
证书SHA256: bd6515d3f58f73aa59ae99ae1d2aff74c4e2665c3bd677fbefea77222e88fc6b
证书SHA512:
e60a549715b200c503969104ddb3854738065fd90140eb270e99bf08d1e819f1c07c5c584f4f981cf86acab1085cc86eb63dd4348ae6cf418b25b83a49da604

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.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.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.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.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等
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。

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	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	高危	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

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 6.0-6.0.1, [minSdk=23]	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

序号	问题	等级	参考标准	文件位置

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/libapkprotect.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	True info 二进制文件有以下加固函数: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	False warning 符号可用
2	arm64-v8a/libninja.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.SYSTEM_ALERT_WINDOW android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK
其它常用权限	3/46	android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET android.permission.FOREGROUND_SERVICE

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
www.openssl.org	安全	否	**IP地址:** 34.36.58.177 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• ftp://%s:%s@%s • 1.2.0.4	lib/arm64-v8a/libninja.so

邮箱地址敏感信息提取

EMAIL	源码文件
ftp@example.com	lib/arm64-v8a/libninja.so

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。