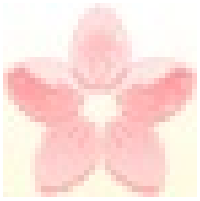
南明离火
移动应用检测平台

ANDROID 静态分析报告



修炼手札 • v2.67

分析日期: 2024-05-30 14:18:50

应用概览

文件名称:	240218mmznxlsz.apk
文件大小:	27.82MB
应用名称:	修炼手札
软件包名:	com.hydrozoa.hhz
主活动:	com.unity3d.player.UnityPlayerActivity
版本号:	2.67
最小SDK:	22
目标SDK:	34
加固信息:	未加壳
应用程序安全分数:	39/100 (高风险)
杀软检测:	8 个杀毒软件报毒
MD5:	eff4bdf1fe223010362cfec393396b83
SHA1:	92fdb5aa43146925fdf39539c43d053f88cc6768
SHA256:	75b45f55d316b90d5282ecada0967a217d8b4606322140b1485b15a59a3cde080

分析结果严重性分布

高危	中危	信息	安全	关注
4	7	1	1	1

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：1个，其中export的有：0个
Receiver组件：0个，其中export的有：0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: True
v2 签名: True
v3 签名: True

本报告由南明离火移动安全分析平台生成

v4 签名: False
主题: C=c, ST=c, L=c, O=c, OU=cc, CN=c
签名算法: rsassa_pkcs1v15
有效期自: 2018-01-19 09:08:41+00:00
有效期至: 2117-12-26 09:08:41+00:00
发行人: C=c, ST=c, L=c, O=c, OU=cc, CN=c
序列号: 0x74150105
哈希算法: sha256
证书MD5: afd12359955c5e9d3f8fa071eb9a4e87
证书SHA1: c7fbd347864fa8123416b2a5d9e015f197b346dd
证书SHA256: 37803c47397861e81ba0447b486a2bdf3e61202c01f178509f88c59b9b98237b
证书SHA512:
a88e86a89159f31ab158dfe3de3ffd3e6872b459a9294394ba7efa8bce3511a4b1161c80eba0ebd0b65931a73986021bf81867a2dae40af[illegible]7509ed09363

公钥算法: rsa
密钥长度: 2048
指纹: 580e921d75263f85881cf31b0522ced27a1535fbc73e2caaee04e96d919e1800
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_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。
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。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。

网络通信安全风险分析

高危: **1** | 警告: **0** | 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。

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: **2** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息

本报告由南明离火移动安全分析平台生成

1	应用程序可以安装在有漏洞的已更新 Android 版本上 Android 5.1-5.1.1, [minSdk=22]	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。
4	应用程序数据存在被泄露的风险 未设置[android:allowBackup]标志	警告	这个标志 [android:allowBackup]应该设置为false，默认情况下它被设置为true，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: **3** | 警告: **4** | 信息: **1** | 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
3	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
4	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
5	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	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

6	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
7	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
8	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	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/libmain.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
2	arm64-v8a/lib_burst_generated.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。		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	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	1/30	android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	3/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE

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
auth-api.heibaige.com	安全	是	**IP地址:** 116.62.35.179 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161580 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• http://www.ascendercorp.com/ • https://github.com/jilleJr/Newtonsoft.Json-for-Unity/issues/65 • http://www.ascendercorp.com/typedesigners.html • http://scripts.sil.org/OFL • https://github.com/jilleJr/Newtonsoft.Json-for-Unity/issues/8 • https://github.com/jilleJr/Newtonsoft.Json-for-Unity/issues/54	自研引擎-A
• http://%s/apicenter/%s/%s	wowvx/slz/c/a.java
• http://auth-api.heibaige.com/apicenter/%s/%s	com/wh/authsdk/h.java
• http://%s/apicenter/%s/%s • http://auth-api.heibaige.com/apicenter/%s/%s	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Unity	Unity Technologies	Unity 游戏使用 Il2Cpp 后端时产生的游戏代码。
Burst	Unity	Burst 是一个运用 LLVM 将 IL/.NET 字节码转换为高度优化的原生代码的编译器。
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。
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。

敏感凭证泄露检测

可能的密钥
"PASSWORD" : "Wachtwoord"

"USERNAME" : "Nutzername"
"PASSWORD" : "Senha"
"PASSWORD" : "Password"
"USERNAME" : "Gebruikersnaam"
"PASSWORD" : "Passwort"
"USERNAME" : "Username"
"USERNAME" : "Brugernavn"
"PASSWORD" : "Adgangskode"
1113a4d40917420d81bb6f20b6a0932f
25fe9a8589d9ff7e1c2450d24c847de0
d9c03ff42cf771efc2d42838c599e550
1cc1de2e96ea47c880000224d8aa5579
c68a23a3b02a90c5a62be3a93824c26442662b92dbf634dfea1fdf321c45ea008bd068e4[illegible]ef8bd733c06fed9cc92b[illegible]9c0c0[illegible]d0cf28c6e6c8d96c51257c6db
amF2YS5uZXQuSHR0cFVSTENvbm5lY3Rpb24=
9903CE71591C3B3D9C167709C0EA010A2C893855CFCA47BFC31F3C[illegible]599A1[illegible]EAE9562CC32C46F49A[illegible]7D254C8F5FB79

Google Play 应用市场信息

标题: 某某宗女修修炼手札

评分: 4.7352943 **安装:** 1,000+ **价格:** 7.437275 **Android版本支持:** **分类:** 角色扮演 **Play Store URL:** com.hydrozoa.hhz

开发者信息: Hydrozoa Works, Hydrozoa+Works, Kitchener, Ontario, Canada, https://hydrozoa.felisworks.com/hhz/, hydrozoa@foxmail.com,

发布日期: None **隐私政策:** Privacy link

关于此应用:

某某宗就是那个用撩汉子推汉子来修炼的宗..... 这是一个业务成鱼充满狗血的乙女向放置类游戏，玩家所要做的就是扮演某某宗的女（妖）修（女）选择撩谁和思考怎么在撩了多人的情况下不翻车..... 友情提示：武力值不足，请谨慎真的会翻车.....

免责声明及风险提示: