南明离火
移动应用检测平台

ANDROID 静态分析报告

Hidden Agenda v1.07

分析日期: 2025-11-21 17:22:41

应用概览

文件名称:	Hidden Agenda v1.07.apk
文件大小:	76.59MB
应用名称:	Hidden Agenda
软件包名:	com.playstation.hiddenagenda
主活动:	com.epicgames.ue4.SplashActivity
版本号:	1.07
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	44/100 (中风险)
杀软检测:	3 个杀毒软件报毒
MD5:	37aa6fe1fe907a61e55752dd0132e2e2
SHA1:	28cb210555de623d218e08c8[illegible]1a2d15709
SHA256:	34547970bf9e04e546fb1[illegible]171a04ed4a122811f14d5[illegible]43ae1d0ed4b0e00a044

分析结果严重性分布

高危	中危	信息	安全	关注
3	10	1	1	0

四大组件导出状态统计

Activity组件：6个，其中export的有： 1个
Service组件：2个，其中export的有： 1个
Receiver组件：3个，其中export的有： 1个
Provider组件：0个，其中export的有： 0个

应用签名证书信息

APK已签名

v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=e, ST=rt, L=yfr, O=y, OU=y, CN=y
签名算法: rsassa_pkcs1v15
有效期自: 2024-12-16 03:16:47+00:00
有效期至: 2052-05-03 03:16:47+00:00
发行人: C=e, ST=rt, L=yfr, O=y, OU=y, CN=y
序列号: 0xd9d26b26f33956c2
哈希算法: sha256
证书MD5: c0e119b10a34114ffb96f34ffdc24acc
证书SHA1: cf17aee75e4ff4aa1e122f49c60508a4d2a70e97
证书SHA256: d99ad2331dff4739c4c31fddd2bb6d12ee3b12d4241ab053048f0126770a9472
证书SHA512:
5e11c138eb480e3bbc69dadf7d8311bf538242e66094f11c1f1cc1bb99f2d7aa63a4a15c8320701d2f4dfc30478022df29e090e3ad7c99191e705288c687c3b0

公钥算法: rsa
密钥长度: 2048
指纹: 72b602a5bae73426cb671c395f5e3012b4b1f0542a26379d609b91e5afe41ac6
共检测到 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.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.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.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。
com.android.vending.CHECK_LICENSE	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.epicgames.ue4.GameActivity	Schemes: HiddenAgenda://,

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全分析

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: **4** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用数据存在泄露风险 未设置[android:allowBackup]标志	警告	建议将 [android:allowBackup] 显式设置为 false。默认值为 true，允许通过 adb 工具备份应用数据，存在数据泄露风险。
2	Activity (com.epicgames.ue4.GameActivity) 未受保护。 存在 intent-filter。	警告	检测到 Activity 已与设备上的其他应用共享，因此可被任意应用访问。intent-filter 的存在表明该 Activity 被显式导出，存在安全风险。
3	Broadcast Receiver (com.epicgames.ue4.MulticastBroadcastReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
4	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: **3** | 警告: **5** | 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，不应记录敏感信息	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
2	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

3	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
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	已启用远程WebView调试	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	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
8	应用程序使用基于PKCS5/PKCS7填充的加密模式CBC，此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
9	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限

Native 库安全加固检测

本报告由南明离火移动安全分析平台生成

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	armeabi-v7a/libbasichook.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	armeabi-v7a/libcorecall.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
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
00072	将 HTTP 输入流写入文件	命令 网络 文件	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
00091	从广播中检索数据	信息收集	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
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
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

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.WAKE_LOCK android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE

其它常用权限	4/46	android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE 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
login.yahoo.com	安全	否	**IP地址:** 87.248.116.12 **国家:** 德国 **地区:** 汉堡 **城市:** 汉堡 **纬度:** 53.575253 **经度:** 10.014778 **查看:** Google 地图
pagead2.googlesyndication.com	安全	是	**IP地址:** 220.181.174.102 **国家:** 中国 **地区:** 中国北京 **城市:** 北京 **纬度:** 39.904211 **经度:** 116.407395 **查看:** 高德地图
twitter.com	安全	否	**IP地址:** 172.66.0.227 **国家:** 美国 **地区:** 美国加利福尼亚州 **城市:** 旧金山 **纬度:** 37.718128 **经度:** -122.4343849 **查看:** Google 地图
www.paypal.com	安全	否	**IP地址:** 151.101.129.21 **国家:** 美国 **地区:** 美国加利福尼亚州 **城市:** 旧金山 **纬度:** 37.718128 **经度:** -122.4343849 **查看:** Google 地图
pop-up.apkomega.com	安全	否	**IP地址:** 188.114.97.0 **国家:** 美国 **地区:** 印第安纳州 **城市:** 弗朗西斯科 **纬度:** 38.333290 **经度:** -87.447083 **查看:** Google 地图
www.linkedin.com	安全	否	**IP地址:** 104.18.41.41 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.774929 **经度:** -122.419418 **查看:** Google 地图

www.moddownloadfast.com	安全	否	No Geolocation information available.
login.live.com	安全	否	**IP地址:** 20.190.160.64 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://www.moddownloadfast.com	OooO0o/OooO00o.java
• https://pop-up.apkomega.com/202307/api/popup_moddownloadfast.php?packagename=	hm/mod/update/up1.java
• https://pop-up.apkomega.com/202307/api/popup_moddownloadfast.php?packagename= • https://www.moddownloadfast.com • https://login.live.com • https://www.facebook.com • https://twitter.com • https://plus.google.com/ • https://accounts.google.com • https://login.yahoo.com • https://www.paypal.com • https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps • https://www.linkedin.com	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
C++ 共享库	Android	在 Android 应用中运行原生代码。
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 Sign-In	Google	允许使用 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。

敏感凭证泄露检测

可能的密钥
凭证信息=> "com.google.android.gms.games.APP_ID" : "@7F050012"
dYdvTgV3hux9klVZAFyOrXaZbQ==
EzJ8Qy5GzuMQAUZFKkWt9RYbZwRm

PXcLL0UKItMidAhxW1FqlTZuEDtXQGbSNmwScA==
acSPoiQQGE5hxJ+1JQ1SAWvegr8lVyopTf0=
Y29tLmFuZHJvaWQudmVuZGluZy5saWNlbnNpbmcuSUxpY2Vuc2luZ1NlcnZpY2U=

免责声明及风险提示: