ANDROID 静态分析报告

VIP NOBITA FF 1.71.7

分析日期: 2024-02-25 08:41:52

应用概览

文件名称:	VIP_NOBITA_FF_1.7.apk
文件大小:	7.79MB
应用名称:	VIP NOBITA FF
软件包名:	com.vip.nobita.ff
主活动:	.MainActivity
版本号:	1.7
最小SDK:	21
目标SDK:	28
加固信息:	未加壳
应用程序安全分数:	41/100 (中风险)
跟踪器检测:	1/432
杀软检测:	6 个杀毒软件报毒
MD5:	01c290aa9de0eb2675349aa00013dc9b
SHA1:	478e10f190da44b7c405f6c2135451f49180de69
SHA256:	64176af1e7e30972df530ef7051cbf1beb32063217ddf6a6356e82e4fa2848d3

分析结果严重性分布

高危	中危	信息	安全	关注
2	0	1	0	2

四大组件呈出状态统计

Activity组件：7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: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea3039772720179584704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
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.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.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android 7 新增权限，读取本地文件，如简历，聊天图片。
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。
android.permission.WRITE_MEDIA_STORAGE	签名(系统)	获取外置SD卡的写权限	允许应用程序在外置SD卡中进行写入操作。
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.WRITE_SECURE_SETTINGS	签名(系统)	修改安全系统设置	允许应用程序修改系统的安全设置数据。普通应用程序不能使用此权限。
android.permission.HIDE_OVERLAY_WINDOWS	普通	隐藏应用叠加窗口	允许应用防止在其上绘制非系统覆盖窗口。

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: **1** | 信息: **1**

标题	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

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	警告	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: **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: **2** | 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,不得记录敏感信息	警告	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	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

4	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
5	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
6	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
7	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
8	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

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.SYSTEM_ALERT_WINDOW
其它常用权限	4/46	android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_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

config.unityads.unitychina.cn	安全	是	**IP地址:** 58.216.88.121 **国家:** China **地区:** Jiangsu **城市:** Changzhou **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
t.me	安全	否	**IP地址:** 149.154.167.99 **国家:** United Kingdom of Great Britain and Northern Ireland **地区:** England **城市:** Warrington **纬度:** 52.184460 **经度:** -0.68759 **查看:** Google 地图
dupload.net	安全	否	**IP地址:** 104.21.3.192 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395201 **查看:** Google 地图
config.unityads.unity3d.com	安全	否	**IP地址:** 43.224.167.60 **国家:** Hong Kong **地区:** Hong Kong **城市:** Hong Kong **纬度:** 22.285521 **经度:** 114.157692 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• javascript:window.nativebridge.receiveEvent(	com/unity3d/services/ads/webplayer/WebPlayerView.java
• https://config.unityads.unitychina.cn/webview/ • https://config.unityads.unity3d.com/webview/	com/unity3d/services/core/properties/SdkProperties.java
• javascript:window.	com/unity3d/services/core/webview/WebViewApp.java
• https://t.me/vip_nobita_f • https://youtube.com/@VIPNOBITAFF?si=Aa0FPqg066tjckuz • https://www.instagram.com/vipnobitaff • https://youtube.com/@VIPNOBITAFF?si=YYWIU_9K_06YiBqa • https://dupload.net/o6fbxt8rnht	com/vip/nobita/ff/MainActivity.java
• javascript:window. • https://config.unityads.unity3d.com/webview/ • javascript:window.nativebridge.receiveEvent(• https://config.unityads.unitychina.cn/webview/	自研引擎分析结果

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Unity Ads	Unity Technologies	Unity Ads SDK 由领先的移动游戏引擎创建，无论您是在 Unity、xCode 还是 Android Studio 中进行开发，都能为您的游戏提供全面的变现服务框架。
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。

第三方追踪器检测

名称	类别	网址
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121

免责声明及风险提示: