南明离火
移动应用检测平台

ANDROID 静态分析报告

Chanty • v0.519

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: 2025-07-09 17:30:42

应用概览

文件名称:	Chanty v0.51.9.apk
文件大小:	16.68MB
应用名称:	Chanty
软件包名:	com.chanty.chat
主活动:	com.chanty.chat.MainActivity
版本号:	0.51.9
最小SDK:	26
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	61/100 (低风险)
跟踪器检测:	1/432
杀软检测:	经检测，该文件安全
MD5:	53bc4ec9a7ac4492ebf636b7dbe87e04
SHA1:	18365c6beb9693a46546ee56b81f3e37bde264
SHA256:	e16a4cf39c4b99cb2fb94c3042d45d6be88df1d859f3e6309a1174a2dc42b6

本报告由南明离火移动安全分析平台生成

分析结果严重性分布

高危	中危	信息	安全	关注
0	10	3	2	0

四大组件导出状态统计

Activity组件：4个，其中export的有： 0个
Service组件：5个，其中export的有： 0个
Receiver组件：3个，其中export的有： 2个
Provider组件：5个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=US, ST=New York, L=New York, O=Chanty, Inc., OU=Development, CN=Dmytro Okunyev
签名算法: rsassa_pkcs1v15
有效期自: 2017-09-07 06:21:44+00:00
有效期至: 2045-01-23 06:21:44+00:00
发行人: C=US, ST=New York, L=New York, O=Chanty, Inc., OU=Development, CN=Dmytro Okunyev
序列号: 0x2a083368
哈希算法: sha256
证书MD5: a95830a5f99fc9fa6d7a6e7a6f87e178
证书SHA1: 7119d4951bc60b7f9336a1d82a4dada93a536a63
证书SHA256: 95ef04d90dfe3a5e3e28107ef85871161933fd4694761d8b34d114c6b0c35567
证书SHA512:
649126a4a5dabdd589fcb9db2a8bb6fffe75f4c6ab6911da86a6b10938c521c662d903c72084cbb1d854d09173c45857bbda3608cffeb1900c2ebc54e06d783

公钥算法: rsa
密钥长度: 2048
指纹: 5171ba3b5315a3f3143d86cd547af7692eda71ab7d6b45291e0a7a6c599c70c6
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.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.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。
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.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.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_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。

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

android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
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.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.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，在手机屏幕关闭后台进程仍然运行。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知
com.chanty.chat.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.sec.android.provider.badge.permission.READ	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	普通	在应用程序上显示通知计数	在apex的应用程序启动图标上显示通知计数或徽章。
com.majeur.launcher.permission.UPDATE_BADGE	普通	在应用程序上显示通知计数	在solid的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
android.permission.READ_APP_BADGE	普通	显示应用程序通知	允许应用程序显示应用程序图标徽章。
com.oppo.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。

本报告由南明离火移动安全分析平台生成

com.oppo.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	未知权限	来自 android 引用的未知权限。
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.chanty.chat.MainActivity	Schemes: @7F0E0037://,

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

序号	问题	严重程度	描述信息
1	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。
2	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。

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

3	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 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: **5** | 信息: **2** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
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	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	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
5	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
6	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
7	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限

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

8	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

应用行为分析

编号	行为	标签	文件
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
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
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	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
00012	读取数据并放入缓冲流	文件	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
00028	从assets目录中读取文件	文件	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
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
00153	通过 HTTP 发送二进制数据	http	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
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
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
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

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

00091	从广播中检索数据	信息收集	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

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	9/30	android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.WAKE_LOCK
其它常用权限	6/46	android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.BLUETOOTH com.google.android.c2dm.permission.RECEIVE

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
chanty-notifications.firebaseio.com	安全	否	**IP**地址: 35.190.39.113 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

URL 链接安全分析

URL信息	源码文件

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

- https://github.com/capawesome-team/capacitor-plugins/blob/main/packages/badge/ios/Plugin/Badge.swift
- https://github.com/salesforce/lwc/blob/master/packages
- https://www.linkedin.com/company/chanty
- https://github.com/zloirock/core-js/issues/86
- https://stackoverflow.com/questions/29249132/wkwebview-complex-communication-between-javascript-native-code/49474323
- https://www.timeanddate.com/time/time-zones-interesting.html
- http://polymer.github.io/PATENTS.txt
- http://polymer.github.io/CONTRIBUTORS.txt
- https://www.chanty.com
- https://angular.io/docs/ts/latest/guide/browser-support.html
- https://github.com/zloirock/core-js
- https://openjsf.org
- http://ionicframework.com
- https://github.com/WICG/webcomponents/issues/847
- https://twitter.com/chanty
- https://github.com/cartant/rxjs-etc
- https://capacitorjs.com
- https://angular.io
- http://drifty.com
- https://tc39.es/ecma262
- http://rock.mit-license.org
- http://creativecommons.org/publicdomain/zero/1.0
- https://www.chanty.com/blog
- https://kossnocorp.mit-license.org
- https://www.chanty.com/help
- https://ionicframework.com/docs/developing/hardware-back-button
- https://www.chanty.com/help/article/manage-tasks
- https://developer.chrome.com/blog/viewport-resize-behavior
- https://github.com/webcomponents/webcomponentsjs/blob/24fecd7e0e/src/ShadowCSS/ShadowCSS.js
- https://angular.io/license
- https://www.facebook.com/groups/chanty.early.adopters
- https://html.spec.whatwg.org/multipage/custom-elements.html
- https://github.com/es-shims/es5-shim
- https://github.com/jonathantneal/closest
- https://stackoverflow.com/a/57382543
- https://ionic.io
- https://github.com/garycourt/uri-js/commit/a1acf730b4bba3f1097c9f52e7d9d3aba8cdcaae
- https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en&gl=US
- https://mrale.ph/blog/2013/01/11/whats-up-with-monomorphism.html
- https://github.com/ionic-team/stencil/issues/3180
- https://apps.apple.com/us/app/google-authenticator/id388497605
- http://polymer.github.io/LICENSE.txt
- https://chanty.com
- https://github.com/ionic-team/ionic-framework/issues/7527
- https://caniuse.com/?search=scrollend
- http://polymer.github.io/AUTHORS.txt
- https://www.facebook.com/TeamCollaboration
- https://github.com/garycourt/uri-js/graphs/contributors
- https://angular.dev/license

自研引擎-A

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

• http://10.0.2.2:8969/stream	io/sentry/SpotlightIntegration.java
• https://chanty-notifications.firebaseio.com	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://chanty-notifications.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/967076036048/namespaces/firebase:fetch?key=AIzaSyCKk_xjnD-gso7ORDA8lMtZKvAHQVjvKiA）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
Sentry	Sentry	Sentry 是一个实时事件日志记录和聚合平台，它专门用于监视错误和提取执行适当的事后操作所需的所有信息。
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 ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
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
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

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

敏感凭证泄露检测

可能的密钥
"firebase_database_url" : "https://chanty-notifications.firebaseio.com"
"google_api_key" : "AIzaSyCKk_xjnD-gso7ORDA8lMtZRyAHQVjvKiA"
"google_app_id" : "1:967076036048:android:2ed3c4c381916a64"
"google_crash_reporting_api_key" : "AIzaSyCKk_xjnD-gso7ORDA8lMtZRyAHQVjvKiA"

Google Play 应用市场信息

标题: Chanty - Team Collaboration

评分: 3.5 **安装:** 10,000+ **价格:** 0 **Android版本支持:** **分类:** 办公 **Play Store URL:** com.chanty.chat

开发者信息: Chanty, Inc., Chanty,+Inc., None, https://www.chanty.com/, info@chanty.com,

发布日期: 2017年9月7日 **隐私政策:** Privacy link

关于此应用:

Canty 帮助团队提高生产力和业务沟通。 使用 Chanty，您可以从一个地方与您的团队进行有效的协作和沟通。 不再需要在应用程序之间进行更改来完成工作。 Chanty 是一个易于使用的团队聊天和协作应用程序，它提供： - 团队成员之间的即时消息：一对一消息、公开和私人对话 - 无限制的可搜索消息历史记录，永远安全无限制的消息传递 - 音视频通话：通过Chanty音视频会议与整个团队（群组通话）或任何团队成员（一对一通话）沟通 - 使用看板进行任务管理：一种灵活而简单的方法来管理您的任务、设置截止日期和任务优先级 - Teambook 中心：一个可以组织您的任务、对话、固定消息、链接和内容的地方 - 语音信息：让您可以即时向您的队友发送语音信息 - 集成：Chanty 与您喜欢的所有第三方应用程序集成 - 固定消息：让您将任何消息固定在 Chanty 上，稍后再回复 - 讨论主题：让您保持主题，无需无休止的历史滚动 - 深色模式：根据您的喜好选择浅色/深色主题 - 文件和屏幕共享：您现在可以举行视频会议并共享您的屏幕以进行演示 - 其他团队协作功能：用户和团队@提及、gif 和表情符号、在线状态、对话操作等等 - 在所有设备上使用：Chanty 可在 Windows、Linux、Mac、Debian、Fedora、iOS 和 Android 上使用 - 24/7 客户支持 Chanty 永远免费。如果您希望获得更多增强的功能和增强的用户控制，您可以选择升级到我们的商业计划。 要了解有关 Chanty 的更多信息，请访问我们的 https://www.chanty.com/

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

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。

© 2025 南明离火 - 移动安全分析平台自动生成