南明离火
移动应用检测平台

ANDROID 静态分析报告

如意 • v5.0.2

分析日期: 2024-05-16 15:31:04

概述

文件名称:	RY_2bb0b5af258ec74c5b7ead43f4ea802a.apk
文件大小:	60.13MB
应用名称:	如意
软件包名:	mtg1.ytc5ntuwntexy.tfmymuyz.uqjgpld
主活动:	h7dpvcbx.ehcmqsn9.i9devu0.saqby8f9.ix2swtpwq.MainActivity
版本号:	5.0.2
最小SDK:	23
目标SDK:	33
加固信息:	网易易盾
MD5:	aa4f4647ca5c07fe05239a2a297616f4
SHA1:	1d6aa3787cae9b402e0f9605aaa7239d20fb924c
SHA256:	ade488b135c23b8f2221a095a331506efde58a0720e81a69e43714f402fe61c7
应用程序安全分数:	58/100 (中风险)
杀软检测:	AI评估：很危险，请谨慎安装

分析结果严重性

高危	中危	信息	安全	关注
0	7	0	1	0

四大组件信息

Activity组件：48个，其中export的有： 0个
Service组件：2个，其中export的有： 1个
Receiver组件：4个，其中export的有： 3个
Provider组件：10个，其中export的有： 0个

证书信息

二进制文件已签名
v1 签名: False
v2 签名: True

v3 签名: False
v4 签名: False
主题: C=CN, ST=xoNUvyyANVtK, L=KPZtJpnBSCgi, O=rNdPKPOLfbqb, OU=cWCfdJTZgrlY, CN=daYkSaUwrhoc
签名算法: dsa
有效期自: 2024-05-16 01:57:54+00:00
有效期至: 2026-07-19 01:57:54+00:00
发行人: C=CN, ST=xoNUvyyANVtK, L=KPZtJpnBSCgi, O=rNdPKPOLfbqb, OU=cWCfdJTZgrlY, CN=daYkSaUwrhoc
序列号: 0x50a8762d
哈希算法: sha256
证书MD5: 41a2334de9a5038484550f7863228a5c
证书SHA1: ad0f2e50509b6bcce1dbffa33873e7df84700b28
证书SHA256: 54c7fbc2ac33319badb1b44d68d2638778cadab94d33fbce305d97e6b611c6e6
证书SHA512:
467d891ae55bdc5e97f525f199e7629c3be101ef95b6699a724a7adcf17e1e843a3cba6aef5de417faa1fa324274cc9875534574b38c960a912e294fcf8058f5

公钥算法: dsa
密钥长度: 2048
指纹: e1bef4d9bbf8daee54bb1cd0569fb238ae88bdae37683c03eb29efa7bc4a0206
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
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.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.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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
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.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.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.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。
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.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.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.PACKAGE_USAGE_STATS	签名	更新组件使用统计	允许修改组件使用情况统计
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.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.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。
mtg1.ytc5ntuwntexy.tfmymuyz.uqjgpld.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	未知权限	来自 android 引用的未知权限。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。

网络安全配置

序号	范围	严重级别	描述

证书分析

高危: **0** | 警告: **0** | 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

MANIFEST分析

高危: **0** | 警告: **6** | 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 6.0-6.0.1, [minSdk=23]	信息	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。
4	Broadcast Receiver (jdq.fibsaa.tngtnykvr.vkxehtmnffiurovpuwg.notification.ngbcbputpnaoaztblopckyvktg) 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，因此可被设备上的任何其他应用程序访问。
5	Broadcast Receiver (jdq.fibsaa.tngtnykvr.vkxehtmnffiurovpuwg.notification.dqsfokmqylqvpqceksxciriip) 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，因此可被设备上的任何其他应用程序访问。
6	Service (jdq.fibsaa.tngtnykvr.vkxehtmnffiurovpuwg.notification.inzjpcqgumpomgkmbun) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
7	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [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。

</> 源代码分析

序号	问题	等级	参考标准	文件位置

动态库分析

序号	动态库	NX(堆栈禁止执行)	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/libapp.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。	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	Not Applicable info RELRO 检查不适用于 Flutter/Dart 二进制文件	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 info 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	False warning 符号可用
2	arm64-v8a/libdownloadproxy.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。	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	False warning 符号可用

3	arm64-v8a/libijkhlscache-master.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。	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	False warning 符号可用
4	arm64-v8a/libkiwi.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。	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	False warning 符号可用

5	arm64-v8a/libkYlILUadeloone.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。	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	True info 二进制文件有以下加固函数: ['__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__memmove_chk', '__memset_chk', '__strncpy_chk']	False warning 符号可用
6	arm64-v8a/libtpcore-master.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。	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	False warning 符号可用

7	arm64-v8a/libtpthirdparties-master.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。	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	False warning 符号可用
8	arm64-v8a/libtxsoundtouch.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。	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	True info 二进制文件有以下加固函数: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	False warning 符号可用

滥用权限

类型	匹配	权限

恶意软件常用权限	13/30	android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.WRITE_SETTINGS android.permission.WAKE_LOCK android.permission.READ_PHONE_STATE android.permission.GET_TASKS android.permission.RECEIVE_BOOT_COMPLETED android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES android.permission.VIBRATE android.permission.PACKAGE_USAGE_STATS android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION
其它常用权限	9/46	android.permission.READ_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FLASHLIGHT android.permission.FOREGROUND_SERVICE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.CHANGE_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。

域名检测

域名	状态	中国境内	位置信息
api.flutter.dev	安全	否	**IP地址:** 199.36.158.100 **国家:** 美利坚合众国 **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

网址

网址信息	源码文件
• https://api.flutter.dev/flutter/material/scaffold/of.html	lib/arm64-v8a/libapp.so

• file:isoff-live:2011 • 127.0.0.1 • http://127.0.0.1:%d/proxy/%d/%d/loop.m3u8?play_id=%d&clip_id=%d&force_online=0 • http://127.0.0.1:%d/proxy/%d/%d/vod.m3u8?play_id=%d&clip_id=%d&force_online=0 • http://127.0.0.1:%d/proxy/%d/%d/live.m3u8?play_id=%d&clip_id=%d&force_online=0 • http://127.0.0.1:%d/proxy/%d/%d/vod.mp4?play_id=%d&clip_id=%d&force_online=0 • http://127.0.0.1:%d/proxy/%d/1/%s.flv?play_id=%d&clip_id=1&force_online=0 • http://127.0.0.1:%d/proxy/%d/%d/master.m3u8?play_id=%d&clip_id=%d&force_online=0 • http://127.0.0.1:%d/proxy/%d/%d/%s?play_id=%d&clip_id=%d&force_online=0 • file:isoff-on-demand:2011 • http://127.0.0.1:%d/proxy/%d/%d/%s_tp_dl_autotype?play_id=%d&clip_id=%d&force_online=0 • file:isoff-main:2011 • 1.2.0.4 • file:isoff-live:2012 • http://127.0.0.1:%d/proxy/%d/%d/%s?play_id=%d&clip_id=%d&force_online=0%s • http://127.0.0.1:%d/proxy/%d/%d/vod_%d.m3u8?play_id=%d&clip_id=%d&force_online=0	lib/arm64-v8a/libdownloadproxy.so
• http://drmprovisionurl • http://drmlicenseurl	lib/arm64-v8a/libtpcore-master.so

第三方SDK

SDK名称	开发者	描述信息
Flutter	Google	Flutter 是谷歌的移动 UI 框架，可以快速在 iOS 和 Android 上构建高质量的原生用户界面。
Fresco	Facebook	Fresco 是一个用于管理图像及其使用的内存的 Android 库。
GIFLIB	GIFLIB	The GIFLIB project maintains the giflib service library, which has been pulling images out of GIFs since 1989. It is deployed everywhere you can think of and some places you probably can't - graphics applications and web browsers on multiple operating systems, game consoles, smartphones, and likely your ATM too.
腾讯云短视频 SDK	Tencent	腾讯云点播推出了短视频一站式解决方案，覆盖了视频生成、上传、处理、分发和播放在内的各个环节，帮助用户以最快速度实现短视频应用的上线。
腾讯云实时音视频 SDK	Tencent	实时音视频（Tencent RTC）基于腾讯多年来在网络与音视频技术上的深度积累，以多人音视频通话和低延时互动直播两大场景化方案，通过腾讯云服务向开发者开放，致力于帮助开发者快速搭建低成本、低延时、高品质的音视频互动解决方案。
WebP Codec	WebM project	WebP codec is a library to encode and decode images in WebP format. This package contains the library that can be used in other programs to add WebP support, as well as the command line tools 'cwebp' and 'dwebp' to compress and decompress images respectively.

密钥凭证

可能的密钥
凭证信息=> "com.appinstall.APP_KEY" : "ucex8xfm"
凭证信息=> "com.abbitairm.nodaeogy.monised.Hrzbuvta.apikey" : "OHGZh7rTnel3UBKZ4PlJ6sjweoq7KWoGijn"
凭证信息=> "5wkQfuYJKey" : "ai6g0xuXkrvSPdzOznLc9RUl40Ai9"
凭证信息=> "RQCkMucKey" : "Nd3wYUceAy7a74dzAsRHf3GMLjpz"
凭证信息=> "LM0ZKLVY2emKey" : "3Km127pB4s0VFv1I1yl6zjgcAe16C4lu"
凭证信息=> "4JKQjw4J2Key" : "dMZHQnkpeP5SfC6H7YvnYd4fvhm5nKPl9ji"
凭证信息=> "org.hallible.sporis.misted.Qiqtelkmltk.apikey" : "OsmIIyZD4vOVGjuVTtCONtYXy01cNwJwQ44"
凭证信息=> "W3aVAkdJKey" : "CoDBp5fIVOMZAu4B9OUcHO6B3nSVcSkejs"
凭证信息=> "com.segate.agovests.Owyobabtjxbac.apikey" : "CxzFZlsu2b8y4aXQPp7WMOq0gZ3CGCxwQX1"

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。