



## ANDROID 静态分析报告



◆ 抖音会议

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: 2025-04-02 09:24:44

## i应用概览

|           |   |
|-----------|---|
| 文件名称:     | uzr0kxcl7q.scmudvies1.tau1podhsb.apk                              |
| 文件大小:     | 22.98MB   |
| 应用名称:     | 抖音会议  |
| 软件包名:     | uzr0kxcl7q.scmudvies1.tau1podhsb                                  |
| 主活动:      | uzr0kxcl7q.scmudvies1.tau1podhsb.MainActivity                     |
| 版本号:      |   |
| 最小SDK:    | 21  |
| 目标SDK:    | 33  |
| 加固信息:     | 未加壳   |
| 开发框架:     | Flutter   |
| 应用程序安全分数: | 64/100 (低风险)  |
| 杀软检测:     | 恶意软件  |
| MD5:      | 5735ce94e3c462b22bec23e050cc6643                                  |
| SHA1:     | cbbf4000f1e214704d0abbb2bfa0611363eba1bc                          |
| SHA256:   | f87ff487bfa06170a261ba36d325d2a8da45629f12a3ca99897c6578c8c23e54a |

## ⚠️ 恶意软件家族信息

|       |   |
|-------|---|
| 恶意家族  | CustServRemoteThief   |
| 描述信息  | CustServRemoteThief (中文名: 六耳吞金, 引自: 《西游记》六耳猕猴伪装孙悟空。) 是一款由南明离火平台命名的恶意软件, 基于 RustDesk 远程控制软件二次开发而成, 采用 Flutter 开发框架构建, 最早可追溯至 2023 年。其主要通过伪造应用程序以及冒充客服等渠道进行传播, 使攻击者得以侵入受害者设备, 获取远程访问权限, 进而窃取受害者的银行资金等敏感信息。目前, 已发现该家族恶意 APP 名称包括但不限于: 银联会议、银保会议、银监会议、通讯会议、专用会议、抖音会议、中银会议、认证会议、在线会议、银办通、云会议、U 会议。 |
| C2服务器 | 运行APP后, 在手机的 "/data/data/{package_name}/app_flutter/" 目录下可以查看到 RustDesk 服务器的配置信息。   |
| 凭证数据  | <a href="#">升级会员: 解锁高级权限</a>  |
| 关联情报  | <a href="#">升级会员: 解锁高级权限</a>  |

## 🔍 分析结果严重性

|             |              |             |             |             |
|-------------|--------------|-------------|-------------|-------------|
| <b>🚨 高危</b> | <b>⚠️ 中危</b> | <b>i 信息</b> | <b>✓ 安全</b> | <b>🔍 关注</b> |
| 0           | 4            | 0           | 1           | 0           |

## 四大组件信息

|                                       |
|---------------------------------------|
| Activity组件: 4个, 其中export的有: 0个        |
| Service组件: 4个, 其中export的有: 0个         |
| Receiver组件: 2个, 其中export的有: <b>2个</b> |
| Provider组件: 2个, 其中export的有: 0个        |

## 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=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown

签名算法: rsassa\_pkcs1v15

有效期自: 2025-02-28 13:56:50+00:00

有效期至: 2125-02-04 13:56:50+00:00

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

序列号: 0xcf0ac1874c432327

哈希算法: sha384

证书MD5: 7f1e09235fdf463c916e42775064624b

证书SHA1: 3b83757867554d673de2bca6527a3cca4cad0754

证书SHA256: ae420344a7198b1c22643cb9bfc6d0a7d799a03c8a6a4778d200768b0a1ba865

证书SHA512:

91716268c945012e9c67a0cddbda573c892f89a11817c6b7f8eac5cc558fe5f9772f27cde106690799cc7cd1039153413de1e7bb5944cef20cbf45fcee777862

公钥算法: rsa

密钥长度: 2048

指纹: 57145d0ecbed676694c8ce35ed17a2026b14d22e436ea85b89c154ffcdeb655b1

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.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.POST_NOTIFICATIONS                   | 危险   | 发送通知的运行时代权限   | 允许应用发布通知, Android 13 引入的新权限。   |
| 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。 |
| 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.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.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.RECORD_AUDIO   | 危险 | 获取录音权限         | 允许应用程序获取录音权限。   |
| 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.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。  |
| uzr0kxcl7q.scmudvies1.tau1podhsb.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | 未知 | 未知权限           | 来自 android 引用的未知权限。   |
| 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。                                       |

## 可浏览的Activity组件

| ACTIVITY                                      | INTENT                |
|---|-----------------------|
| uzr0kxcl7q.scmudvies1.tau1podhsb.MainActivity | Schemes: zeonfqku://, |

## 网络通信安全

| 序号 | 范围 | 严重级别 | 描述 |
|----|----|------|----|
|----|----|------|----|

## 证书安全分析

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分析

高危: 0 | 警告: 4 | 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<br>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 | Broadcast Receiver (uzr0kxcl7q.scmudvies1.tau1podhsb.BootReceiver) 未被保护。<br>[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。  |
| 3 | Broadcast Receiver (androidx.profileinstaller.ProfileInstallerReceiver) 受权限保护, 但是应该检查权限的保护级别。<br>Permission: android.permission.DUMP<br>[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。 |
| 4 | 高优先级的Intent (1000) - {1} 个命中<br>[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。  |

## </> 安全漏洞检测

| 序号 | 问题 | 等级 | 参考标准 | 文件位置 |
|----|----|----|------|------|
|----|----|----|------|------|

## 动态库分析

| 序号 | 动态库 | PIE<br>(堆栈禁止执行) | STACK CANARY(栈保护) | RELRO | RPATH (指定SO搜索路径) | FORTIFY(常用函数加强检查) | SYMBOL STRIPPED (裁剪符号表) |
|----|-----|-----------------|-------------------|-------|------------------|-------------------|-------------------------|
|    |     |                 |                   |       |                  |                   |                         |

|   |                          |   |  |  |  |                     |   |   |                     |
|---|--------------------------|---|--|--|--|---------------------|---|---|---------------------|
| 1 | arm64-v8a/libapp.so      | <p>True<br/><b>info</b></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)<br/><b>info</b></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<br/><b>info</b></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>Not Applicable<br/><b>info</b></p> <p>RELRO 检查不适用于 Flutter/Dart 二进制文件</p>   | None<br><b>info</b> | <p>None<br/><b>info</b></p> <p>二进制文件没有设置 RUNPATH</p>  | <p>False<br/><b>info</b></p> <p>二进制文件没有任何加固函数。加固函数提供了针对 libc 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>           | True<br><b>info</b> |
| 2 | arm64-v8a/libzeonfqku.so | <p>True<br/><b>info</b></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)<br/><b>info</b></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<br/><b>info</b></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>Full RELRO<br/><b>info</b></p> <p>此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在受攻击的 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。</p> | None<br><b>info</b> | <p>\$ORIGIN:../..../..../..../<br/>../root/.rustup/toolchains/1.78-x86_64-unknown-linux-gnu/lib/rustlib/aarch64-linux-android/lib<br/><b>high</b></p> <p>二进制文件设置了 RUNPATH。在某些情况下, 攻击者可以滥用这个特性或者修改环境变量来运行任意的库, 从而实现代码执行和权限提升。库应该设置 RUNPATH 的唯一时间是当它链接到同一个包中的私有库时。移除编译选项 --enable-new-dtags, -rpath 来移除 RUNPATH</p> | <p>True<br/><b>info</b></p> <p>二进制文件有以下加固函数: ['_memcpy_chk', '_memset_chk', '_vsprintf_chk', '_memcpy_chk', '_strchr_chk', '_strcpy_chk', '_strlen_chk', '_read_chk']</p> | True<br><b>info</b> |

行为分析

| 编号    | 行为             | 标签 | 文件           |
|-------|----------------|----|--------------|
| 00013 | 读取文件并将其放入流中    | 文件 | 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 |
| 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 |

## 敏感权限分析

| 类型       | 匹配   | 权限  |
|----------|------|---|
| 恶意软件常用权限 | 5/30 | android.permission.RECORD_AUDIO<br>android.permission.WAKE_LOCK<br>android.permission.RECEIVE_BOOT_COMPLETED<br>android.permission.SYSTEM_ALERT_WINDOW<br>android.permission.CAMERA   |
| 其它常用权限   | 6/46 | android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS<br>android.permission.READ_EXTERNAL_STORAGE<br>android.permission.WRITE_EXTERNAL_STORAGE<br>android.permission.INTERNET<br>android.permission.ACCESS_NETWORK_STATE<br>android.permission.FOREGROUND_SERVICE |

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   |
|--------------------------------|----|------|--|
| zeonfqku.com                   | 安全 | 否    | No Geolocation information available.  |
| journeyapps.com                | 安全 | 否    | IP地址: 13.226.225.21<br>国家: 美国<br>地区: 加利福尼亚<br>城市: 洛杉矶<br>纬度: 34.052570<br>经度: -118.243904<br>查看: <a href="#">Google 地图</a> |
| admin.zeonfqku.comzeonfqku.com | 安全 | 否    | No Geolocation information available.  |
| docs.rs                        | 安全 | 否    | IP地址: 13.226.225.21<br>国家: 美国<br>地区: 加利福尼亚<br>城市: 洛杉矶<br>纬度: 34.052570<br>经度: -118.243904<br>查看: <a href="#">Google 地图</a> |

## URL链接分析

| URL信息   | 源码文件                         |
|---|------------------------------|
| <ul style="list-style-type: none"> <li>https://github.com/journeyapps/zxing-android-embedded</li> <li>https://journeyapps.com/</li> </ul>   | 自研引擎-S                       |
| <ul style="list-style-type: none"> <li>https://zeonfqku.com/docs/en/manual/linux/#x11-requiredinput-2fare-input-passworddo</li> <li>http://errorinvalid</li> <li>https://github.com/zeonfqku/zeonfqku/wiki/headless-linux-supportconfigenc_idkey_confirmedkey_s_confirmedstruct</li> <li>https://zeonfqku.com/docs/en/zeonfqku</li> <li>https://docs.rs/flexi_logger/latest/flexi_logger/error_info/index.html#writeflushformatlogfilepoison_symlinkwriterspecerror</li> <li>https://admin.zeonfqku.comzeonfqku.com/api/audit/content-typewrong</li> <li>https://docs.rs/getrandom#nodejs-es-module-support/dev/urandom</li> <li>https://zeonfqku.com/docs/en/manual/linux/#x11-requiredzeonfqku</li> </ul> | lib/arm64-v8a/libzeonfqku.so |

## 第三方SDK

| SDK名称   | 开发者                     | 描述信息   |
|---------|-------------------------|--|
| Flutter | <a href="#">Google</a>  | 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。 |
| C++ 共享库 | <a href="#">Android</a> | 在 Android 应用中运行原生代码。                                     |

## 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