



ANDROID 静态分析报告



Talking Hippo v1.0

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析日期: 2025-04-04 07:08:46

i应用概览

文件名称:	Talking Hippo v1.0.apk
文件大小:	4.35MB
应用名称:	Talking Hippo
软件包名:	com.outfit7.talkinghippo
主活动:	BackgroundActivity
版本号:	1.0
最小SDK:	3
目标SDK:	4
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	40/100 (中风险)
跟踪器检测:	1/432
杀软检测:	36 个杀毒软件报毒
MD5:	d9f5806497a4104cd8064dc506149865
SHA1:	51f20479787ab130832dfe0b8da1c938d61a833
SHA256:	39b8fed38694656c1b0b7aa87bcdcb68194dfe53785ce5c14e2c4cf8e51e045

📊 分析结果严重性分布

🚨 高危	⚠️ 中危	ℹ️ 信息	✅ 安全	🔍 关注
5	21	1	0	0

📦 四大组件导出状态统计

Activity组件: 13个, 其中export的有: 12个
Service组件: 1个, 其中export的有: 0个
Receiver组件: 1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

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=IT, ST=Unknown, L=Unknown, O=Obfuscapk, OU=Obfuscapk, CN=Obfuscapk

签名算法: rsassa_pkcs1v15

有效期自: 2019-08-15 18:58:38+00:00

有效期至: 2049-08-07 18:58:38+00:00

发行人: C=IT, ST=Unknown, L=Unknown, O=Obfuscapk, OU=Obfuscapk, CN=Obfuscapk

序列号: 0x5f122eb3

哈希算法: sha256

证书MD5: 654f7f55899d0720aa524e768e0e98cf

证书SHA1: 09dceb70d91de79335b6c143d05f9a6b6de9e59c

证书SHA256: ed1399b288d3aac9ef9d43fc9fbf90c7662b3ed0050b08f3c2988d24a8a42c9

证书SHA512:

348846cd1573e362aa88d7dc65ffc1b1c47cee87281355719db7f0c4c08c0d7f16ad1f581eb172fb2a5250680b7880eadbb0172cf31064f381847de324e225e2

公钥算法: rsa

密钥长度: 2048

指纹: fbb4874e266f7bb91caf414a03f58255e03f169ab8a45998a39083de7a09990f

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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
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.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。
com.android.vending.CHECK_LICENSE	未知	未知权限	来自 android 引用的未知权限。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。

android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
android.permission.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
com.android.browser.permission.READ_HISTORY_BOOKMARKS	危险	获取自带浏览器上网记录	恶意代码可有利用此权限窃取用户的上网记录和书签。
com.android.browser.permission.WRITE_HISTORY_BOOKMARKS	危险	修改自带浏览器上网记录	恶意代码可有利用此权限篡改用户的上网记录和书签。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在50~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.ACCESS_GPS	签名(系统)	使用GPS权限	这个权限已经被废弃，不再被系统支持。这个权限曾经用于访问GPS位置，但是现在已经被 android.permission.ACCESS_FINE_LOCATION 替代。
android.permission.ACCESS_LOCATION	未知	未知权限	来自 android 引用的未知权限。

🔒 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
已签名应用	信息	应用程序使用代码签名证书进行签名

🔍 Manifest 配置安全分析

高危: 2 | 警告: 14 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	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。
2	Activity (.Main) 的启动模式不是Standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。

3	Activity (.Main) 容易受到 Android Task Hijacking/StrandHogg 的攻击。	高危	活动不应将启动模式属性设置为“singleTask”。然后，其他应用程序可以将恶意活动放置在活动栈顶部，从而导致任务劫持/StrandHogg 1.0 漏洞。这使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”或设置空 taskAffinity (taskAffinity=“”) 属性来修复此漏洞。您还可以将应用的目标 SDK 版本 (4) 更新到 28 或更高版本以在平台级别修复此问题。
4	Activity (.Main) 未被保护。存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
5	Activity (AnimationPlayer) 未被保护。存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
6	Activity (YouTubeLoginActivity) 未被保护。存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
7	Activity (Info) 未被保护。存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
8	Activity (VideoCommentActivity) 未被保护。存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
9	Activity (News) 未被保护。存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
10	Activity (VideoUploadedToFacebookActivity) 未被保护。存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
11	Activity (VideoUploadedToYouTubeActivity) 未被保护。存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
12	Activity (Grid) 未被保护。存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
13	Activity (GridProxy) 未被保护。存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
14	Activity (Menu) 未被保护。存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
15	Broadcast Receiver (com.geinimi.GeinimiServiceReceiver) 未被保护。存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
16	Activity (com.geinimi.custom.Ad3019_30190001) 未被保护。存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。

</> 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
2	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
3	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
4	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
5	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
6	使用弱加密算法	高危	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
7	该文件是World Writable，任何应用程序都可以写入文件	高危	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
8	MD5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

9	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
---	----------------------------------	----	--	-----------------------------

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	armeabi/libsoundtouch.so	<p>True info</p> <p>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。</p>	<p>动态共享对象(DSO) info</p> <p>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。</p>	<p>True info</p> <p>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。</p>	<p>No RELRO high</p> <p>此共享对象未启用RELRO。整个GOT(.got和.got.plt)都是可写的。如果没有此编译器标志，全局变量上的缓冲区溢出可能会覆盖GOT条目。使用选项-z,relro,-z,now启用完整RELRO，仅使用-z,relro启用部分RELRO。</p>	No	No	<p>False warning</p> <p>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。</p>	False
---	--------------------------	--	--	--	--	----	----	--	-------

应用行为分析

编号	行为	标签	文件
00022	从给定的文件绝对路径打开文件	文件	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
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
00013	读取文件并将其放入流中	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
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
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
00030	通过给定的URL连接到远程服务器	网络	升级会员：解锁高级权限
00153	通过HTTP发送二进制数据	http	升级会员：解锁高级权限
00094	连接到URL并从中读取数据	命令 网络	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
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00003	将压缩后的位图数据放入JSON对象中	相机	升级会员：解锁高级权限
00123	连接到远程服务器后将响应保存为 JSON	网络命令	升级会员：解锁高级权限
00115	获取设备的最后已知位置	信息收集位置	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集联系人	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集短信 通话记录 日历	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集通话记录	升级会员：解锁高级权限
00074	获取 IMSI 和 ISO 国家代码	信息收集电话服务	升级会员：解锁高级权限
00146	获取网络运营商名称和 IMSI	电话服务信息收集	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集电话服务	升级会员：解锁高级权限
00038	查询电话号码	信息收集	升级会员：解锁高级权限
00034	查询当前数据网络类型	信息收集网络	升级会员：解锁高级权限
00117	获取 IMSI 和网络运营商名称	电话服务信息收集	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00065	获取SIM卡提供商的国家代码	信息收集	升级会员：解锁高级权限
00066	查询ICCID号码	信息收集	升级会员：解锁高级权限
00067	查询IMSI号码	信息收集	升级会员：解锁高级权限
00084	获取 ISO 国家代码和 IMSI	信息收集电话服务	升级会员：解锁高级权限
00132	查询ISO国家代码	电话服务信息收集	升级会员：解锁高级权限
00015	将缓冲流（数据）放入 JSON 对象	文件	升级会员：解锁高级权限

00193	发送短信	短信	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	11/30	android.permission.RECORD_AUDIO android.permission.GET_TASKS android.permission.READ_PHONE_STATE android.permission.ACCESS_FINE_LOCATION android.permission.CALL_PHONE android.permission.READ_CONTACTS android.permission.READ_SMS android.permission.SEND_SMS android.permission.SET_WALLPAPER android.permission.WRITE_CONTACTS android.permission.ACCESS_COARSE_LOCATION
其它常用权限	4/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE com.android.launcher.permission.INSTALL_SHORTCUT

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.mobclix.com	安全	否	IP地址: 52.219.116.67 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
vc.mobclix.com	安全	否	No Geolocation information available.
i.ytimg.com	安全	否	IP地址: 142.250.68.54 国家: 美国 地区: 加利福尼亚 城市: 洛杉矶 纬度: 34.052570 经度: -118.243904 查看: Google 地图
data.mobclix.com	安全	否	No Geolocation information available.
outfit7-affirmations.appspot.com	安全	否	IP地址: 142.250.217.148 国家: 美国 地区: 佛罗里达州 城市: 迈阿密 纬度: 25.774269 经度: -80.193604 查看: Google 地图

search.yahoo.com	安全	否	IP地址: 98.136.144.138 国家: 美国 地区: 纽约 城市: 纽约市 纬度: 40.731323 经度: -73.990089 查看: Google 地图
ads.mobclix.com	安全	否	No Geolocation information available.

🌐 URL 链接安全分析

URL信息	源码文件
<ul style="list-style-type: none"> • http://www.facebook.com/connect/prompt_permissions.php 	com/codecarpet/fbconnect/FBPermissionDialog.java
<ul style="list-style-type: none"> • http://www.mobclix.com 	com/mobclix/android/sdk/MobclixBrowseActivity.java
<ul style="list-style-type: none"> • http://data.mobclix.com/post/senddata • http://data.mobclix.com/post/config • http://vc.mobclix.com • http://ads.mobclix.com/ • http://data.mobclix.com/post/feedback 	com/mobclix/android/sdk/Mobclix.java
<ul style="list-style-type: none"> • http://www.facebook.com/login.php 	com/codecarpet/fbconnect/FBLoginDialog.java
<ul style="list-style-type: none"> • http://www.facebook.com/connect/prompt_feed.php 	com/codecarpet/fbconnect/FBFeedDialog.java
<ul style="list-style-type: none"> • https://api.facebook.com/restserver.php • http://api.facebook.com/restserver.php 	com/codecarpet/fbconnect/FBSession.java
<ul style="list-style-type: none"> • https://api.facebook.com/restserver.php • https://www.facebook.com/connect/user.php • https://graph.facebook.com/oauth/authorize • https://graph.facebook.com/ 	com/a/a/e.java
<ul style="list-style-type: none"> • http://search.yahoo.com/nrs/ • https://www.google.com/youtube/accounts/client/sign 	com/outfit7/b/a.java
<ul style="list-style-type: none"> • http://api-video.facebook.com/restserver.php 	com/outfit7/talkinghippo/ar.java
<ul style="list-style-type: none"> • http://i.yimg.com/vi/ 	com/outfit7/talkinghippo/dn.java
<ul style="list-style-type: none"> • http://www.facebook.com/plugins/likebox.php?width=292&connections=0&stream=false&header=true 	com/outfit7/talkinghippo/VideoUploadedToFbActivity.java
<ul style="list-style-type: none"> • https://outfit7-affirmations.appspot.com/rest/talkingfriends/v1/android/?appname=talkingbabyhippo&model= • http://outfit7-affirmations.appspot.com/rest/v1/news/android/talking/en/?appname=talkingbabyhippo&did= 	com/outfit7/talkinghippo/TalkingHippoApplication.java

📦 第三方 SDK 组件分析

SDK名称	开发者	描述信息
SoundTouch	Olli Parviainen	SoundTouch 是开源音频处理库，用于更改音频流或音频文件的节奏、音调和播放速度，以及较准确地估计音轨的 BPM。

🕵️ 第三方追踪器检测

名称	类别	网址
Axonix		https://reports.exodus-privacy.eu.org/trackers/226

🔑 敏感凭证泄露检测

可能的密钥
"yt_field_username" : "Username:"
"yt_field_password" : "Password:"
77d49fd04a3d23d0953e03aa0500a5df
078e67147c67ccf83e20f257542b75d2
jj54m5V32xBLZH2cweZF8DMuwpYjNpWJSpLsSUCfTCfkCUuhokFvxFLBq3mWlND7Q
boundary=3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f
3i2ndDfv2rTHiSisAbouNdArYfORhtTPEefj3q2f

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，深入扫描软件中潜在的漏洞和安全隐患。

© 2025 南明离火 - 移动安全分析平台自动生成