南明离火
移动应用检测平台

ANDROID 静态分析报告

Youtube plugin • v40.66.72.42

分析日期: 2024-03-26 12:13:14

应用概览

文件名称:	youtube_plugin signed.apk
文件大小:	0.91MB
应用名称:	Youtube plugin
软件包名:	css.contains.lp
主活动:	not_found_main_activity!!
版本号:	40.66.72.42
最小SDK:	16
目标SDK:	29
加固信息:	未加壳
应用程序安全分数:	41/100 (中风险)
杀软检测:	28 个杀毒软件报毒
MD5:	7f8ecf5a6921f1df4bece49a46c94586
SHA1:	e0edc04ebb159130494c092b827e218a3534c42f
SHA256:	3a01a39e80cc5f24735ac74852[illegible]a9ced0f95622fed331f7ec42fffdf898a9

分析结果严重性分布

高危	中危	信息	安全	关注
6	21	1	1	0

四大组件导出状态统计

Activity组件：16个，其中export的有：4个
Service组件：8个，其中export的有：2个
Receiver组件：6个，其中export的有： 6个
Provider组件：1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: CN=ffffffff OU=fffffffff O=ddddddddd L=ddddddddd S=aaaaaaaaaa C=sssssss
签名算法: rsassa_pkcs1v15
有效期自: 2023-07-01 23:07:31+00:00
有效期至: 2048-06-24 23:07:31+00:00
发行人: CN=ffffffff OU=fffffffff O=ddddddddd L=ddddddddd S=aaaaaaaaaa C=sssssss
序列号: 0xc9d7f3b
哈希算法: sha256
证书MD5: c0b9bebbdee65707797c1f63babaebb7
证书SHA1: 0905a5719778e01073f97be612a2572df1f16b97
证书SHA256: 345e185b87581fa4e1690079d615d0dcabb90f7440c4e712fe237252b186cf5e
证书SHA512:
fda7f401b16d0a85f2c042b8ca2ad558d7ee973f675749e121653aaf5cce01e8e19882732be14a2afc5bb0a929f9ed3feb70d80423660d2b9d15fb7b411db997

公钥算法: rsa
密钥长度: 2048
指纹: 5c90f98d6aaf571dba90ad7c41a8dd6e6f02c8c42341cdbe696ed17f4459b6a3
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.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.PROCESS_OUTGOING_CALLS	危险	拦截外拨电话	允许应用程序处理外拨电话或更改要拨打的号码。恶意应用程序可能会借此监视、另行转接甚至阻止外拨电话。
android.permission.SET_WALLPAPER	普通	设置壁纸	允许应用程序设置壁纸。
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.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.READ_CONTACTS	危险	读取联系人信息	允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.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
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错略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
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.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。
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.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.BACKGROUND_ACTIVITY_STARTER	未知	未知权限	来自 android 引用的未知权限。
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。
oppo.permission.OPPO_COMPONENT_SAFE	签名	特定于 OPPO 设备的权限	它用于授予应用访问某些系统级功能或组件的能力，否则这些功能或组件会因安全原因而受到限制。此权限可确保只有受信任的应用程序才能与 OPPO 系统的敏感部分进行交互。
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.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.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.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.alarm.permission.SET_ALARM	未知	未知权限	来自 android 引用的未知权限。
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。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
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.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。
android.permission.REQUEST_DELETE_PACKAGES	普通	请求删除应用	允许应用程序请求删除包。
android.permission.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。

可浏览 Activity 组件分析

ACTIVITY	INTENT
css.contacts.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.vvzaidrczndvjufmudjbpfudajnfxqibfdlgoojhxayenuszxj20	Schemes: rating://,

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
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: **3** | 警告: **16** | 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 4.1-4.1.2, [minSdk=16]	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	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/netsecconfig]	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。
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。
4	Activity (css.contains.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.wzaidrczndvjufmudjbqfuajnfxqibfdlgoojhxzvenuszxj20) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
5	Activity (css.contains.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.omhysmndikomszxabinvxuwqeodvjulurmxoetaxoizwdmyyh14_CA) 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。
6	Activity (css.contains.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.omhysmndikomszxabinvxuwqeodvjulurmxoetaxoizwdmyyh14_CA) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。

7	Activity (css.contains.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.odhiaoprlwlhrqxgcwngvktojfpdqcciqsivycnuwnhckdfoqb72_SCA) 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。
8	Activity (css.contains.MainActive) 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。
9	Activity-Alias (css.contains.MainActive) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
10	Activity-Alias (css.contains.costm) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
11	Service (css.contains.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.uehaivcakrsbgyjwmgiihucgxphjzyhhptiokizubybplfdcyd5.odhiaoprlwlhrqxgcwngvktojfpdqcciqsivycnuwnhckdfoqb7_WKJ) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
12	Broadcast Receiver (css.contains.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.uehaivcakrsbgyjwmgiihucgxphjzyhhptiokizubybplfdcyd5.SRodhiaoprlwlhrqxgcwngvktojfpdqcciqsivycnuwnhckdfoqb74B) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
13	Service (css.contains.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.bixkrzdlzslmkakkfubyjdvarhzmsbscrnvsynscatbrkzlkech3.odhiaoprlwlhrqxgcwngvktojfpdqcciqsivycnuwnhckdfoqb72) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_ACCESSIBILITY_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

本报告由南明离火移动安全分析平台生成

14	Broadcast Receiver (css.contains.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.uehaivcakrsbgyjwmgiihucgxphjzyhhptiokizubybplfdcyd5.odhiaoprlwlhrqxgcwngvktojfpdqcciqsivycnuwnhckdfoqb7) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
15	Broadcast Receiver (css.contains.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.uehaivcakrsbgyjwmgiihucgxphjzyhhptiokizubybplfdcyd5.omhysmndikomszxabinvxuuwqeodvjulurmxoetaxoizwdmyyh14_RC) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
16	Broadcast Receiver (css.contains.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.uehaivcakrsbgyjwmgiihucgxphjzyhhptiokizubybplfdcyd5.odhiaoprlwlhrqxgcwngvktojfpdqcciqsivycnuwnhckdfoqb74) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
17	Broadcast Receiver (css.contains.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.ianbrlnlzizszfkaztiqouywscqdvmrdrfdovxkgrymrurcwsv33) 未被保护。[android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此使其对设备上的任何其他应用程序都可访问。
18	Broadcast Receiver (css.contains.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.uehaivcakrsbgyjwmgiihucgxphjzyhhptiokizubybplfdcyd5.odhiaoprlwlhrqxgcwngvktojfpdqcciqsivycnuwnhckdfoqb7_AR) 受权限保护，但是应该检查权限的保护级别。Permission: android.permission.BIND_DEVICE_ADMIN [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

19	Service (css.contains.edmwetyobeekowsiqodvakdnocjumuvmqftvbhiokpawzmpear2.bjxkzflzslmkakkfubyjdvarhzmsbscrnvsynscatbrkzlkech3.Slggdaqlzkiugpehbtqjuxlgarosehjucsjhwzyvjpkpxqahder6IME) 受权限保护, 但是应该检查权限的保护级别。Permission: android.permission.BIND_INPUT_METHOD [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
20	高优先级的Intent (999) [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

代码安全漏洞检测

高危: **2** | 警告: **3** | 信息: **1** | 安全: **0** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
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	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	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

6	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	17/30	android.permission.SEND_SMS android.permission.PROCESS_OUTGOING_CALLS android.permission.SET_WALLPAPER android.permission.READ_SMS android.permission.READ_CALL_LOG android.permission.READ_CONTACTS android.permission.GET_ACCOUNTS android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CALL_PHONE android.permission.RECEIVE_BOOT_COMPLETED android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_PHONE_STATE android.permission.WAKE_LOCK android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	9/46	android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 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。

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。

敏感凭证泄露检测

可能的密钥

本报告由南明离火移动安全分析平台生成

谷歌地图的 "com.google.android.maps.v2.API_KEY" : "AIzaSyCGOJbGQ95SWrXxl8wk-_cRQZcJl42bvDU"
"google_api_key" : "AIzaSyCGOJbGQ95SWrXxl8wk-_cRQZcJl42bvDU"
"google_crash_reporting_api_key" : "AIzaSyCGOJbGQ95SWrXxl8wk-_cRQZcJl42bvDU"
"drawsdoexlangkshadowe711" : "oxidenscaxjpxmpmooomxsybtjlrab712"
"generatedauthorityv949" : "tiffanycuoetcohdlrchyxywamjmlxsf950"
aHR0cDovL3lvdGhlbWVzLnlvdXNlZmFsYmFzaGEuY29tL3NjcmVlbnMv

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患。