南明离火
移动应用检测平台

ANDROID 静态分析报告

EhViewer • v1.0.9.8

分析日期: 2025-05-15 15:46:52

应用概览

文件名称:	EhViewer v1.9.9.8.apk
文件大小:	23.48MB
应用名称:	EhViewer
软件包名:	com.xjs.ehviewer
主活动:	com.hippo.ehviewer.ui.splash.SplashActivity
版本号:	1.9.9.8
最小SDK:	23
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:	45/100 (中风险)
跟踪器检测:	2/432
杀软检测:	7 个杀毒软件报毒
MD5:	f081a6a2dec0158a2676490c211c87f4
SHA1:	9260250146ea70422eeb58a7a05d42c5978e35e7
SHA256:	ab93fe27ca604df5a2b0b8de85be2c33a402e5c86817b25ec222d59f0279030

分析结果严重性分布

高危	中危	信息	安全	关注
5	17	3	2	0

四大组件导出状态统计

Activity组件：17个，其中export的有： 2个
Service组件：7个，其中export的有： 0个
Receiver组件：4个，其中export的有： 1个
Provider组件：3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=inject, ST=inject, L=inject, O=inject, OU=inject, CN=inject.keystore
签名算法: rsassa_pkcs1v15
有效期自: 2019-10-11 02:39:57+00:00
有效期至: 2841-02-23 02:39:57+00:00
发行人: C=inject, ST=inject, L=inject, O=inject, OU=inject, CN=inject.keystore
序列号: 0x47f931c3
哈希算法: sha256
证书MD5: 64843786c6ada15ca4254f4da77e4978
证书SHA1: b2e643d00042e8e23481794e88eedd3966c65dfa
证书SHA256: 28afa96de62296ef3b7598b27d00b673920d3e0bf5fad9c95ad4ef8de5d8df99
证书SHA512:
2bcfcb9c6759eb8689d05d7f2393725c1ebea61bf8c4559c9057dc654ad28c1c776ddbe55a6f8a6af71968f2883555e7a14e6c588854a5a2c275ddb4cf0536d2

公钥算法: rsa
密钥长度: 1024
指纹: 61cc7d71417395a5265a787e508b72c4fdc6d6d0107c97d17221206671ae528f
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.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.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
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。
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.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.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
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.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
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.ACCESS_DOWNLOAD_MANAGER	签名(系统)	访问下载管理器	这个权限是允许应用访问下载管理器，以便管理大型下载操作。
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。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。

android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
com.xjs.ehviewer.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
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.BIND_VPN_SERVICE	签名	VpnServices 需要进行系统绑定	必须是VpnService, 以确保只有系统可以绑定到它。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	文件列表访问权限	Android11新增权限，读取本地文件，如简历，聊天图片。
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.hippo.ehviewer.ui.MainActivity	Schemes: http://, https://, Hosts: exhentai.org, e-hentai.org, g.e-hentai.org, lofi.e-hentai.org, Mime Types: text/plain, image/*,
com.hippo.ehviewer.ui.GalleryActivity	Schemes: file://, content://, Hosts: *, Mime Types: application/octet-stream, application/7z, application/rar, application/zip, application/x-7z-compressed, application/x-rar-compressed, application/x-zip-compressed, */*, Path Patterns: .*\\.7z, .*\\.rar, .*\\.zip,

网络通信安全风险分析

高危: **2** | 警告: **1** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	警告	基本配置配置为信任系统证书。
2	*	高危	基本配置配置为信任用户安装的证书。
3	*.ehtracker.org	高危	域配置不安全地配置为允许明文流量到达范围内的这些域。

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	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **3** | 警告: **5** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用允许明文网络流量（如 HTTP、FTP 协议、DownloadManager、MediaPlayer 等）。API 级别 27 及以下默认启用，28 及以上默认禁用。明文流量缺乏机密性、完整性和真实性保护，攻击者可窃听或篡改传输数据。建议关闭明文流量，仅使用加密协议。
2	应用已配置网络安全策略 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
3	应用数据允许备份 [android:allowBackup=true]	警告	该标志允许通过 adb 工具备份应用数据。启用 USB 调试的用户可直接复制应用数据，存在数据泄露风险。
4	Activity (com.hippo.ehviewer.ui.splash.SplashActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。
5	Activity (com.hippo.ehviewer.ui.MainActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。
6	Activity (com.hippo.ehviewer.ui.MainActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
7	Activity (com.hippo.ehviewer.ui.GalleryActivity) 易受 StrandHogg 2.0 攻击	高危	检测到 Activity 存在 StrandHogg 2.0 任务劫持漏洞。攻击者可将恶意 Activity 置于易受攻击应用的任务栈顶部，使应用极易成为钓鱼攻击目标。可通过将启动模式设置为 "singleInstance" 并将 taskAffinity 设为空（taskAffinity=""），或将应用的 target SDK 版本（28）升级至 29 及以上，从平台层面修复该漏洞。
8	Activity (com.hippo.ehviewer.ui.GalleryActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
9	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限的保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 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: **0** | 警告: **9** | 信息: **2** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
2	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
3	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
4	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
5	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
6	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
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
9	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

10	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
11	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
12	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	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/libehviewer.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	True info 符号被剥离
2	arm64-v8a/libp7zip-extract-lite.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	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
00163	创建新的 Socket 并连接到它	socket	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
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

00088	创建到给定主机地址的安全套接字连接	命令 网络	升级会员：解锁高级权限
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
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 控制	升级会员：解锁高级权限
00046	方法反射	反射	升级会员：解锁高级权限
00047	查询本地IP地址	网络 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
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	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
00109	连接到 URL 并获取响应代码	网络 命令	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
00036	从 res/raw 目录获取资源文件	反射	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	4/30	android.permission.WAKE_LOCK android.permission.CAMERA android.permission.REQUEST_INSTALL_PACKAGES android.permission.READ_PHONE_STATE

本报告由南明离火移动安全分析平台生成

其它常用权限	9/46	android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.ACCESS_WIFI_STATE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE android.permission.REORDER_TASKS

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
upld.e-hentai.org	安全	否	**IP地址:** 104.21.48.1 **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
exhentai.org	安全	否	**IP地址:** 104.21.48.1 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
jsoup.org	安全	否	**IP地址:** 104.21.48.1 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
upld.exhentai.org	安全	否	**IP地址:** 104.21.48.1 **国家:** 摩尔多瓦（共和国） **地区:** 基希讷乌 **城市:** 基希讷乌 **纬度:** 47.006042 **经度:** 28.856674 **查看:** Google 地图
ehwiki.org	安全	否	**IP地址:** 172.67.187.219 **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

comxjsehviewer.firebaseio.com	安全	否	**IP地址:** 34.120.206.254 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
e-hentai.org	安全	否	**IP地址:** 104.21.48.1 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.ccil.org	安全	否	**IP地址:** 172.250.189.19 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
forums.e-hentai.org	安全	否	**IP地址:** 104.21.48.1 **国家:** 美国 **地区:** 加利福尼亚 **城市:** SeverinCarazoCarchiCarlowCarolina Cartago **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
ehgt.org	安全	否	**IP地址:** 172.67.187.219 **国家:** 荷兰（王国） **地区:** 南荷兰省 **城市:** 纳尔德韦克 **纬度:** 51.994064 **经度:** 4.209895 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• 172.64.102.249 • 104.18.115.242	mirrorb/android/service/persistentdata/C0106.java
• 162.159.38.227	mirrorb/android/service/persistentdata/C0068.java
• 162.159.38.227	mirrorb/android/service/persistentdata/C0107.java
• 1.9.9.8	com/hippo/ehviewer/BuildConfig.java

• http://www.ccil.org/~cowan/tagsoup/features/bogons-empty • http://www.ccil.org/~cowan/tagsoup/features/translate-colons • http://www.ccil.org/~cowan/tagsoup/features/root-bogons • http://www.ccil.org/~cowan/tagsoup/properties/schema • http://www.ccil.org/~cowan/tagsoup/features/cdata-elements • http://www.ccil.org/~cowan/tagsoup/properties/scanner • http://www.ccil.org/~cowan/tagsoup/features/default-attributes • http://www.ccil.org/~cowan/tagsoup/properties/auto-detector • http://www.ccil.org/~cowan/tagsoup/features/ignorable-whitespace • http://www.ccil.org/~cowan/tagsoup/features/restart-elements • http://www.ccil.org/~cowan/tagsoup/features/ignore-bogons	org/ccil/cowan/tagsoup/Parser.java
• 162.159.253.217	mirrorb/android/view/accessibility/C0111.java
• 162.159.253.217	mirrorb/android/view/accessibility/C0072.java
• 104.21.231.104	mirrorb/android/os/storage/C0096.java
• https://github.com/xiaojieonly/ehviewer_cn_sxj/blob/bili_pc_gamer/readme.md • https://github.com/xiaojieonly/ehviewer_cn_sxj/releases	com/hippo/ehviewer/ui/dialog/UpdateDialog.java
• https://exhentai.org/img/kokomade.jpg • https://forums.e-hentai.org/index.php?act=login&code=00 • https://forums.e-hentai.org	com/hippo/ehviewer/client/EhEngine.java
• 104.21.231.104	mirrorb/android/os/storage/C0057.java
• 172.64.197.29	mirrorb/android/media/session/C0087.java
• 104.19.109.228	mirrorb/android/net/wifi/C0053.java
• 104.19.109.228	mirrorb/android/net/wifi/C0092.java
• 172.64.197.29	mirrorb/android/media/session/C0048.java

• https://exhentai.org/toplist.php • https://exhentai.org/t/ • https://e-hentai.org/toplist.php • https://ehgt.org/ • https://e-hentai.org/favorites.php • https://e-hentai.org/popular • https://exhentai.org/favorites.php • https://forums.e-hentai.org/index.php?act=login&code=01 • https://e-hentai.org/news.php • https://exhentai.org/uconfig.php • https://forums.e-hentai.org/index.php?act=reg&code=00 • https://e-hentai.org/api.php • https://forums.e-hentai.org/ • https://exhentai.org/watched • https://e-hentai.org/ • https://upld.e-hentai.org/image_lookup.php • https://e-hentai.org/uconfig.php • https://exhentai.org/api.php • https://e-hentai.org/watched • https://exhentai.org • https://exhentai.org/home.php • https://e-hentai.org/mytags • https://exhentai.org/ • https://ehwiki.org/wiki/ • https://forums.e-hentai.org/index.php?act=login • https://upld.exhentai.org/upld/image_lookup.php • https://e-hentai.org • https://exhentai.org/mytags • https://exhentai.org/popular • https://e-hentai.org/home.php	com/hippo/ehviewer/client/EhUrl.java
• 104.18.124.253	com/cloudinject/customview/C0020.java
• https://www.google.com/recaptcha/api/challenge?k= • https://www.google.com/recaptcha/api/image	com/hippo/android/recaptcha/RecaptchaV1Task.java

• 151.101.128.133 • 178.175.128.253 • 178.162.145.152 • 178.175.128.252 • 62.112.8.21 • 178.162.139.34 • 178.175.132.22 • 178.175.129.251 • 104.20.18.168 • 94.100.18.247 • 178.175.132.21 • 178.175.132.19 • 151.101.192.133 • 151.101.0.133 • 178.175.128.251 • 89.39.106.43 • 151.101.64.133 • 104.20.19.168 • 94.100.18.249 • 178.162.139.33 • 178.175.132.20 • https://77.88.8.1/dns-query • 178.162.145.131 • 94.100.28.57 • 178.175.129.254 • 104.24.56.202 • 178.175.128.254 • 178.162.139.36 • 178.175.129.253 • 172.67.2.238 • 94.100.29.73 • 178.175.129.252 • 109.236.85.28 • 94.100.18.243 • 178.162.145.132	com/hippo/ehviewer/client/EhHosts.java
• 104.18.124.243	com/cloudinject/customview/C0026.java
• 172.64.136.152	mirrorb/android/security/net/config/C0065.java
• 172.64.102.243 • 104.18.115.242	mirrorb/android/service/persistentdata/C0067.java

• 172.64.203.72	mirrorb/android/hardware/display/C0085.java
• 172.64.136.152	mirrorb/android/security/net/config/C0104.java
• 104.22.31.162	mirrorb/java/io/C0091.java
• 172.64.109.246	mirrorb/android/bluetooth/C0081.java
• 104.19.78.48	mirrorb/android/providers/C0098.java
• 104.19.78.48	mirrorb/android/providers/C0059.java
• 104.22.31.162	mirrorb/java/io/C0130.java
• http://www.ccil.org/~cowan/tagsoup/properties/schema	com/hippo/text/Html.java
• 172.64.109.246	mirrorb/android/bluetooth/C0042.java
• 104.19.244.87	mirrorb/android/app/job/C0071.java
• 172.64.139.148	mirrorb/android/app/job/C0029.java
• 192.168.43.1	com/hippo/ehviewer/ui/wifi/WiFiServerActivity.java
• http://undefined/ • https://jsoup.org/cookbook/extracting-data/working-with-urls	org/jsoup/helper/HttpConnection.java
• 172.64.139.148	mirrorb/android/app/job/C0068.java
• 127.0.0.1	com/hippo/ehviewer/client/data/ListUrlBuilder.java
• 104.19.244.87	mirrorb/android/app/job/C0032.java
• 104.19.31.141	mirrorb/android/rms/C0064.java
• 104.19.31.141	mirrorb/android/rms/C0103.java
• 104.18.127.20	mirrorb/android/rms/C0063.java
• 104.18.127.20	mirrorb/android/rms/C0102.java
• 104.19.81.88	mirrorb/android/webkit/C0073.java
• 172.64.203.72	mirrorb/android/hardware/display/C0046.java
• 172.64.141.217	mirrorb/android/graphics/drawable/C0045.java
• 162.159.243.216	mirrorb/android/webkit/C0113.java
• 172.64.110.164	mirrorb/android/app/servertransaction/C0077.java
• 172.64.110.164	mirrorb/android/app/servertransaction/C0038.java

• 104.21.234.149	mirrorb/android/app/role/C0074.java
• 172.64.141.217	mirrorb/android/graphics/drawable/C0084.java
• 104.21.234.149	mirrorb/android/app/role/C0035.java
• 104.19.81.88	mirrorb/android/webkit/C0112.java
• 162.159.243.215	mirrorb/android/webkit/C0074.java
• https://comxjsehviewer.firebaseio.com • https://placeholder • https://www.google.com/policies/privacy/ • https://github.com/mapaler/ehtagtranslator/wiki	自研引擎-S

Firebase 配置安全检测

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://comxjsehviewer.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/902803992147/namespaces/firebase:fetch?key=AIzaSyDkOHaCpY6XWdBnzzrycasyg4T3q8pGHZs ） 已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Conscrypt	Google	Conscrypt 是一个 Java 安全提供程序 (JSP)，它实现了部分 Java 加密扩展 (JCE) 和 Java 安全套接字扩展 (JSSE)。它使用 BoringSSL 为 Android 和 OpenJDK 上的 Java 应用程序提供加密原语和传输层安全性 (TLS)。有关所提供内容的详细信息，请参阅功能文档。
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。
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。
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).

第三方追踪器检测

名称	类别	网址
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
"key_posted" : "Publicado"
"settings_about_author" : "Entwickler"
"key_title" : "Titel"
"key_visible" : "Sichtbar?"
"google_crash_reporting_api_key" : "AIzaSyDIOHaCpY6XWdBnzznycasyg4T3q8pGHZs"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"key_url" : "Url"
"username" : "Benutzername"
"key_token" : "Token"
"username" : "Usuario"
"key_size" : "Size"
"key_pages" : "Pages"
"key_category" : "Kategorie"
"header_key" : "Key"
"username" : "Username"
"key_posted" : "Posted"
"google_app_id" : "1:902803992147:android:17f3d7271db705d396e0a6"
"google_api_key" : "AIzaSyDIOHaCpY6XWdBnzznycasyg4T3q8pGHZs"
"key_category" : "Category"

"key_favorited" : "Favorited"
"key_torrents" : "Torrents"
"key_language" : "Idioma"
"key_language" : "Sprache"
"key_rating" : "Bewertung"
"key_pages" : "Seiten"
"header_key" : "Clave"
"password" : "Kennwort"
"key_rating" : "Rating"
"key_favorited" : "Favorito"
"key_title" : "Titre"
"key_posted" : "Hochladungsdatum"
"key_parent" : "Elternteil"
"key_language" : "Language"
"key_visible" : "Visible"
"key_gid" : "GID"
"key_thumb" : "Vorschau"
"key_language" : "Langue"
"key_thumb" : "Miniatura"
"key_gid" : "Gid"
"key_url" : "URL"
"key_torrent_url" : "Torrent"
"key_rating" : "Notation"
"key_parent" : "Parent"
"firebase_database_url" : "https://comixfenviewer.firebaseio.com"
"key_token" : "Clave"
"key_title" : "Title"
"password" : "Password"
"settings_about_author" : "Author"
"settings_about_author" : "Autor"

"key_uploader" : "Uploader"
"key_size" : "Taille"
"key_thumb" : "Thumb"
"key_parent" : "Padre"
WebKitFormBoundaryU7CgQs9WnqlZYKs6
0df18c17d79aca1b65c8a70136f788ca871f646a86e5939bf879610ad6834f895f2057262991f4bc
d577377e4c1a566df58500c2056b7152
5oKo55qE5pSv5oyB5piv5oiR5pu05paw55qE5pyA5aSn5Yqo5Yqb77yM5oKo5Y+v5Lul5oiq5Zu+5ZCO5Zyo5b6u5L+h5oiW5pSv5LuY5a6d5Lit5omr5o+P5LqM57u056CB5o+Q5L6b546w6YeR5pSv5oyB77yM5Lmf5Y+v6YCa6L+H6YKu566x5Y+R6YCB5aW955uu5YmN5piv5LiN5aW955So55qE5Yqf6IO977yM5oiR5Lya5LiA5LiA5Zue5aSN5bm25YGa5Ye65Sf6LCi44CCKCDigKLMgCDPiSDigKLMgSAp4pyn
71cfeaed8cbdee2e0000242d50cf1f9f

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。