苏宁金融

标题

北京梆梆安全科技有限公司

测评时间：2020-12-11

1 说明

1.1 保护级别的定义

本报告中将 Android 系统权限分为几个保护级别，其中最重要的两个保护级别是“正常”和“危险”。保护级别的定义基于 Google 官方文档。

- 特殊权限

涵盖应用需要访问其沙盒外部数据或资源，但对用户隐私或其他应用操作风险很小的区域。例如，设置时区的权限就是正常权限。如果应用声明其需要正常权限，系统会自动向应用授予该权限。

- 危险权限

涵盖应用需要涉及用户隐私信息的数据或资源，或者可能对用户存储的数据或其他应用的操作产生影响的区域。例如，能够读取用户的联系人属于危险权限。如果应用声明其需要危险权限，则用户必须明确向应用授予该权限。

1.2 可收集个人信息权限

本报告中将“可收集个人信息权限”与“安卓特殊敏感权限”简称为“敏感权限”，相关权限的定义基于全国信息安全标准化技术委员会发布的《网络安全标准实践指南—移动互联网应用程序（App）系统权限申请使用指南》附录 A 与附录 B。

2 检测结果

2.1 App 基本信息

软件名称	苏宁金融
类型	其他
包名	com.suning.mobile.epa
软件大小	68.40MB
软件版本	6.7.10
安装包文件名	苏宁金融_V2.apk
安装包 MD5	080b3221e9a769665d76e23388a33cdc
安装包 SHA-1	6397c7c5c3782e5dd6ee806d165f61f6ab0959e8
安装包 SHA-256	ccc537315b9ae4d4f88cc0fa84185a1cce24da4ce9f1b22f6bcdcaf8a9cdec9f
签名信息	CN=Suning
targetSdkVersion	26
minSdkVersion	14
加固	未加固
分析时间	2020-12-11 10:07:27

2.2 声明权限情况

该 App 在 AndroidManifest.xml 中声明权限共 84 个，其中涉及 8 个可收集个人信息权限，占比为 9.52%，具体情况如下：

序号	声明权限	权限含义	类型	保护级别	敏感权限
1	INTERNET	访问网络	官方	正常	否
2	VIBRATE	控制振动器	官方	正常	否
3	SYSTEM_ALERT_WINDOW	显示系统级警报	官方	特殊	否
4	CAMERA	访问相机	官方	危险	是
5	FLASHLIGHT	控制闪光灯	官方	正常	否
6	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是
7	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是
8	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是

9	WRITE_EXTERNAL_STORAGE	修改/删除 SD 卡中的内容	官方	危险	是
10	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是
11	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否
12	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否
13	WAKE_LOCK	防止手机休眠	官方	正常	否
14	READ_CONTACTS	读取联系人数据	官方	危险	是
15	EXPAND_STATUS_BAR	展开/收拢状态栏	官方	正常	否
16	USE_FINGERPRINT	允许使用指纹	官方	正常	否
17	RECORD_AUDIO	录音	官方	危险	是
18	READ_SETTINGS	读取全局系统设置	官方	N/A	否
19	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否
20	REQUEST_INSTALL_PACKAGES	允许程序安装文件	官方	特殊	否
21	com.android.launcher.INSTALL_SHORTCUT	自定义权限	自定义	N/A	否
22	com.android.launcher.UNINSTALL_SHORTCUT	自定义权限	自定义	N/A	否
23	com.android.launcher.READ_SETTINGS	自定义权限	自定义	N/A	否
24	com.android.launcher.WRITE_SETTINGS	自定义权限	自定义	N/A	否
25	com.android.launcher2.READ_SETTINGS	自定义权限	自定义	N/A	否

26	com.android.launcher2.WRITE_SETTINGS	自定义权限	自定义	N/A	否
27	com.android.launcher3.READ_SETTINGS	自定义权限	自定义	N/A	否
28	com.android.launcher3.WRITE_SETTINGS	自定义权限	自定义	N/A	否
29	org.adw.launcher.READ_SETTINGS	自定义权限	自定义	N/A	否
30	org.adw.launcher.WRITE_SETTINGS	自定义权限	自定义	N/A	否
31	com.htc.launcher.READ_SETTINGS	自定义权限	自定义	N/A	否
32	com.htc.launcher.WRITE_SETTINGS	自定义权限	自定义	N/A	否
33	com.qihoo360.launcher.READ_SETTINGS	自定义权限	自定义	N/A	否
34	com.qihoo360.launcher.WRITE_SETTINGS	自定义权限	自定义	N/A	否
35	com.lge.launcher.READ_SETTINGS	自定义权限	自定义	N/A	否
36	com.lge.launcher.WRITE_SETTINGS	自定义权限	自定义	N/A	否
37	net.qihoo.launcher.	自定义权限	自定义	N/A	否

	READ_SETTINGS				
38	net.qihoo.launcher.WRITE_SETTINGS	自定义权限	自定义	N/A	否
39	org.adwfreak.launcher.READ_SETTINGS	自定义权限	自定义	N/A	否
40	org.adwfreak.launcher.WRITE_SETTINGS	自定义权限	自定义	N/A	否
41	org.adw.launcher_donut.READ_SETTINGS	自定义权限	自定义	N/A	否
42	org.adw.launcher_donut.WRITE_SETTINGS	自定义权限	自定义	N/A	否
43	com.huawei.launcher3.READ_SETTINGS	自定义权限	自定义	N/A	否
44	com.huawei.launcher3.WRITE_SETTINGS	自定义权限	自定义	N/A	否
45	com.fede.launcher.READ_SETTINGS	自定义权限	自定义	N/A	否
46	com.fede.launcher.WRITE_SETTINGS	自定义权限	自定义	N/A	否
47	com.sec.android.twlauncher.settings.READ_SETTINGS	自定义权限	自定义	N/A	否
48	com.sec.android.twlauncher.set	自定义权限	自定义	N/A	否

	tings.WRITE_SETTINGS				
49	com.anddoes.launcher.READ_SETTINGS	自定义权限	自定义	N/A	否
50	com.anddoes.launcher.WRITE_SETTINGS	自定义权限	自定义	N/A	否
51	com.tencent.qqlauncher.READ_SETTINGS	自定义权限	自定义	N/A	否
52	com.tencent.qqlauncher.WRITE_SETTINGS	自定义权限	自定义	N/A	否
53	com.huawei.launcher2.READ_SETTINGS	自定义权限	自定义	N/A	否
54	com.huawei.launcher2.WRITE_SETTINGS	自定义权限	自定义	N/A	否
55	com.android.mylauncher.READ_SETTINGS	自定义权限	自定义	N/A	否
56	com.android.mylauncher.WRITE_SETTINGS	自定义权限	自定义	N/A	否
57	com.ebproductions.android.permission.READ_SETTINGS	自定义权限	自定义	N/A	否
58	com.ebproductions.android.permission.WRITE_SETTINGS	自定义权限	自定义	N/A	否
59	com.oppo.launcher.READ_SETTIN	自定义权限	自定义	N/A	否

	GS				
60	com.oppo.launcher.WRITE_SETTINGS	自定义权限	自定义	N/A	否
61	com.huawei.android.permission.READ_SETTINGS	自定义权限	自定义	N/A	否
62	com.huawei.android.permission.WRITE_SETTINGS	自定义权限	自定义	N/A	否
63	telecom.mdesk.permission.READ_SETTINGS	自定义权限	自定义	N/A	否
64	telecom.mdesk.permission.WRITE_SETTINGS	自定义权限	自定义	N/A	否
65	dianxin.permission.ACCESS_LAUNCHER_DATA	自定义权限	自定义	N/A	否
66	SYSTEM_OVERLAY_WINDOW	自定义权限	自定义	N/A	否
67	ACCESS_LOCATION_EXTRA_COMMANDS	访问额外的位置信息提供程序命令	官方	正常	否
68	com.suning.mobile.permission.MIPUSH_RECEIVE	自定义权限	自定义	N/A	否
69	com.meizu.flyme.permission.RECEIVE	自定义权限	自定义	N/A	否
70	com.suning.mobile.push.permission.MESSAGE	自定义权限	自定义	N/A	否
71	com.meizu.c2	自定义权限	自定义	N/A	否

	dm. RECEIVE				
72	com.suning.mobile. permission.C2D_MESSAGE	自定义权限	自定义	N/A	否
73	BLUETOOTH	创建蓝牙连接	官方	正常	否
74	BLUETOOTH_ADMIN	蓝牙管理	官方	正常	否
75	CHANGE_NETWORK_STATE	更改网络连接性	官方	正常	否
76	CHANGE_WIFI_STATE	更改 WLAN 状态	官方	正常	否
77	com.asus.msa.ACCESS	自定义权限	自定义	N/A	否
78	cn.org.ifaa.USE_IFAA_MANAGER	自定义权限	自定义	N/A	否
79	USE_FACERECOGNITION	自定义权限	自定义	N/A	否
80	CHANGE_WIFI_MULTICAST_STATE	允许接收 WLAN 多播	官方	正常	否
81	GET_TASKS	检索当前运行的应用程序	官方	特殊	否
82	REORDER_TASKS	对正在运行的应用程序重新排序	官方	正常	否
83	FLAG_ACTIVITY_NEW_TASK	自定义权限	自定义	N/A	否
84	BROADCAST_STICKY	发送置顶广播	官方	正常	否

2.3 总体情况

成分分析	集成 SDK 共 65 个，其中涉及 13 个类别，来自 37 个开发者
	在 AndroidManifest.xml 中声明权限共 84 个
漏洞分析	检测出 7 项漏洞
行为分析	对外通信共 301 次，其中涉及 15 个域名
	该 App 在检测期间发生异常通信行为共 301 次，其中涉及 13 个 IP 地址。
	读取设备信息共 70 次，其中涉及 8 个 SDK
	使用权限共 314 次，其中涉及可收集个人信息权限 106 次
	该 App 的 targetSDKVersion 值为 26，不存在一揽子授权行为，推荐设置

	targetSDKVersion 值不低于 28。

3 检测结果

3.1 成分分析

3.1.1 SDK 集成情况

该 APP 集成 SDK 共 65 个，其中涉及到 13 个类别, 来自 37 个开发者，具体情况如下:

3.1.1.1 网易云信 IM 聊天室 SDK

序号	1
SDK 名称	网易云信 IM 聊天室 SDK
开发者	网易
类别	社交
描述	网易云通信 IM 聊天室采用多层架构设计，可以实现真正意义上的大型聊天室，参与人数无上限，又可满足消息到达的实时性要求
来源	https://yunxin.163.com/education-demo
包名	com.netease.nimlib.sdk.chatroom

3.1.1.2 Volley

序号	2
SDK 名称	Volley
开发者	Google
类别	工具
描述	Volley 是一个可让 Android 应用更轻松、（最重要的是）更快捷地联网的 HTTP 库。
来源	https://developer.android.com/training/volley
包名	com.android.volley

3.1.1.3 魅族 Flyme 推送 SDK

序号	3
SDK 名称	魅族 Flyme 推送 SDK
开发者	魅族
类别	消息推送
描述	魅族推送(Push)是魅族公司向开发者提供的消息推送服务，通过在云端与客户端之间建立一 条稳定，可靠的长连接，为开发者提供向客户端应用实时推送消息的服务，通过推

	送消息， 魅族推送服务能有效地帮助开发者拉动用户活跃度，改善产品体验。
来源	http://open-wiki.flyme.cn/doc-wiki/index#id?130
包名	com.meizu.cloud.pushsdk

3.1.1.4 Okio

序号	4
SDK 名称	Okio
开发者	Square
类别	工具
描述	Okio is a library that complements java.io and java.nio to make it much easier to access, store, and process your data. It started as a component of OkHttp, the capable HTTP client included in Android. It's well-exercised and ready to solve new problems.
来源	https://github.com/square/okio
包名	okio

3.1.1.5 网易云信互动白板 SDK

序号	5
SDK 名称	网易云信互动白板 SDK
开发者	网易
类别	工具
描述	网易云信提供互动白板（可靠 TCP 传输通道）来满足白板的多人互动功能。 互动白板：互动白板是基于多人实时会话功能实现的用有白板多人交互能力的应用场景。支持多人参与白板操作，进行实时互动。实时记录会 话操作的全面内容，方便回放查看。支持把 PPT、PPTX、PDF 等文档格式转码为 png 及 jpg 格式，翻页、标注实时进行，方便共享展示。
来源	http://dev.yunxin.163.com/docs/product/%E4%BA%92%E5%8A%A8%E7%99%BD%E6%9D%BF/%E4%BA%A7%E5%93%81%E4%BB%8B%E7%BB%8D/%E7%AE%80%E4%BB%8B
包名	com.netease.nimlib.rts

3.1.1.6 Facebok ImagePipeline

序号	6
SDK 名称	Facebok ImagePipeline
开发者	Facebook
类别	工具
描述	The underlying image loading mechanism of the Fresco library
来源	https://mvnrepository.com/artifact/com.facebook.fresco/imagepipeline

包名	com.facebook.imagepipeline

3.1.1.7 hongyangAndroid okhttputils

序号	7
SDK 名称	hongyangAndroid okhttputils
开发者	hongyangAndroid
类别	工具
描述	对 okhttp 的封装类
来源	https://github.com/hongyangAndroid/okhttputils
包名	e.o.a.a

3.1.1.8 小米开放平台消息推送 SDK

序号	8
SDK 名称	小米开放平台消息推送 SDK
开发者	小米
类别	消息推送
描述	小米消息推送服务在 MIUI 上为系统级通道，并且全 平台通用，可以为开发者提供稳定、可靠、高效的 推送服务
来源	https://dev.mi.com/console/appservice/push.html
包名	com.xiaomi.mipush com.xiaomi.mipush.sdk com.xiaomi.push

3.1.1.9 FastJson

序号	9
SDK 名称	FastJson
开发者	阿里巴巴
类别	工具
描述	Fastjson is a JSON processor (JSON parser + JSON generator) written in Java
来源	https://github.com/alibaba/fastjson
包名	com.alibaba.fastjson

3.1.1.10 岳鹰全景监控 SDK

序号	10
SDK 名称	岳鹰全景监控 SDK
开发者	支付宝-杭州

类别	APM
描述	岳鹰全景监控，是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。岳鹰提供服务包括：WEB 前端监控、APP 崩溃监控、小程序监控、IoT 设备稳定性监控等。岳鹰全景监控，为开发者及企业提供一套完整的移动应用线上质量监控解决方案，支持智能分析、智能预警，大幅提升了问题发现和定位的效率，让用户体验提升更简单。
来源	https://www.yuque.com/efs-yueying/yueying/yueying-intro
包名	com.uc.crashsdk

3.1.1.11 Apache Commons Codec

序号	11
SDK 名称	Apache Commons Codec
开发者	Apache.org
类别	工具
描述	The Apache Commons Codec package contains simple encoder and decoders for various formats such as Base64 and Hexadecimal. In addition to these widely used encoders and decoders, the codec package also maintains a collection of phonetic encoding utilities
来源	http://commons.apache.org/proper/commons-codec/
包名	org.apache.commons.codec

3.1.1.12 pinyin4j

序号	12
SDK 名称	pinyin4j
开发者	pinyin4j
类别	工具
描述	Pinyin4j 是一个流行的 Java 库，支持中文字符和拼音之间的转换。拼音输出格式可以定制。
来源	https://sourceforge.net/projects/pinyin4j/
包名	net.sourceforge.pinyin4j

3.1.1.13 Facebook AnimatedGif

序号	13
SDK 名称	Facebook AnimatedGif
开发者	Facebook
类别	图像
描述	The classes to support animated gif
来源	https://mvnrepository.com/artifact/com.facebook.fresco/animated-gif

包名	com.facebook.animated.gif

3.1.1.14 dagger

序号	14
SDK 名称	dagger
开发者	Google
类别	工具
描述	Dagger 是一个依赖注入框架,第一代由大名鼎鼎的 Square 公司共享出来，第二代则是由谷歌接手后推出的，现在由 Google 接手维护
来源	https://github.com/google/dagger
包名	dagger

3.1.1.15 Commons Lang

序号	15
SDK 名称	Commons Lang
开发者	Apache.org
类别	工具
描述	Commons Lang, a package of Java utility classes for the classes that are in java.lang's hierarchy, or are considered to be so standard as to justify existence in java.lang.
来源	http://commons.apache.org/lang/
包名	org.apache.commons.lang

3.1.1.16 Apache HttpClient

序号	16
SDK 名称	Apache HttpClient
开发者	Apache.org
类别	工具
描述	Designed for extension while providing robust support for the base HTTP protocol, HttpClient may be of interest to anyone building HTTP-aware client applications such as web browsers, web service clients, or systems that leverage or extend the HTTP protocol for distributed communication.
来源	https://mvnrepository.com/artifact/org.apache.httpcomponents/httpclient
包名	org.apache.http

3.1.1.17 Facebook AnimatedWebp

序号	17
SDK 名称	Facebook AnimatedWebp
开发者	Facebook
类别	图像
描述	The classes to support animated webp
来源	https://mvnrepository.com/artifact/com.facebook.fresco/animated-webp
包名	com.facebook.animated.webp

3.1.1.18 阿里设备标识 SDK

序号	18
SDK 名称	阿里设备标识 SDK
开发者	阿里云
类别	工具
描述	UTDID 是一个 APP 级别的设备标识 ID。通过设备标识组件，开发者可以实现简单快捷地获取设备 ID，以利于应用程序安全有效地找到特定设备。 UTDID 的设计目标是给每一台物理设备提供一个唯一且独立的设备 ID。在理想状况下，不同的 APP 在同一台设备上可以获取到相同的 UTDID；同一个 App 在同一个设备上卸载重装后，可以获取到相同的 UTDID；不同的设备的 UTDID 不一样。但是随着设备变化和隐私权限控制增强，UTDID 在同一台物理设备上可能会发生变化。因此 UTDID 不提供强一致性的保证，所以不要把 UTDID 应用到有强一致性保证需求的业务中。
来源	https://help.aliyun.com/document_detail/159082.html?spm=5176.11065259.1996646101.searchclickresult.5032d47fngebBU
包名	com.ut.device com.ta.utdid2

3.1.1.19 Facebook Fresco

序号	19
SDK 名称	Facebook Fresco
开发者	Facebook
类别	图像
描述	Fresco is a powerful system for displaying images in Android applications. Fresco takes care of image loading and display, so you don't have to. It will load images from the network, local storage, or local resources, and display a placeholder until the image has arrived. It has two levels of cache; one in memory and another in internal storage.
来源	https://github.com/facebook/fresco
包名	com.facebook.drawee.backends.pipeline

3.1.1.20 ImageViewZoom

序号	20
SDK 名称	ImageViewZoom
开发者	sephiroth74
类别	工具
描述	Android ImageView widget with zoom and pan capabilities
来源	https://github.com/sephiroth74/ImageViewZoom
包名	it.sephiroth.android.library.imagezoom

3.1.1.21 声网互动游戏 SDK

序号	21
SDK 名称	声网互动游戏 SDK
开发者	声网
类别	游戏
描述	Agora Interactive Gaming SDK，是 Agora 针对游戏开发者 （Unity，Cocos）提供的音视频通话软件开发包。
来源	https://docs.agora.io/cn/Interactive%20Gaming/downloads
包名	io.agora.live

3.1.1.22 华为 HMS 核心功能 SDK

序号	22
SDK 名称	华为 HMS 核心功能 SDK
开发者	华为
类别	工具
描述	HMS SDK 核心功能包
来源	https://developer.huawei.com/consumer/cn/doc/HMSCore-Library-V5/sdk-download-0000001050151556-V5
包名	com.huawei.hms.core

3.1.1.23 Greenrobot EventBus

序号	23
SDK 名称	Greenrobot EventBus
开发者	Markus Junginger
类别	工具
描述	Event bus for Android and Java that simplifies communication between Activities, Fragments, Threads, Services, etc. Less code, better quality.

来源	https://github.com/greenrobot/EventBus
包名	org.greenrobot.eventbus

3.1.1.24 PhotoView

序号	24
SDK 名称	PhotoView
开发者	chrisbanes
类别	工具
描述	PhotoView 是一款扩展自 Android ImageView ,支持通过单点/多点触摸来进行图片缩放，使用方法简单，是一个很好的图片框架
来源	https://github.com/chrisbanes/PhotoView
包名	com.suning.service.ebuy.view.photoview

3.1.1.25 Vlayout

序号	25
SDK 名称	Vlayout
开发者	阿里巴巴
类别	工具
描述	Project vlayout is a powerfull LayoutManager extension for RecyclerView, it provides a group of layouts for RecyclerView. Make it able to handle a complicate situation when grid, list and other layouts in the same recyclerview.
来源	https://github.com/alibaba/vlayout
包名	com.suning.mobile.components.vlayout

3.1.1.26 声网音视频 SDK

序号	26
SDK 名称	声网音视频 SDK
开发者	声网
类别	音视频
描述	Agora 实时音视频（Agora Video Call）基于 UDP 协议以及声网自研的音视频编解码技术，提供可靠的实时音视频服务。
来源	https://docs.agora.io/cn/Video/downloads
包名	io.agora.rtc

3.1.1.27 友盟消息推送 SDK

序号	27

SDK 名称	友盟消息推送 SDK
开发者	友盟
类别	消息推送
描述	消息推送组件，提供给用户准时的 Push 通知功能，聚合小米、华为、魅族、OPPO/ vivo 通道。集成了 UMID 以及淘宝 TUDID 组件。
来源	https://developer.umeng.com/sdk
包名	com.umeng.message

序号	使用权限	权限含义	保护级别	次数
1	READ_PHONE_STATE	读取手机状态和身份	危险	2

3.1.1.28 MPAndroidChart

序号	28
SDK 名称	MPAndroidChart
开发者	PhilJay
类别	工具
描述	A powerful & easy to use chart library for Android
来源	https://github.com/PhilJay/MPAndroidChart
包名	com.github.mikephil.charting

3.1.1.29 Picasso

序号	29
SDK 名称	Picasso
开发者	square
类别	工具
描述	A powerful image downloading and caching library for Android
来源	https://github.com/square/picasso
包名	com.squareup.picasso

3.1.1.30 网易云信 IM 基础功能 SDK

序号	30
SDK 名称	网易云信 IM 基础功能 SDK
开发者	网易
类别	工具
描述	网易云信即时通讯基础功能 SDK，包含账号登陆，基础消息，群聊等基础功能

来源	https://yunxin.163.com/im-sdk-demo
包名	com.netease.nimlib.sdk

3.1.1.31 腾讯移动分析 SDK

序号	31
SDK 名称	腾讯移动分析 SDK
开发者	腾讯
类别	统计
描述	提供实时数据统计分析服务，监控版本质量、渠道状况、用户画像属性及用户细分行为，通过数据可视化展现，协助产品、运营和市场决策。
来源	https://mta.qq.com/docs/
包名	com.tencent.stat

3.1.1.32 高德定位 SDK

序号	32
SDK 名称	高德定位 SDK
开发者	高德
类别	地图
描述	高德地图 Android SDK 是一套地图开发调用接口，开发者可以轻松地在自己的 Android 应用中加入地图相关的功能，包括：地图显示（含室内、室外地图）、与地图交互、在地图上绘制、兴趣点搜索、地理编码、离线地图等功能。
来源	https://lbs.amap.com/api/android-sdk/summary/
包名	com.amap.api.location

3.1.1.33 Lottie

序号	33
SDK 名称	Lottie
开发者	airbnb
类别	工具
描述	Lottie is a mobile library for Android and iOS that parses Adobe After Effects animations exported as json with Bodymovin and renders them natively on mobile!
来源	https://github.com/airbnb/lottie-android
包名	com.airbnb.lottie

3.1.1.34 DNSJava

序号	34
SDK 名称	DNSJava
开发者	xbill
类别	工具
描述	DNSJava IS An Implementation of DNS In Java
来源	https://mvnrepository.com/artifact/org.xbill/dns
包名	org.xbill.DNS

3.1.1.35 NineOldAndroids

序号	35
SDK 名称	NineOldAndroids
开发者	Jake Wharton
类别	工具
描述	Android library for using the Honeycomb (Android 3.0) animation API on all versions of the platform back to 1.0!
来源	http://nineoldandroids.com/
包名	com.nineoldandroids

3.1.1.36 Facebook ImagePipeline OkHttp 3

序号	36
SDK 名称	Facebook ImagePipeline OkHttp 3
开发者	Facebook
类别	工具
描述	An integration library to use OkHttp 3 as the networking layer in ImagePipeline
来源	https://mvnrepository.com/artifact/com.facebook.fresco/imagepipeline-okhttp3
包名	com.facebook.imagepipeline.backends.okhttp3

3.1.1.37 Google Protocol Buffers

序号	37
SDK 名称	Google Protocol Buffers
开发者	Google
类别	工具
描述	Protocol Buffers(Profbuff) 是一种语言无关、平台无关的可扩展机制，用于序列化结构化数据。
来源	https://developers.google.com/protocol-buffers
包名	com.google.protobuf

3.1.1.38 Facebook Drawee

序号	38
SDK 名称	Facebook Drawee
开发者	Facebook
类别	工具
描述	A fast, feature-rich image display library for Android
来源	https://mvnrepository.com/artifact/com.facebook.fresco/drawee
包名	com.facebook.drawee

3.1.1.39 阿里云 HTTPDNS SDK

序号	39
SDK 名称	阿里云 HTTPDNS SDK
开发者	阿里巴巴
类别	工具
描述	HTTPDNS 是面向多端应用（移动端 APP，PC 客户端应用）的域名解析服务，具有域名防劫持、精准调度、实时解析生效的特性。
来源	https://help.aliyun.com/document_detail/150879.html?spm=a2c4g.11174283.3.2.4a41110c7EJ2nP
包名	com.alibaba.sdk.android.httpdns

3.1.1.40 DanmakuFlameMaster

序号	40
SDK 名称	DanmakuFlameMaster
开发者	bilibili
类别	弹幕
描述	android 上开源弹幕解析绘制引擎项目
来源	https://github.com/bilibili/DanmakuFlameMaster
包名	master.flame.danmaku

3.1.1.41 Gson

序号	41
SDK 名称	Gson
开发者	Google
类别	工具
描述	Google JSON 工具类
来源	https://mvnrepository.com/artifact/com.google.code.gson/gson

包名	com.google.gson

3.1.1.42 中国移动号码认证 SDK

序号	42
SDK 名称	中国移动号码认证 SDK
开发者	中国移动
类别	认证
描述	号码认证能力提供一键登录、本机号码校验服务。一键登录能力，即通过移动认证的网络认证能力，实现 APP 用户无需输入帐号密码，即可使用本机手机号码自动登录的能力。利用应用层无法截取的网络层号码认证能力验证号码的真实性，本机号码自动校验是现有短信验证方式的优化，能消除现有短信验证模式等待时间长、操作繁琐和容易泄露的痛点。通过 SDK/JSSDK 提供的本机号码校验功能，调用网关鉴权方式，验证用户输入的手机号码是否为本机号码。用户在输入手机号码后，后台利用应用层无法截取的网络层号码认证能力来验证手机号码是否为用户的本机号码，实现快捷登入和安全风控，帮助应用拉新促活，安全高效。
来源	http://dev.10086.cn/docInside?contentId=10000067529678
包名	com.cmic.sso.sdk

3.1.1.43 MSA 移动安全联盟 SDK

序号	43
SDK 名称	MSA 移动安全联盟 SDK
开发者	信通院
类别	工具
描述	根据“移动智能终端补充设备标识体系”技术要求，华为、小米、OPPO、vivo、中兴、努比亚、魅族、联想、三星等设备厂商均将逐步实现本标识体系，联盟计划开发并发布支持多厂商的统一的补充设备标识调用 SDK，协助移动应用开发者更便捷的访问移动智能终端补充设备标识体系，推进相关业务。
来源	http://www.msa-alliance.cn/col.jsp?id=120
包名	com.asus.msa

3.1.1.44 新浪微博 SDK

序号	44
SDK 名称	新浪微博 SDK
开发者	新浪
类别	社交
描述	微博 Android 平台 SDK 为第三方微博应用提供了文档易用的微博 API 调用服务，使第三方客户端无需了解复杂的验证，API 调用过程。并可以实现分享到微博的功能，可以分享文字，或者多媒体信息到内置的分享页面，并发送到微博。

来源	https://open.weibo.com/wiki/SDK
包名	com.sina.weibo.sdk

3.1.1.45 百度地图基础定位 SDK

序号	45
SDK 名称	百度地图基础定位 SDK
开发者	百度
类别	地图
描述	包含基础定位能力（GPS/WiFi/基站）、基础位置描述能力；
来源	http://lbs.baidu.com/index.php?title=%E9%A6%96%E9%A1%B5
包名	com.baidu.location

3.1.1.46 VIVO 消息推送 SDK

序号	46
SDK 名称	VIVO 消息推送 SDK
开发者	VIVO
类别	消息推送
描述	vivo 推送是 vivo 公司向开发者提供的消息推送服务，通过在云端与客户端之间建立一条稳定、可靠的长连接，为开发者提供向客户端应用实时推送消息的服务，支持百亿级的通知/消息推送，秒级触达移动用户。 开发者可以方便地通过嵌入 SDK，通过 API 调用或者 Web 端可视化操作，实现对特定用户人群推送，大幅提升用户活跃度，有效唤醒沉睡用户，并实时查看推送效果。
来源	https://dev.vivo.com.cn/documentCenter/doc/365
包名	com.vivo.push

3.1.1.47 淘宝通道服务 SDK

序号	47
SDK 名称	淘宝通道服务 SDK
开发者	淘宝
类别	工具
描述	通道服务是阿里巴巴淘宝无线向开发者提供全双工、低延时、高安全的通道服务，同时具备实时推送消息能力。 支持了手淘的淘友、推送服务)、无线配置推送、优酷、Lazada 等中间件和业务，支撑了海量的数据请求和推送需求，经受住了每年双十一的大流量冲击的考验。
来源	https://help.aliyun.com/document_detail/88790.html?spm=a2c4g.11174283.6.557.799054b5mObqjL
包名	com.taobao.accs com.taobao.agoo

3.1.1.48 Facebook WebpSupport

序号	48
SDK 名称	Facebook WebpSupport
开发者	Facebook
类别	图像
描述	Decoding WebP images on older versions of Android that cannot do so natively
来源	https://mvnrepository.com/artifact/com.facebook.fresco/webpsupport
包名	com.facebook.webpsupport

3.1.1.49 微信 SDK

序号	49
SDK 名称	微信 SDK
开发者	腾讯
类别	社交
描述	提供微信分享、登录、收藏、支付等功能
来源	https://developers.weixin.qq.com/doc/oplatform/Mobile_App/Access_Guide/Android.html
包名	com.tencent.mm.opensdk

3.1.1.50 netty

序号	50
SDK 名称	netty
开发者	Netty 项目社区
类别	通信
描述	Netty 是一个非阻塞 I/O 客户端-服务器框架，主要用于开发 Java 网络应用程序，如协议服务器和客户端。
来源	https://mvnrepository.com/artifact/io.netty/netty-all
包名	io.netty

3.1.1.51 友盟移动统计 SDK

序号	51
SDK 名称	友盟移动统计 SDK
开发者	友盟
类别	APM
描述	统计分析组件可精准统计应用的新增、启动、活跃、自定义事件等指标，并包含定位

	crash 错误定位功能。新版本统计 SDK（8.0.0 以上）简化集成过程，支持一行代码完成基础统计指标集成；支持多种页面统计模式，方便老用户无缝升级。
来源	https://developer.umeng.com/sdk
包名	com.umeng.commonsdk.statistics

3.1.1.52 Android-PickerView

序号	52
SDK 名称	Android-PickerView
开发者	Bigkoo
类别	工具
描述	这是一款仿 iOS 的 PickerView 控件，有时间选择器和选项选择器，新版本的详细特性如下： ——TimePickerView 时间选择器，支持年月日时分，年月日，年月，时分等格式。 ——OptionsPickerView 选项选择器，支持一，二，三级选项选择，并且可以设置是否联动 。
来源	https://github.com/Bigkoo/Android-PickerView
包名	com.bigkoo.pickerview

3.1.1.53 Google Play Services Auth

序号	53
SDK 名称	Google Play Services Auth
开发者	Google
类别	认证
描述	Google Account Login
来源	https://developers.google.com/android/guides/setup
包名	com.google.android.gms.auth

3.1.1.54 Robust

序号	54
SDK 名称	Robust
开发者	美团
类别	工具
描述	Robust 是新一代热更新系统，无差别兼容 Android2.3-10 版本；无需重启补丁实时生效，快速修复线上问题，补丁修补成功率高达 99.9%。
来源	https://github.com/Meituan-Dianping/Robust
包名	com.meituan.robust

3.1.1.55 Retrofit 2

序号	55
SDK 名称	Retrofit 2
开发者	Square
类别	通信
描述	Retrofit 是一个网络访问框架，和 OkHttp 同样出自 Square 公司，Retrofit 内部依赖于 OkHttp，但是功能上做了更多的扩展,比如返回结果的转换功能，可以直接对返回数据进行处理。
来源	https://github.com/square/retrofit
包名	retrofit2

3.1.1.56 Zxing

序号	56
SDK 名称	Zxing
开发者	Google
类别	工具
描述	ZXing ("Zebra Crossing") barcode scanning library for Java, Android
来源	https://github.com/zxing/zxing
包名	com.google.zxing

3.1.1.57 华为消息推送 SDK

序号	57
SDK 名称	华为消息推送 SDK
开发者	华为
类别	消息推送
描述	推送服务（Push Kit）是华为为开发者提供的消息推送平台，建立了从云端到终端的消息推送通道。开发者通过集成 Push Kit 可以实时推送消息到用户终端应用，构筑良好的用户关系，提升用户的感知度和活跃度。
来源	https://developer.huawei.com/consumer/cn/doc/HMSCore-Library-V5/eclipse-sdk-download-0000001051065996-V5
包名	com.huawei.hms.support.api.entity.push com.huawei.hms.support.api.push

3.1.1.58 Facebook Common Android SDK

序号	58
SDK 名称	Facebook Common Android SDK

开发者	Facebook
类别	工具
描述	Facebook Android SDK 中的公有部分
来源	https://mvnrepository.com/artifact/com.facebook.android/facebook-common
包名	com.facebook.common

3.1.1.59 Google Play Services Ads

序号	59
SDK 名称	Google Play Services Ads
开发者	Google
类别	广告
描述	Google Mobile Ads
来源	https://developers.google.com/android/guides/setup
包名	com.google.android.gms.ads

3.1.1.60 网易云信音视频通话 1.0SDK

序号	60
SDK 名称	网易云信音视频通话 1.0SDK
开发者	网易
类别	音视频
描述	网易云通信实时音视频服务适用于各种实时音视频场景，比如社交行业的视频聊天、视频交友、教育行业的小班化教学、点对点视频教学、企业内部的多人会议、远程医疗、游戏语音等等。
来源	http://dev.yunxin.163.com/docs/product/%E9%9F%B3%E8%A7%86%E9%A2%91%E9%80%9A%E8%AF%9D1.0/%E4%BA%A7%E5%93%81%E4%BB%8B%E7%BB%8D/%E7%AE%80%E4%BB%8B
包名	com.netease.nimlib.sdk.avchat

3.1.1.61 讯飞 MSC SDK

序号	61
SDK 名称	讯飞 MSC SDK
开发者	科大讯飞
类别	工具
描述	讯飞开放平台作为全球首个开放的智能交互技术服务平台，致力于为开发者打造一站式智能人机交互解决方案。用户可通过互联网、移动互联网，使用任何设备、在任何时间、任何地点，随时随地享受讯飞开放平台提供的“听、说、读、写……”等全方位的人工智能服务。目前，开放平台以“云+端”的形式向开发者提供语音合成、语音识别、语音唤醒、语义理解、人脸识别等多项服务。

来源	https://www.xfyun.cn/doc/platform/xfyunreadme.html#%E5%B9%B3%E5%8F%B0%E7%89%B9%E8%89%B2
包名	com.iflytek.msc

3.1.1.62 OkHttp

序号	62
SDK 名称	OkHttp
开发者	Square Open Source
类别	工具
描述	Square’ s meticulous HTTP client for Java and Kotlin.
来源	https://square.github.io/okhttp
包名	okhttp3.internal

3.1.1.63 腾讯移动开放平台 SDK

序号	63
SDK 名称	腾讯移动开放平台 SDK
开发者	腾讯
类别	社交
描述	腾讯 QQ 互联平台 SDK，辅助开发者快速接入 QQ 登录、分享等功能。
来源	https://wiki.connect.qq.com/
包名	com.tencent.tauth com.tencent.open com.tencent.connect

3.1.1.64 Google Play Services Location

序号	64
SDK 名称	Google Play Services Location
开发者	Google
类别	工具
描述	Google Location and Activity Recognition
来源	https://developers.google.com/android/guides/setup
包名	com.google.android.gms.location

3.1.1.65 AndroidSVG

序号	65
SDK 名称	AndroidSVG

开发者	BigBadaboom
类别	工具
描述	AndroidSVG is a SVG parser and renderer for Android. It has almost complete support for the static visual elements of the SVG 1.1 and SVG 1.2 Tiny specifications (except for filters). AndroidSVG correctly renders the SVG Acid Test.
来源	https://github.com/BigBadaboom/androidsvg
包名	com.caverock.androidsvg

3.2 漏洞分析

该 APP 检测出 7 项漏洞。

3.2.1 HTTPS 允许任意主机名漏洞

测评目的	检测 App 在使用 HTTPS 协议传输数据时是否允许任意服务器主机名。
危险等级	中
危害	使用 HTTPS 协议时，客户端必须对服务器身份进行完整性校验，以验证服务器是真实合法的目标服务器。如果没有校验，客户端可能与仿冒的服务器建立通信链接，即“中间人攻击”。Android 中默认的 HTTPS 证书验证机制不接受不可信的连接，因而是安全的，但 Android 允许开发者重定义证书验证方法：1）使用 X509TrustManager 类检查证书是否合法并且是否未过期；2）使用 HostnameVerifier 类检查证书中的主机名与使用该证书的服务器的主机名是否一致。重写的 HostnameVerifier，当被配置为接受任何服务器主机名时，等同不对主机名进行校验，是导致“中间人攻击”的主要原因之一。当发生中间人攻击时，仿冒的中间人可以冒充服务器与手机客户端进行交互，同时冒充手机客户端与服务器进行交互，在充当中间人转发信息的时候，窃取手机号，账号，密码等敏感信息，甚至可能对通信内容进行篡改。
测评结果	安全
测评结果描述	该 App 在使用 HTTPS 协议传输数据时未允许任意服务器主机名。

3.2.2 RSA 加密算法不安全使用漏洞

测评目的	检测 App 中是否存在 RSA 加密算法不安全使用的漏洞。
危险等级	中
危害	RSA 算法是最为典型的非对称加密算法，也是当今应用范围最为广泛的非对称加密算法，也是第一个能用于数据加密也能用于数字签名的算法。使用 RSA 加密算法时，应注意以下两点：1.密钥长度过短，会导致密钥被破解，通常小于 512bit 的密钥即存在破解的风险；2.加密算法没有使用正确的工作模式和填充方式，容易导致部分加密数

	据被破解或者遭到选择明文攻击（CPA）。RSA 加密算法的不安全使用，可能导致客户端隐私数据泄露，加密文件破解，传输数据被获取，中间人攻击等后果，造成用户敏感信息被窃取，甚至造成财产损失。
测评结果	发现 21 处风险
测评结果描述	该 App 中存在不安全的 RSA 加密算法使用漏洞。
测评详细信息	1.[文件] com/suning/mobile/epaencryption/RSAEncrypt 1.[方法] public static decryptByPrivateKey(Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String; 2.[文件] com/suning/mobile/epaencryption/RSAEncrypt 2.[方法] public static decryptByPrivateKey([BLjava/lang/String;)[B 3.[文件] com/suning/mobile/epaencryption/RSAEncrypt 3.[方法] public static decryptByPublicKey([BLjava/lang/String;)[B 4.[文件] com/suning/mobile/epaencryption/RSAEncrypt 4.[方法] public static encryptByPrivateKey([BLjava/lang/String;)[B 5.[文件] com/suning/mobile/epaencryption/RSAEncrypt 5.[方法] public static encryptByPublicKey(Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String; 6.[文件] com/suning/mobile/epaencryption/RSAEncrypt 6.[方法] public static encryptByPublicKey([BLjava/lang/String;)[B 7.[文件] com/suning/mobile/epa/NetworkKits/net/basic/RSAUtil 7.[方法] public static decryptByPrivateKey(Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String; 8.[文件] com/suning/mobile/epa/NetworkKits/net/basic/RSAUtil 8.[方法] public static decryptByPrivateKey([BLjava/lang/String;)[B 9.[文件] com/suning/mobile/epa/NetworkKits/net/basic/RSAUtil 9.[方法] public static decryptByPublicKey([BLjava/lang/String;)[B 10.[文件] com/suning/mobile/epa/NetworkKits/net/basic/RSAUtil 10.[方法] public static encryptByPrivateKey([BLjava/lang/String;)[B 11.[文件] com/suning/mobile/epa/NetworkKits/net/basic/RSAUtil 11.[方法] public static encryptByPublicKey(Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String; 12.[文件] com/suning/mobile/epa/NetworkKits/net/basic/RSAUtil 12.[方法] public static encryptByPublicKey([BLjava/lang/String;)[B 13.[文件] com/suning/mobile/epa/NetworkKits/net/basic/RSAUtil

	13.[方法] public static otpEncryptByPublicKey(Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String; 14.[文件] com/android/recharge/RSAUtils 14.[方法] public static decryptByPrivateKey(Ljava/lang/String;Ljava/security/interfaces/RSAPrivateKey;)Ljava/lang/String; 15.[文件] com/android/recharge/RSAUtils 15.[方法] public static decryptData(Ljava/security/interfaces/RSAPrivateKey;[B)[B 16.[文件] com/android/recharge/RSAUtils 16.[方法] public static encryptByPublicKey(Ljava/lang/String;Ljava/security/interfaces/RSAPublicKey;)Ljava/lang/String; 17.[文件] com/android/recharge/RSAUtils 17.[方法] public static encryptData(Ljava/security/interfaces/RSAPublicKey;[B)[B 18.[文件] com/android/recharge/RSAEncrypt 18.[方法] public static decrypt(Ljava/security/interfaces/RSAPrivateKey;[B)[B 19.[文件] com/android/recharge/RSAEncrypt 19.[方法] public static decrypt(Ljava/security/interfaces/RSAPublicKey;[B)[B 20.[文件] com/android/recharge/RSAEncrypt 20.[方法] public static encrypt(Ljava/security/interfaces/RSAPrivateKey;[B)[B 21.[文件] com/android/recharge/RSAEncrypt 21.[方法] public static encrypt(Ljava/security/interfaces/RSAPublicKey;[B)[B
解决方案	开发者自查：使用 RSA 加密算法时，密钥长度建议设置为 2048bit，同时分别设置工作模式为 ECB，填充模式为 OAEPWithSHA256AndMGF1Padding。以下为修复代码示例： 1.KeyPairGeneratorDemoKey=KeyPairGenerator.getInstance("RSA");DemoKey.initialize(2048);2.CipherDemoCipher=Cipher.getInstance("RSA/ECB/OAEPWithSHA256AndMGF1Padding");DemoCipher.init(Cipher.ENCRYPT_MODE,keyPrivate);"

3.2.3 getDir 数据全局可读写漏洞

测评目的	检测 App 中是否存在 getDir 数据全局可读写的漏洞

危险等级	中
危害	Context.getDir（String name , int mode）是访问 Andoid 系统的 Internal Storage 的一个重要方式，用于在应用程序的数据文件夹下获取或者创建一个存放应用程序自定义文件的文件夹。当该函数的第二参数使用了如果使用了 MODE_WORLD_READABLE 模式，或者使用了 MODE_WORLD_WRITEABLE 模式，或者配置了“android:sharedUserId”属性值时，可能导致储存于该文件夹中的敏感信息被其他程序读写，导致应用内明文存储的个人身份信息、密码以及 token 等重要敏感信息泄露，或者存储的用户信息、历史数据被篡改，诱导用户误操作等。更为严重的是具备 root 权限的程序或用户可对所有应用程序通过任意模式（包括 MODE_PRIVATE）创建的文件夹进行读写操作。
测评结果	安全
测评结果描述	该 App 中不存在 getDir 数据全局可读写的漏洞。

3.2.4 全局可读写的内部文件漏洞

测评目的	检测 App 应用中是否存在内部文件，可被其他任意 App 读写。
危险等级	中
危害	为了实现不同软件之间的数据共享，设置内部文件为全局可读或全局可写，导致其他应用可以读取和修改该文件。如果此类文件包含了关键配置信息，账户信息数据等敏感信息，可能会被盗取或者恶意篡改，导致如程序无法运行，业务逻辑被修改等问题。
测评结果	发现 1 处风险
测评结果描述	该 App 应用中存在全局可读写的内部文件，其中内部文件中可能存在敏感信息，其他应用可以直接读写该文件信息。
测评详细信息	1.[文件] com/baidu/a/a/a/b/c 1.[方法] private a(Ljava/lang/String;)Z
解决方案	开发者自查：根据需要严格控制文件的全局读写权限；对于必须使用的全局可读写文件，严格审核其中是否包含敏感信息。"

3.2.5 Internal Storage 数据全局可读写漏洞

测评目的	检测 App 中是否存在 Internal Storage 数据全局可读写漏洞。
危险等级	中
危害	Internal Storage 作为 Android 系统的本地数据存储方式之一，可将应用数据直接存储于设备的内部存储器中。当使用 Internal Storage 方式在创建本地存储文件时，如果使用了 MODE_WORLD_READABLE 模式，或者使用了 MODE_WORLD_WRITEABLE 模式，或者配置了“android:sharedUserId”属性值时，可能导致储存于 Internal Storage 文件中的敏感信息被其他程序读写，导致应用内明文存储的个人身份信息、密码以及 token 等重要敏感信息泄露，或者存储的用户信息、历史数据被篡改，诱导用户误操作等。更为严重的是具备 root 权限的程序或

	用户可对所有应用程序通过任意模式（包括 MODE_PRIVATE）创建的 Internal Storage 文件进行读写操作。
测评结果	发现 1 处风险
测评结果描述	该 App 中存在 Internal Storage 数据可被全局读写的漏洞。
测评详细信息	1.[文件] com/baidu/a/a/a/b/c 1.[方法] private a(Ljava/lang/String;)Z
解决方案	开发者自查：避免使用 InternalStorage 的存储方式来保存用户名、密码等敏感数据信息，当 Android 设备被 root 之后，该安全机制将失效而导致信息泄露；当必需使用 InternalStorage 的存储方式来实现功能时，需要将创建模式设置为"MODE_PRIVATE"，并禁用“android:sharedUserId”属性值。避免在进程间通信时使用具有全局可读写模式的 InternalStorage 文件来进行数据共享，建议使用更加正式的方式，包括 ContentProvider 和 BroadcastReceiver。"

3.2.6 病毒扫描

测评目的	检测 App 程序中是否包含病毒
危险等级	高
危害	
测评结果	
测评结果描述	
测评详细信息	
解决方案	

3.2.7 “应用克隆”漏洞攻击风险

测评目的	检测 App 中是否存在利用 webview 跨域访问进行“应用克隆”漏洞攻击的风险。
危险等级	高
危害	WebView 是 Android 用于显示网页的控件。当 Android 应用中存在包含 webview 的可被导出 Activity 组件时，若该 WebView 允许通过 file url 对 http 域进行访问，并且未对访问的路径进行严格校验，则可能导致“应用克隆”漏洞攻击。攻击者利用该漏洞，可远程获取用户隐私信息（包括手机应用数据、照片、文档等敏感信息）导致数据泄露，可远程打开并加载恶意 HTML 文件，甚至获取 App 中包括用户登录凭证在内的所有本地敏感数据。
测评结果	安全
测评结果描述	该 App 应用无法利用“应用克隆”漏洞进行攻击。

3.2.8 AES/DES 加密方法不安全使用漏洞

测评目的	检测 App 程序中使用 AES/DES 加密算法时是否使用了不安全的加密模式。
危险等级	低
危害	AES/DES 是 android 程序中常用的两种对称加密算法，其工作模式有 ECB、CBC、CFB 和 OFB。当其使用 ECB 或 OFB 工作模式时，加密数据可能被选择明文攻击 CPA 破解。加密方法失效后可能导致客户端隐私数据泄露，加密文件破解，传输数据被获取，中间人攻击等后果，造成用户敏感信息被窃取。
测评结果	发现 4 处风险
测评结果描述	该 App 程序中的加密算法使用了不安全的加密模式。
测评详细信息	1.[文件] smali_classes6/tmsdkobf/ec 1.[方法] private static a([B[B)[B 2.[文件] smali_classes3/com/suning/mobile/epa/etc/m/f 2.[方法] public static a(Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String; 3.[文件] smali_classes3/com/suning/mobile/epa/etc/m/f 3.[方法] public static b(Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String; 4.[文件] smali_classes2/e/e/k1 4.[方法] public static b([B[B)[B
解决方案	开发者自查：使用 AES/DES 加密算法时应显示设定工作模式为 CBC 或 CFB 模式。"

3.2.9 SharedPreferences 数据全局可读写漏洞

测评目的	检测 App 中是否存在 SharedPreferences 数据全局可读写漏洞。
危险等级	中
危害	SharedPreferences 作为 Android 系统的本地数据存储方式之一，可将应用数据以键值对（key-value）的存储形式永久保存于 App 应用中。当使用 SharedPreferences 方式在创建本地存储文件时，如果使用了 MODE_WORLD_READABLE 模式，或者使用了 MODE_WORLD_WRITEABLE 模式并且配置了“android:sharedUserId”属性值时，可能导致储存于 SharedPreferences 文件中的敏感信息被其他程序读写，导致应用内明文存储的个人身份信息、密码以及 token 等重要敏感信息泄露，或者存储的用户信息、历史数据被篡改，诱导用户误操作等。更为严重的是具备 root 权限的程序或用户可对所有应用程序通过任意模式（包括 MODE_PRIVATE）创建的的 Shared Preferences 文件进行读写操作。
测评结果	安全
测评结果描述	该 App 中不存在 SharedPreferences 数据可被全局读写的漏洞。

3.2.10 HTTPS 未校验服务器证书漏洞

测评目的	检测 App 在使用 HTTPS 协议传输数据时是否对服务器证书进行校验。
危险等级	中
危害	使用 HTTPS 协议时，客户端必须对服务器身份进行完整性校验，以验证服务器是真实合法的目标服务器。如果没有校验，客户端可能与仿冒的服务器建立通信链接，即“中间人攻击”。Android 中默认的 HTTPS 证书验证机制不接受不可信的连接，因而是安全的，但 Android 允许开发者重定义证书验证方法：1）使用 X509TrustManager 类检查证书是否合法并且是否未过期；2）使用 HostnameVerifier 类检查证书中的主机名与使用该证书的服务器的主机名是否一致。重写的 X509TrustManager，其中的 checkServerTrusted()方法不对验证失败做任何处理，即不对证书进行正确校验结果，是导致“中间人攻击”的主要原因之一。当发生中间人攻击时，仿冒的中间人可以冒充服务器与手机客户端进行交互，同时冒充手机客户端与服务器进行交互，在充当中间人转发信息的时候，窃取手机号，账号，密码等敏感信息，甚至可能对通信内容进行篡改。
测评结果	发现 4 处风险
测评结果描述	该 App 应用在使用 HTTPS 进行数据传输时未校验服务器证书。
测评详细信息	1.[文件] com/suning/mobile/epa/riskcontrolkba/utils/net/NonAuthenticationX509TrustManager 1.[方法] public checkServerTrusted([Ljava/security/cert/X509Certificate;Ljava/lang/String;)V 2.[文件] e/o/a/a/d/a$d 2.[方法] public checkServerTrusted([Ljava/security/cert/X509Certificate;Ljava/lang/String;)V 3.[文件] com/weconex/jsykt/http/base/secure/SSLDefaultConfig$2 3.[方法] public checkServerTrusted([Ljava/security/cert/X509Certificate;Ljava/lang/String;)V 4.[文件] anet/channel/util/bba 4.[方法] public checkServerTrusted([Ljava/security/cert/X509Certificate;Ljava/lang/String;)V
解决方案	开发者自查：开发者在使用 https 时应对服务器证书进行合法性校验并且当校验失败时正确处理。以下为修复代码示例： privateclassDemoTrustManagerimplementsX509TrustManager{@OverridepublicvoidcheckClientTrusted(X509Certificate[]chain,StringauthType)throwsCertificateException{}@OverridepublicvoidcheckServerTrusted(X509Certificate[]chain,StringauthType)throwsCertificateException{for(X509Certificatecert:chain){//Makesurethatithasn'texpired.cert.checkValidity();//Verifythecertificate'spublickeychain.try{cert.verify(((X509Certificate)ca).getPublicKey());}catch(NoSuchAlgorithmExceptione){}catch(InvalidKeyExceptione){}catch(NoSuchProviderExceptione){}catch(SignatureExceptione){}}}@OverridepublicX509Certificate[]getAcceptedIssuers()

	{returnnewX509Certificate[0];}。"

3.2.11 数据库文件任意读写漏洞

测评目的	检测 App 中是否存在可被任意读写的数据库文件。
危险等级	中
危害	database 配置模式安全风险源于:创建数据库(Database)时没有正确的选取合适的创建模式(MO DE_PRIVATE、MODE_WORLD_READABLE 以及 MODE_WORLD_WRITEABLE)进行权限控制，从而导致数据库(Database)内容被恶意读写，造成账户密码、身份信息、金融账户其他敏感信息的泄露， 甚至可能导致攻击者进一步实施恶意攻击。
测评结果	安全
测评结果描述	该 Apk 程序不存在可被任意读写的数据库文件。

3.2.12 HTTPS 未校验主机名漏洞

测评目的	检测 App 在使用 HTTPS 协议传输数据时是否对服务器主机名进行校验。
危险等级	中
危害	使用 HTTPS 协议时，客户端必须对服务器身份进行完整性校验，以验证服务器是真实合法的目标服务器。如果没有校验，客户端可能与仿冒的服务器建立通信链接，即“中间人攻击”。Android 中默认的 HTTPS 证书验证机制不接受不可信的连接，因而是安全的，但 Android 允许开发者重定义证书验证方法：1）使用 X509TrustManager 类检查证书是否合法并且是否未过期；2）使用 HostnameVerifier 类检查证书中的主机名与使用该证书的服务器的主机名是否一致。重写的 HostnameVerifier，其中的 Verify()方法不对主机名验证失败做任何处理，即不对主机名进行正确校验，是导致“中间人攻击”的主要原因之一。当发生中间人攻击时，仿冒的中间人可以冒充服务器与手机客户端进行交互，同时冒充手机客户端与服务器进行交互，在充当中间人转发信息的时候，窃取手机号，账号，密码等敏感信息，甚至可能对通信内容进行篡改。
测评结果	发现 4 处风险
测评结果描述	该 App 应用在使用 HTTPS 进行数据传输时未校验服务器主机名。
测评详细信息	1.[文件] com/suning/sastatistics/tools/d$1 1.[方法] public final verify(Ljava/lang/String;Ljavax/net/ssl/SSLSession;)Z 2.[文件] e/g/a/p/a/c/b$b 2.[方法] public final verify(Ljava/lang/String;Ljavax/net/ssl/SSLSession;)Z 3.[文件] e/g/a/p/a/c/b$a 3.[方法] public final verify(Ljava/lang/String;Ljavax/net/ssl/SSLSession;)Z

	4.[文件] e/e/o0$a 4.[方法] public final verify(Ljava/lang/String;Ljavax/net/ssl/SSLSession;)Z
解决方案	开发者自查：开发者在使用 https 时应对服务器主机名进行校验并且当校验失败时正确处理。以下为修复代码示例：HostnameVerifierhnv=newHostnameVerifier() {@Overridepublicbooleanverify(Stringhostname,SSLSessionsession) {if("Demohostname".equals(hostname)) {returntrue;}else{HostnameVerifierhv=HttpsURLConnection.getDefaultHostnameVerifier();returnhv.verify(hostname,session);}}};"

3.2.13 Java 代码反编译风险

测评目的	检测 java 层代码是否存在源代码被反编译而泄露的风险。
危险等级	高
危害	Apk 如果未采取有效的保护措施，可能面临被反编译的风险。反编译是将二进制程序转换成人们易读的一种描述语言的形式。反编译的结果是应用程序的代码，这样就暴露了客户端的所有逻辑，比如与服务端的通讯方式，加解密算法、密钥，转账业务流程、软键盘技术实现等等。攻击者可以利用这些信息窃取客户端的敏感数据，包括手机号、密码；截获与服务器之间的通信数据；绕过业务安全认证流程，直接篡改用户账号信息；对服务器接口发起攻击等。
测评结果	发现 1 处风险
测评结果描述	该 Apk 可以被反编译后获取源代码。
测评详细信息	
解决方案	第三方支持：使用具有防反编译功能的第三方专业加固方案，防止应用被反编译。"

3.2.14 Janus 签名机制漏洞

测评目的	检测 App 程序是否存在 Janus 签名机制漏洞。
危险等级	高
危害	Google 披露了一个名为“Janus”的安卓漏洞（漏洞编号：CVE-2017-13156），该漏洞可以让攻击者绕过安卓系统的 Signature scheme V1 签名机制，用篡改过的 APK 覆盖原有的应用，并可访问原应用所有的数据，直接对 App 进行篡改。由于安卓系统的其他安全机制也是建立在签名和校验基础上的，所以可以说该漏洞相当于绕过了安卓系统的整个安全机制。该漏洞的影响范围：安卓 5.0-8.0 的各个版本系统；使用安卓 Signature scheme V1 签名的 App APK 文件。该漏洞的危害：对存储在原手机上的数据进行读取； 对用户的输入做各种监听、拦截、欺诈，引导用户输入密码，转账；更新 Android 的系统 APP，从获得更高的系统权限，甚至 root/越狱，为其他攻击做准备。
测评结果	安全
测评结果描述	该 App 不存在 Janus 签名机制漏洞

3.2.15 So 文件破解风险

测评目的	检测 SDK 中的 so 文件是否可被破解读取。
危险等级	低
危害	So 文件属于动态链接库文件，它是将 C/C++语言实现的核心代码编译为 so 库供 Java 层调用。So 被破解可能导致核心功能的汇编代码甚至源代码泄露，不仅损害开发者的知识产权，并且可能暴露了 SDK 的核心技术和核心功能逻辑。如果 App 集成了该 SDK，攻击者可以利用这些信息窃取客户端的敏感数据，包括手机号、密码；截获与服务器之间的通信数据；绕过业务安全认证流程，直接篡改用户账号信息；对服务器接口发起攻击等。
测评结果	安全
测评结果描述	该 SDK 中不存在可被破解的 so 文件。

3.3 行为分析

3.3.1 数据通信

该 APP 在检测时间内，共产生访问外部 URL 15 个，共计 301 次，具体情况如下：

序号	主体	包名	域名	IP	IP 归属地	协议	次数
1	Volley	com.android.okhttp	click.suning.cn	118.112.11.143	中国 四川省 成都市	https	148
2	Volley	com.android.okhttp	apm.suning.cn	101.125.252.192	中国 江苏省 南京市	https	36
3	百度云推送 SDK	com.baidu.security	msc.baidu.com	220.181.107.218	中国 北京 北京市	https	28
4	阿里云 HTTPDNS SDK	com.alibaba.sdk	adash.man.aliyuncs.com	106.11.248.37	中国 上海 上海市	http	17
5	友盟移动统计 SDK	com.umeng.commonsdk	plbslog.umeng.com	203.119.207.252	中国 河北省 张家口市	https	15
6	Volley	com.android.okhttp	mmds.suning.com	183.134.25.30	中国 浙江省 台州市	https	11
7	Volley	com.android.okhttp	dt.netease.im	59.111.160.235	中国 浙江省 杭州市	https	9
8	Volley	com.android.okhttp	scs.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	9
9	App	anet.channel.strate	106.11.61.137	106.11.61.137	中国 上海 上海市	http	6

		gy					
10	讯飞 MSC SDK	com.iflytek.cloud	data.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	5
11	Volley	com.android.okhttp	mfg.suning.com	183.134.25.31	中国 浙江省 台州市	https	5
12	Volley	com.android.okhttp	dfp.suning.com	183.134.25.31	中国 浙江省 台州市	https	5
13	PhotoView	com.suning.maa	fastcfg.suning.com	222.190.116.13	中国 江苏省 南京市	http	4
14	App	anet.channel.strategy	106.11.61.135	106.11.61.135	中国 上海 上海市	http	2
15	PhotoView	com.suning.maa	oss.suning.com	183.134.25.32	中国 浙江省 台州市	https	1

3.3.2 异常通信

该 App 在检测期间发生异常通信行为共 301 次，其中涉及 13 个 IP 地址,具体情况如下：

序号	主体	包名	IP	通信次数	异常行为
1	Volley	com.android.okhttp	118.112.11.143	148	未做证书校验可进行中间人攻击,检测出个人信息:
2	Volley	com.android.okhttp	101.125.252.192	36	未做证书校验可进行中间人攻击,检测出个人信息:
3	Volley	com.android.okhttp	220.181.107.218	28	未做证书校验可进行中间人攻击,检测出个人信息:
4	Volley	com.android.okhttp	106.11.248.37	17	未做证书校验可进行中间人攻击,检测出个人信息:
5	Volley	com.android.okhttp	203.119.207.252	15	未做证书校验可进行中间人攻击,检测出个人信息:
6	Volley	com.android.okhttp	183.134.25.30	11	未做证书校验可进行中间人攻击,检测出个人信息:

7	Volley	com.android.okhttp	59.111.160.235	9	未做证书校验可进行中间人攻击,检测出个人信息:
8	Volley	com.android.okhttp	220.248.230.134	9	未做证书校验可进行中间人攻击,检测出个人信息:
9	Volley	com.android.okhttp	106.11.61.137	6	未做证书校验可进行中间人攻击,检测出个人信息:
10	Volley	com.android.okhttp	220.248.230.134	5	未做证书校验可进行中间人攻击,检测出个人信息:
11	Volley	com.android.okhttp	183.134.25.31	5	未做证书校验可进行中间人攻击,检测出个人信息:
12	PhotoView	com.suning.fpcore	183.134.25.31	5	未做证书校验可进行中间人攻击,检测出个人信息:
13	Volley	com.android.okhttp	222.190.116.13	4	未做证书校验可进行中间人攻击,检测出个人信息:
14	Volley	com.android.okhttp	106.11.61.135	2	未做证书校验可进行中间人攻击,检测出个人信息:
15	PhotoView	com.suning.maa	183.134.25.32	1	未做证书校验可进行中间人攻击,检测出个人信息:

3.3.3 数据跨境传输行为

该 App 在检测期间未发生数据跨境传输行为。

3.3.4 输入个人信息

该 App 在检测期间共检测输入个人信息 17 次,具体情况如下:

序号	输入内容	文件路径
1	[请输入持卡人姓名]	/res/layout/creditcard_repayment_fragment_add_creditcard.xml
2	[请输入您的身份证号码]	/res/layout/paysdk_fragment_retrieve_paypwd_sms.xml
3	[请输入支付密码]	/res/layout/paysdk_fastpay_dense_old_fragment.xml
4	[请输入您的姓名, 请输入您的身份证号]	/res/layout/prn_sdk_fragment_bankcard_info.xml
5	[请输入手机号/邮箱]	/res/layout/paysdk2_sms_login_fragment.xml
6	[请输入手机号/邮箱, 请输入登录密码]	/res/layout/paysdk2_pwd_login_fragment.xml
7	[请输入手机号，方便我们联系您]	/res/layout/fragment_userfeedback.xml
8	[请输入手机号码]	/res/layout/paysdk_fragment_eppbindphone_layout.xml
9	[请输入支付密码]	/res/layout/pay_kernel_dense_pwd_widget.xml
10	[请输入收款人手机号]	/res/layout/fragment_transfer_qrcode.xml
11	[请输入收款人手机号]	/res/layout/transfer_manager_frag_t_account_validation.xml
12	[请输入支付密码]	/res/layout/sheet_penghua_pay_dense_fragment.xml
13	[请输入银行预留手机号]	/res/layout/paysdk2_fragment_epp_changephone_layout.xml
14	[请输入身份证号]	/res/layout/paysdk_fragment_scap_layout.xml
15	[请输入账号]	/res/layout/rlp_sdk_activity_account.xml
16	[请输入手机号码]	/res/layout/

		fragment_user_feedback.xml
17	[请输入持卡人姓名]	/res/layout/ creditcard_repayment_fragment_add_credit_card.xml

3.3.5 使用权限

该 APP 在检测期间使用权限共 9 个，其中涉及可收集个人信息权限 4 个,具体情况如下:

序号	权限项	权限含义	类型	保护级别	是否敏感
1	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是
2	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否
3	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否
4	INTERNET	访问网络	官方	正常	否
5	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是
6	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是
7	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是
8	BLUETOOTH	创建蓝牙连接	官方	正常	否
9	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否

该 App 在检测期间使用权限共 314 次，其中涉及可收集个人信息权限 106 次，具体情况如下:

序号	主体	包名	使用权限	次数
1	讯飞 MSC SDK	com.iflytek.cloud	ACCESS_FINE_LOCATION	8
2	App	lte.NCall.IV	ACCESS_NETWORK_STATE	10
3	App	org.chromium.media	MODIFY_AUDIO_SETTINGS	2
4	App	sun.util.logging	INTERNET	35
5	讯飞 MSC SDK	com.iflytek.cloud	READ_EXTERNAL_STORAGE	31
6	讯飞 MSC SDK	com.iflytek.cloud	ACCESS_COARSE	3

			_LOCATION	
7	App	e.g.a	READ_PHONE_STATE	64
8	App	org.chromium.media	BLUETOOTH	4
9	App	ct0000.ct0001.ct0000	ACCESS_WIFI_STATE	157

3.3.6 后台使用权限

该 App 在检测期间后台使用权限共 7 个，其中涉及可收集个人信息权限 3 个，具体情况如下：

序号	权限项	权限含义	类型	保护级别	是否敏感
1	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是
2	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否
3	INTERNET	访问网络	官方	正常	否
4	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是
5	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是
6	BLUETOOTH	创建蓝牙连接	官方	正常	否
7	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否

该 App 在检测期间后台使用权限共 44 次，其中涉及可收集个人信息权限 15 次，具体情况如下：

序号	主体	包名	使用权限	次数
1	讯飞 MSC SDK	com.iflytek.cloud	ACCESS_FINE_LOCATION	1
2	App	org.chromium.media	MODIFY_AUDIO_SETTINGS	2
3	App	sun.util.logging	INTERNET	4
4	讯飞 MSC SDK	com.iflytek.cloud	READ_EXTERNAL_STORAGE	6
5	App	e.g.a	READ_PHONE_STATE	8
6	App	org.chromium.me	BLUETOOTH	4

		dia		
7	App	ct0000.ct0001.ct0000	ACCESS_WIFI_STATE	19

3.3.7 尝试使用未声明权限

该 APP 在检测期间访问未申请权限情况如下表：

序号	主体	包名	权限名称	权限含义	类型	保护级别	敏感权限	次数
1	APP	org.chromium.content	WRITE_SETTINGS	修改全局系统设置	官方	特殊	否	30

3.3.8 声明权限但未使用

该 App 在 AndroidManifest.xml 中声明权限共 84 个，其中 139 个权限在检测期间未使用，占比为 165.48%，具体情况如下：

序号	声明权限但未使用	权限含义	类型	保护级别	敏感权限
1	FLASHLIGHT	控制闪光灯	官方	正常	否
2	SYSTEM_OVERLAY_WINDOW	自定义权限	自定义	N/A	否
3	RECORD_AUDIO	录音	官方	危险	是
4	CHANGE_WIFI_STATE	更改 WLAN 状态	官方	正常	否
5	USE_FACERECOGNITION	自定义权限	自定义	N/A	否
6	READ_SETTINGS	读取全局系统设置	官方	N/A	否
7	WAKE_LOCK	防止手机休眠	官方	正常	否
8	WRITE_EXTERNAL_STORAGE	修改/删除 SD 卡中的内容	官方	危险	是
9	REORDER_TASKS	对正在运行的应用程序重新排序	官方	正常	否
10	SYSTEM_ALERT_WINDOW	显示系统级警报	官方	特殊	否
11	EXPAND_STAT	展开/收拢状态	官方	正常	否

	US_BAR	栏			
12	FLAG_ACTIVITY_NEW_TASK	自定义权限	自定义	N/A	否
13	ACCESS_LOCATION_EXTRA_COMMANDS	访问额外的位置信息提供程序命令	官方	正常	否
14	CAMERA	访问相机	官方	危险	是
15	BLUETOOTH_ADMIN	蓝牙管理	官方	正常	否
16	REQUEST_INSTALL_PACKAGES	允许程序安装文件	官方	特殊	否
17	GET_TASKS	检索当前运行的应用程序	官方	特殊	否
18	BROADCAST_STICKY	发送置顶广播	官方	正常	否
19	READ_CONTACTS	读取联系人数据	官方	危险	是
20	USE_FINGERPRINT	允许使用指纹	官方	正常	否
21	CHANGE_NETWORK_STATE	更改网络连接性	官方	正常	否
22	CHANGE_WIFI_MULTICAST_STATE	允许接收 WLAN 多播	官方	正常	否
23	VIBRATE	控制振动器	官方	正常	否
24	FLASHLIGHT	控制闪光灯	官方	正常	否
25	SYSTEM_OVERLAY_WINDOW	自定义权限	自定义	N/A	否
26	RECORD_AUDIO	录音	官方	危险	是
27	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是
28	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否
29	CHANGE_WIFI_STATE	更改 WLAN 状态	官方	正常	否
30	USE_FACERECOGNITION	自定义权限	自定义	N/A	否
31	READ_SETTINGS	读取全局系统设置	官方	N/A	否
32	WAKE_LOCK	防止手机休眠	官方	正常	否
33	WRITE_EXTERNAL_STORAG	修改/删除 SD 卡中的内容	官方	危险	是

	E				
34	REORDER_TASKS	对正在运行的应用程序重新排序	官方	正常	否
35	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否
36	INTERNET	访问网络	官方	正常	否
37	SYSTEM_ALERT_WINDOW	显示系统级警报	官方	特殊	否
38	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是
39	EXPAND_STATUS_BAR	展开/收拢状态栏	官方	正常	否
40	FLAG_ACTIVITY_NEW_TASK	自定义权限	自定义	N/A	否
41	ACCESS_LOCATION_EXTRA_COMMANDS	访问额外的位置信息提供程序命令	官方	正常	否
42	CAMERA	访问相机	官方	危险	是
43	BLUETOOTH_ADMIN	蓝牙管理	官方	正常	否
44	REQUEST_INSTALL_PACKAGES	允许程序安装文件	官方	特殊	否
45	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是
46	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是
47	GET_TASKS	检索当前运行的应用程序	官方	特殊	否
48	BROADCAST_STICKY	发送置顶广播	官方	正常	否
49	READ_CONTACTS	读取联系人数据	官方	危险	是
50	USE_FINGERPRINT	允许使用指纹	官方	正常	否
51	BLUETOOTH	创建蓝牙连接	官方	正常	否
52	CHANGE_NETWORK_STATE	更改网络连接性	官方	正常	否
53	CHANGE_WIFI_MULTICAST_STATE	允许接收 WLAN 多播	官方	正常	否
54	VIBRATE	控制振动器	官方	正常	否
55	ACCESS_WIFI_	查看 WLAN 状	官方	正常	否

	STATE	态			
56	FLASHLIGHT	控制闪光灯	官方	正常	否
57	SYSTEM_OVERLAY_WINDOW	自定义权限	自定义	N/A	否
58	RECORD_AUDIO	录音	官方	危险	是
59	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是
60	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否
61	CHANGE_WIFI_STATE	更改 WLAN 状态	官方	正常	否
62	USE_FACERECOGNITION	自定义权限	自定义	N/A	否
63	READ_SETTINGS	读取全局系统设置	官方	N/A	否
64	WAKE_LOCK	防止手机休眠	官方	正常	否
65	WRITE_EXTERNAL_STORAGE	修改/删除 SD 卡中的内容	官方	危险	是
66	REORDER_TASKS	对正在运行的应用程序重新排序	官方	正常	否
67	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否
68	INTERNET	访问网络	官方	正常	否
69	SYSTEM_ALERT_WINDOW	显示系统级警报	官方	特殊	否
70	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是
71	EXPAND_STATUS_BAR	展开/收拢状态栏	官方	正常	否
72	FLAG_ACTIVITY_NEW_TASK	自定义权限	自定义	N/A	否
73	ACCESS_LOCATION_EXTRA_COMMANDS	访问额外的位置信息提供程序命令	官方	正常	否
74	CAMERA	访问相机	官方	危险	是
75	BLUETOOTH_ADMIN	蓝牙管理	官方	正常	否
76	REQUEST_INSTALL_PACKAGES	允许程序安装文件	官方	特殊	否
77	ACCESS_COA	访问大概位置	官方	危险	是

	RSE_LOCATIO N				
78	READ_PHONE _STATE	读取手机状态和身份	官方	危险	是
79	GET_TASKS	检索当前运行的应用程序	官方	特殊	否
80	BROADCAST_ STICKY	发送置顶广播	官方	正常	否
81	READ_CONTA CTS	读取联系人数据	官方	危险	是
82	USE_FINGERP RINT	允许使用指纹	官方	正常	否
83	BLUETOOTH	创建蓝牙连接	官方	正常	否
84	CHANGE_NET WORK_STATE	更改网络连接性	官方	正常	否
85	CHANGE_WIFI _MULTICAST_ STATE	允许接收 WLAN 多播	官方	正常	否
86	VIBRATE	控制振动器	官方	正常	否
87	ACCESS_WIFI_ STATE	查看 WLAN 状态	官方	正常	否
88	com.android.l auncher.permi ssion.INSTALL _SHORTCUT	自定义权限	自定义	正常	否
89	com.android.l auncher.permi ssion.UNINST ALL_SHORTC UT	自定义权限	自定义	正常	否
90	com.android.l auncher.permi ssion.READ_SE TTINGS	自定义权限	自定义	正常	否
91	com.android.l auncher.permi ssion.WRITE_S ETTINGS	自定义权限	自定义	正常	否
92	com.android.l auncher2.per mission.READ _SETTINGS	自定义权限	自定义	正常	否
93	com.android.l auncher2.per mission.WRIT	自定义权限	自定义	正常	否

	E_SETTINGS				
94	com.android.launcher3.permission.READ_SETTINGS	自定义权限	自定义	正常	否
95	com.android.launcher3.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
96	org.adw.launcher.permission.READ_SETTINGS	自定义权限	自定义	正常	否
97	org.adw.launcher.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
98	com.htc.launcher.permission.READ_SETTINGS	自定义权限	自定义	正常	否
99	com.htc.launcher.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
100	com.qihoo360.launcher.permission.READ_SETTINGS	自定义权限	自定义	正常	否
101	com.qihoo360.launcher.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
102	com.lge.launcher.permission.READ_SETTINGS	自定义权限	自定义	正常	否
103	com.lge.launcher.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
104	net.qihoo.launcher.permission.READ_SETTINGS	自定义权限	自定义	正常	否
105	net.qihoo.laun	自定义权限	自定义	正常	否

	cher.permission.WRITE_SETTINGS				
106	org.adwfreak.launcher.permission.READ_SETTINGS	自定义权限	自定义	正常	否
107	org.adwfreak.launcher.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
108	org.adw.launcher_donut.permission.READ_SETTINGS	自定义权限	自定义	正常	否
109	org.adw.launcher_donut.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
110	com.huawei.launcher3.permission.READ_SETTINGS	自定义权限	自定义	正常	否
111	com.huawei.launcher3.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
112	com.fede.launcher.permission.READ_SETTINGS	自定义权限	自定义	正常	否
113	com.fede.launcher.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
114	com.sec.android.app.twlauncher.settings.READ_SETTINGS	自定义权限	自定义	正常	否
115	com.sec.android.app.twlauncher.settings.WRITE_SETTINGS	自定义权限	自定义	正常	否
116	com.anddoes.l	自定义权限	自定义	正常	否

	auncher.permission.READ_SETTINGS				
117	com.anddoes.launcher.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
118	com.tencent.qqlauncher.permission.READ_SETTINGS	自定义权限	自定义	正常	否
119	com.tencent.qqlauncher.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
120	com.huawei.launcher2.permission.READ_SETTINGS	自定义权限	自定义	正常	否
121	com.huawei.launcher2.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
122	com.android.mylauncher.permission.READ_SETTINGS	自定义权限	自定义	正常	否
123	com.android.mylauncher.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
124	com.ebproductions.android.launcher.permission.READ_SETTINGS	自定义权限	自定义	正常	否
125	com.ebproductions.android.launcher.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
126	com.oppo.launcher.permission.READ_SETTINGS	自定义权限	自定义	正常	否
127	com.oppo.lau	自定义权限	自定义	正常	否

	ncher.permission.WRITE_SETTINGS				
128	com.huawei.android.launcher.permission.READ_SETTINGS	自定义权限	自定义	正常	否
129	com.huawei.android.launcher.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
130	telecom.mdesk.permission.READ_SETTINGS	自定义权限	自定义	正常	否
131	telecom.mdesk.permission.WRITE_SETTINGS	自定义权限	自定义	正常	否
132	dianxin.permission.ACCESS_LAUNCHER_DATA	自定义权限	自定义	正常	否
133	com.suning.mobile.epa.permission.MIPUSH_RECEIVE	自定义权限	自定义	正常	否
134	com.meizu.flyme.push.permission.RECEIVE	自定义权限	自定义	正常	否
135	com.suning.mobile.epa.push.permission.MESSAGE	自定义权限	自定义	正常	否
136	com.meizu.c2dm.permission.RECEIVE	自定义权限	自定义	正常	否
137	com.suning.mobile.epa.permission.C2D_MESSAGE	自定义权限	自定义	正常	否
138	com.asus.msa.SupplementaryDID.ACCESS	自定义权限	自定义	正常	否

139	cn.org.ifaa.permission.USE_IFAA_MANAGER	自定义权限	自定义	正常	否

3.3.9 高频使用敏感权限行为

该 APP 在检测期间访问敏感权限情况如下表：

序号	主体	包名	时间范围	使用敏感权限	每秒最高访问次数
1	讯飞 MSC SDK	com.iflytek.cloud	2020-12-11 10:17:19~2020-12-11 10:21:26	ACCESS_COARSE_LOCATION	1
2	友盟移动统计 SDK	com.umeng.commonsdk	2020-12-11 10:17:19~2020-12-11 10:21:26	ACCESS_COARSE_LOCATION	1
3	讯飞 MSC SDK	com.iflytek.cloud	2020-12-11 10:17:19~2020-12-11 10:21:26	ACCESS_FINE_LOCATION	2
4	友盟移动统计 SDK	com.umeng.commonsdk	2020-12-11 10:17:19~2020-12-11 10:21:26	ACCESS_FINE_LOCATION	2
5	讯飞 MSC SDK	com.iflytek.cloud	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_EXTERNAL_STORAGE	4
6	Vlayout	com.suning.mobile	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_EXTERNAL_STORAGE	2
7	PhotoView	com.suning.mmds	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_EXTERNAL_STORAGE	2
8	PhotoView	com.suning.fpcore	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_EXTERNAL_STORAGE	2
9	百度云推送	com.baidu.sec	2020-12-11	READ_EXTERN	1

	SDK	urity	10:17:19~2020-12-11 10:21:26	AL_STORAGE	
10	百度云推送 SDK	com.baidu.security	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_PHONE_STATE	18
11	PhotoView	com.suning.fpcore	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_PHONE_STATE	2
12	讯飞 MSC SDK	com.iflytek.cloud	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_PHONE_STATE	2
13	App	e.g.a	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_PHONE_STATE	1
14	PhotoView	com.suning.sastatistics	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_PHONE_STATE	1
15	淘宝通道服务 SDK	com.taobao.accs	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_PHONE_STATE	1
16	友盟 消息推送 SDK	com.umeng.message	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_PHONE_STATE	1
17	友盟移动统计 SDK	com.umeng.commonsdk	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_PHONE_STATE	1
18	App	f.b.a	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_PHONE_STATE	1
19	App	ct0000.ct0001.ct0000	2020-12-11 10:17:19~2020-12-11 10:21:26	READ_PHONE_STATE	1

3.3.10 声明/使用不建议申请权限情况

根据《网络安全标准实践指南—移动互联网应用程序（App）系统权限申请使用指引》附录 C 要求，该 App 声明、使用“不建议申请权限”情况如下：

序号	声明权限但未使用	权限含义	类型	保护级别	声明后使用
1	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是
2	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是
3	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是
4	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是
5	RECORD_AUDIO	录音	官方	危险	否
6	WRITE_EXTERNAL_STORAGE	修改/删除 SD 卡中的内容	官方	危险	否
7	CAMERA	访问相机	官方	危险	否
8	READ_CONTACTS	读取联系人数据	官方	危险	否
9	RECORD_AUDIO	录音	官方	危险	否
10	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	否
11	WRITE_EXTERNAL_STORAGE	修改/删除 SD 卡中的内容	官方	危险	否
12	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	否
13	CAMERA	访问相机	官方	危险	否
14	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	否
15	READ_PHONE_STATE	读取手机状态和身份	官方	危险	否
16	READ_CONTACTS	读取联系人数据	官方	危险	否
17	RECORD_AUDIO	录音	官方	危险	否

18	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	否
19	WRITE_EXTERNAL_STORAGE	修改/删除 SD 卡中的内容	官方	危险	否
20	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	否
21	CAMERA	访问相机	官方	危险	否
22	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	否
23	READ_PHONE_STATE	读取手机状态和身份	官方	危险	否
24	READ_CONTACTS	读取联系人数据	官方	危险	否

3.3.11 声明/使用非最小必要权限情况

根据《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范》附录 B 要求，该 App 声明、使用非“最小必要权限”情况如下：

序号	声明权限但未使用	权限含义	类型	保护级别	声明后使用
1	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是
2	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是
3	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是
4	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是
5	RECORD_AUDIO	录音	官方	危险	否
6	WRITE_EXTERNAL_STORAGE	修改/删除 SD 卡中的内容	官方	危险	否
7	CAMERA	访问相机	官方	危险	否
8	READ_CONTACTS	读取联系人数据	官方	危险	否
9	RECORD_AUDIO	录音	官方	危险	否
10	ACCESS_FINE_	访问精确位置	官方	危险	否

	LOCATION				
11	WRITE_EXTERNAL_STORAGE	修改/删除 SD 卡中的内容	官方	危险	否
12	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	否
13	CAMERA	访问相机	官方	危险	否
14	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	否
15	READ_PHONE_STATE	读取手机状态和身份	官方	危险	否
16	READ_CONTACTS	读取联系人数据	官方	危险	否
17	RECORD_AUDIO	录音	官方	危险	否
18	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	否
19	WRITE_EXTERNAL_STORAGE	修改/删除 SD 卡中的内容	官方	危险	否
20	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	否
21	CAMERA	访问相机	官方	危险	否
22	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	否
23	READ_PHONE_STATE	读取手机状态和身份	官方	危险	否
24	READ_CONTACTS	读取联系人数据	官方	危险	否

3.3.12 疑似过度声明权限情况

该 APP 申请权限 84 个，实际使用权限 9 个，超出比例为 89.29%。我们认为该 APP 存在过度申请授权的情况。

3.3.13 读取设备信息行为

该 App 在检测期间读取设备信息共 70 次，具体情况如下：

序号	SDK 名称	包名	类别	使用次数
1	淘宝通道服务 SDK	com.taobao.accs	IMSI	3

2	App	e.g.a	IMEI	3
	PhotoView	com.suning.sastatistics	IMEI	3
	友盟移动统计 SDK	com.umeng.commonsdk	IMEI	2
			Wi-Fi MAC	3
	PhotoView	com.suning.fpcore	IMSI	2
			IMEI	2
	讯飞 MSC SDK	com.iflytek.cloud	IMEI	2
			Wi-Fi MAC	5
			IMSI	2
	百度云推送 SDK	com.baidu.security	IMSI	9
			IMEI	32
3	友盟 消息推送 SDK	com.umeng.message	IMEI	2

3.3.14 读取应用列表

该 App 在检测期间读取应用列表共 4 次，其中涉及 2 个 SDK，具体情况如下：

序号	主体	包名	时间	次数
1	App	com.ijm.security	1970-01-01 08:00:00	1 次
2	百度云推送 SDK	com.baidu.security	1970-01-01 08:00:00、1970-01-01 08:00:00、1970-01-01 08:00:00	3 次

3.3.15 未经同意使用可收集个人信息权限

共有 0 个未同意使用可收集个人信息权限,具体情况如下：

序号	权限项	权限含义	类型	保护级别	敏感	次数

3.3.16 自启动

该 App 的自启情况如下:

是否自启	否

3.3.17 一揽子授权情况检查

该 App 的 targetSDKVersion 值为 26，不存在一揽子授权行为，推荐设置 targetSDKVersion 值不低于 28。

3.4 事件分析

在 APP 检查期间共发生 6 次事件记录

3.4.1

序号	1
截屏时间	1970-01-01 08:26:47
运行阶段	前台运行
备注	调用敏感权限，自动截图

序号	域名	IP	IP 归属地	协议	次数
1	click.suning.cn	118.112.11.143	中国 四川省 成都市	https	82
2	apm.suning.cn	101.125.252.192	中国 江苏省 南京市	https	22
3	msc.baidu.com	220.181.107.218	中国 北京 北京市	https	28
4	adash.man.aliyuncs.com	106.11.248.37	中国 上海 上海市	http	5
5	mmds.suning.com	183.134.25.30	中国 浙江省 台州市	https	2
6	dt.netease.im	59.111.160.235	中国 浙江省 杭州市	https	6
7	scs.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	3
8	106.11.61.137	106.11.61.137	中国 上海 上海市	http	2
9	data.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	1
10	mfg.suning.com	183.134.25.31	中国 浙江省 台州市	https	5
11	dfp.suning.com	183.134.25.31	中国 浙江省 台州市	https	2

12	fastcfg.suning.com	222.190.116.13	中国 江苏省 南京市	http	1
13	oss.suning.com	183.134.25.32	中国 浙江省 台州市	https	1

序号	权限项	权限含义	类型	保护级别	敏感	次数
1	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
2	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
3	INTERNET	访问网络	官方	正常	否	24
4	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	10
5	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
6	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	48
7	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
8	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	99
9	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
10	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
11	INTERNET	访问网络	官方	正常	否	24
12	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	10
13	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
14	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	48
15	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
16	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	99

17	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
18	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
19	INTERNET	访问网络	官方	正常	否	24
20	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	10
21	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
22	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	48
23	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
24	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	99

3.4.2

序号	2
截屏时间	1970-01-01 08:26:47
运行阶段	后台运行
备注	调用敏感权限，自动截图

序号	域名	IP	IP 归属地	协议	次数
1	click.suning.cn	118.112.11.143	中国 四川省 成都市	https	84
2	apm.suning.cn	101.125.252.192	中国 江苏省 南京市	https	22
3	msc.baidu.com	220.181.107.218	中国 北京 北京市	https	28
4	adash.man.aliyuncs.com	106.11.248.37	中国 上海 上海市	http	5
5	mmds.suning.com	183.134.25.30	中国 浙江省 台州市	https	2
6	dt.netease.im	59.111.160.235	中国 浙江省 杭州市	https	6

7	scs.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	3
8	106.11.61.137	106.11.61.137	中国 上海 上海市	http	2
9	data.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	1
10	mfg.suning.com	183.134.25.31	中国 浙江省 台州市	https	5
11	dfp.suning.com	183.134.25.31	中国 浙江省 台州市	https	5
12	fastcfg.suning.com	222.190.116.13	中国 江苏省 南京市	http	1
13	oss.suning.com	183.134.25.32	中国 浙江省 台州市	https	1

序号	权限项	权限含义	类型	保护级别	敏感	次数
1	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
2	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
3	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
4	INTERNET	访问网络	官方	正常	否	24
5	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	14
6	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
7	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	50
8	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
9	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	104
10	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
11	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10

12	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
13	INTERNET	访问网络	官方	正常	否	24
14	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	14
15	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
16	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	50
17	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
18	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	104
19	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
20	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
21	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
22	INTERNET	访问网络	官方	正常	否	24
23	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	14
24	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
25	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	50
26	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
27	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	104

3.4.3

序号	3
截屏时间	1970-01-01 08:26:47
运行阶段	后台运行

备注	调用敏感权限，自动截图

序号	域名	IP	IP 归属地	协议	次数
1	click.suning.cn	118.112.11.143	中国 四川省 成都市	https	88
2	apm.suning.cn	101.125.252.192	中国 江苏省 南京市	https	22
3	msc.baidu.com	220.181.107.218	中国 北京 北京市	https	28
4	adash.man.aliyuncs.com	106.11.248.37	中国 上海 上海市	http	5
5	mmds.suning.com	183.134.25.30	中国 浙江省 台州市	https	5
6	dt.netease.im	59.111.160.235	中国 浙江省 杭州市	https	9
7	scs.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	3
8	106.11.61.137	106.11.61.137	中国 上海 上海市	http	2
9	data.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	1
10	mfg.suning.com	183.134.25.31	中国 浙江省 台州市	https	5
11	dfp.suning.com	183.134.25.31	中国 浙江省 台州市	https	5
12	fastcfg.suning.com	222.190.116.13	中国 江苏省 南京市	http	1
13	oss.suning.com	183.134.25.32	中国 浙江省 台州市	https	1

序号	权限项	权限含义	类型	保护级别	敏感	次数
1	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
2	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
3	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2

4	INTERNET	访问网络	官方	正常	否	27
5	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	20
6	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
7	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	54
8	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
9	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	108
10	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
11	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
12	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
13	INTERNET	访问网络	官方	正常	否	27
14	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	20
15	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
16	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	54
17	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
18	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	108
19	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
20	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
21	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
22	INTERNET	访问网络	官方	正常	否	27

23	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	20
24	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
25	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	54
26	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
27	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	108

3.4.4

序号	4
截屏时间	1970-01-01 08:26:47
运行阶段	后台运行
备注	调用敏感权限，自动截图

序号	域名	IP	IP 归属地	协议	次数
1	click.suning.cn	118.112.11.143	中国 四川省 成都市	https	88
2	apm.suning.cn	101.125.252.192	中国 江苏省 南京市	https	22
3	msc.baidu.com	220.181.107.218	中国 北京 北京市	https	28
4	adash.man.aliyuncs.com	106.11.248.37	中国 上海 上海市	http	5
5	mmds.suning.com	183.134.25.30	中国 浙江省 台州市	https	5
6	dt.netease.im	59.111.160.235	中国 浙江省 杭州市	https	8
7	scs.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	3
8	106.11.61.137	106.11.61.137	中国 上海 上海市	http	2
9	data.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	1
10	mfg.suning.co	183.134.25.31	中国 浙江省 台	https	5

	m		州市		
11	dfp.suning.com	183.134.25.31	中国 浙江省 台州市	https	5
12	fastcfg.suning.com	222.190.116.13	中国 江苏省 南京市	http	1
13	oss.suning.com	183.134.25.32	中国 浙江省 台州市	https	1

序号	权限项	权限含义	类型	保护级别	敏感	次数
1	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
2	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
3	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
4	INTERNET	访问网络	官方	正常	否	27
5	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	20
6	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
7	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	52
8	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
9	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	108
10	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
11	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
12	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
13	INTERNET	访问网络	官方	正常	否	27
14	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	20

15	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
16	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	52
17	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
18	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	108
19	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
20	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
21	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
22	INTERNET	访问网络	官方	正常	否	27
23	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	20
24	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
25	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	52
26	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
27	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	108

3.4.5

序号	5
截屏时间	1970-01-01 08:26:47
运行阶段	后台运行
备注	调用敏感权限，自动截图

序号	域名	IP	IP 归属地	协议	次数

1	click.suning.cn	118.112.11.143	中国 四川省 成都市	https	88
2	apm.suning.cn	101.125.252.192	中国 江苏省 南京市	https	22
3	msc.baidu.com	220.181.107.218	中国 北京 北京市	https	28
4	adash.man.aliyuncs.com	106.11.248.37	中国 上海 上海市	http	5
5	mmds.suning.com	183.134.25.30	中国 浙江省 台州市	https	5
6	dt.netease.im	59.111.160.235	中国 浙江省 杭州市	https	6
7	scs.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	3
8	106.11.61.137	106.11.61.137	中国 上海 上海市	http	2
9	data.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	1
10	mfg.suning.com	183.134.25.31	中国 浙江省 台州市	https	5
11	dfp.suning.com	183.134.25.31	中国 浙江省 台州市	https	5
12	fastcfg.suning.com	222.190.116.13	中国 江苏省 南京市	http	1
13	oss.suning.com	183.134.25.32	中国 浙江省 台州市	https	1

序号	权限项	权限含义	类型	保护级别	敏感	次数
1	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
2	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
3	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
4	INTERNET	访问网络	官方	正常	否	26
5	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	18
6	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1

7	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	50
8	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
9	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	108
10	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
11	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
12	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
13	INTERNET	访问网络	官方	正常	否	26
14	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	18
15	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
16	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	50
17	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
18	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	108
19	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
20	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
21	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
22	INTERNET	访问网络	官方	正常	否	26
23	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	18
24	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
25	READ_PHO	读取手机状	官方	危险	是	50

	NE_STATE	态和身份				
26	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
27	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	108

3.4.6

序号	6
截屏时间	1970-01-01 08:26:47
运行阶段	后台运行
备注	调用敏感权限，自动截图

序号	域名	IP	IP 归属地	协议	次数
1	click.suning.cn	118.112.11.143	中国 四川省 成都市	https	88
2	apm.suning.cn	101.125.252.192	中国 江苏省 南京市	https	22
3	msc.baidu.com	220.181.107.218	中国 北京 北京市	https	28
4	adash.man.aliyuncs.com	106.11.248.37	中国 上海 上海市	http	5
5	mmds.suning.com	183.134.25.30	中国 浙江省 台州市	https	5
6	dt.netease.im	59.111.160.235	中国 浙江省 杭州市	https	8
7	scs.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	3
8	106.11.61.137	106.11.61.137	中国 上海 上海市	http	2
9	data.openspeech.cn	220.248.230.134	中国 安徽省 合肥市	http	1
10	mfg.suning.com	183.134.25.31	中国 浙江省 台州市	https	5
11	dfp.suning.com	183.134.25.31	中国 浙江省 台州市	https	5
12	fastcfg.suning.com	222.190.116.13	中国 江苏省 南京市	http	1
13	oss.suning.com	183.134.25.32	中国 浙江省 台州市	https	1

序号	权限项	权限含义	类型	保护级别	敏感	次数
1	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
2	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
3	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
4	INTERNET	访问网络	官方	正常	否	26
5	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	18
6	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
7	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	51
8	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
9	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	108
10	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
11	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
12	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
13	INTERNET	访问网络	官方	正常	否	26
14	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	18
15	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
16	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	51
17	BLUETOOTH	创建蓝牙连接	官方	正常	否	4

18	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	108
19	ACCESS_FINE_LOCATION	访问精确位置	官方	危险	是	2
20	ACCESS_NETWORK_STATE	查看网络状态	官方	正常	否	10
21	MODIFY_AUDIO_SETTINGS	更改您的音频设置	官方	正常	否	2
22	INTERNET	访问网络	官方	正常	否	26
23	READ_EXTERNAL_STORAGE	读取 SD 卡上的内容	官方	危险	是	18
24	ACCESS_COARSE_LOCATION	访问大概位置	官方	危险	是	1
25	READ_PHONE_STATE	读取手机状态和身份	官方	危险	是	51
26	BLUETOOTH	创建蓝牙连接	官方	正常	否	4
27	ACCESS_WIFI_STATE	查看 WLAN 状态	官方	正常	否	108

3.5 合规检查

3.5.1 私自共享给第三方

检查目的	“私自共享给第三方”。即 APP 未经用户同意与其他应用共享、使用用户个人信息，如设备识别信息、商品浏览记录、搜索使用习惯、常用软件应用列表等。
检查结论	发现问题
检查结果	不安全

3.5.2 频繁申请权限

检查目的	“频繁申请权限”。即 APP 在用户明确拒绝权限申请后，频繁申请开启通讯录、定位、短信、录音、相机等与当前服务场景无关的权限，骚扰用户。
检查结论	发现问题
检查结果	不安全

3.5.3 私自收集个人信息

检查目的	“私自收集个人信息”。即 APP 未明确告知收集使用个人信息的目的、方式和范围并获得用户同意前，收集用户个人信息。
检查结论	发现问题
检查结果	不安全

3.5.4 超范围收集个人信息

检查目的	“超范围收集个人信息”。即 APP 收集个人信息，非服务所必需或无合理应用场景，超范围或超频次收集个人信息，如通讯录、位置、身份证、人脸等。
检查结论	未发现问题
检查结果	安全

3.5.5 不给权限不让用

检查目的	“不给权限不让用”。即 APP 安装和运行时，向用户索取与当前服务场景无关的权限，用户拒绝授权后，应用退出或关闭。
检查结论	未发现问题
检查结果	安全