南明离火
移动应用检测平台

ANDROID 静态分析报告

短信转发器 • v3.3.0

分析日期: 2025-04-03 15:39:06

应用概览

文件名称:	SmsF_3.3.0_100051_universal_20240827_release.apk
文件大小:	16.96MB
应用名称:	短信转发器
软件包名:	com.idormy.sms.forwarder
主活动:	com.idormy.sms.forwarder.activity.SplashActivity
版本号:	3.3.0
最小SDK:	19
目标SDK:	33
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	43/100 (中风险)
跟踪器检测:	1/432
杀软检测:	17 个杀毒软件报毒
MD5:	47689d0f35e6d77ea41e953649c4f9da
SHA1:	fb8656cf5ea8d70f09a4d8db8abecf5fb7472a4b
SHA256:	a2f3be3c082cc2fa9e03d01c92f3b6b74365f9adcf450da1bc4fb6d8b0f65f8f

分析结果严重性分布

高危	中危	信息	安全	关注
7	33	2	1	10

四大组件导出状态统计

Activity组件：16个，其中export的有： 8个
Service组件：14个，其中export的有： 3个
Receiver组件：6个，其中export的有： 8个
Provider组件：6个，其中export的有： 0个

应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: CN=cc, OU=cc, O=cc, L=cc, ST=cc, C=91
签名算法: rsassa_pkcs1v15
有效期自: 2024-03-21 11:17:54+00:00
有效期至: 2049-03-15 11:17:54+00:00
发行人: CN=cc, OU=cc, O=cc, L=cc, ST=cc, C=91
序列号: 0x1
哈希算法: sha256
证书MD5: 40574cef6ea6ac5c59f42a535a7f37be
证书SHA1: 7e42b88c344533fa5bd1cc5ec3a908b343a3053a
证书SHA256: bb559c846f373763b4863da71a6b27e15a6cc3854316ca98efd58efebe06466d
证书SHA512:
5e94398edca6e4dbccf2fe322e4f480c3c3159ad2d72eb6894ea4a9b23061d27130b9a23de4cf7d3e549fe7a96ec31194[illegible]e550056d065a89c04ccfd97d999e

公钥算法: rsa
密钥长度: 2048
指纹: 3f7e18834108f571db32327fa8e9d10d6347321cd679b550fc7075a83e6fa9eb
找到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
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_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_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
android.permission.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.ACCESS_WIFI_STATE	普通	查看Wi-Fi状态	允许应用程序查看有关Wi-Fi状态的信息。
android.permission.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
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_PRIVILEGED_PHONE_STATE	签名(系统)	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.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.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.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
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.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.RECEIVE_SMS	危险	接收短信	允许应用程序接收短信。 恶意程序会在用户未知的情况下监视或删除。
android.permission.RECEIVE_MMS	危险	接收彩信	允许应用程序接收和处理彩信。恶意应用程序可借此监视您的信息，或者将信息删除而不向您显示。
android.permission.RECEIVE_WAP_PUSH	危险	接收WAP	允许应用程序接收和处理 WAP 信息。恶意应用程序可借此监视您的信息，或者将信息删除而不向您显示。
android.permission.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送短信。恶意应用程序可能会不经您的确认就发送信息，给您带来费用。
android.permission.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不允许拨打紧急电话。
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.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集，但对即时应用程序公开。
android.permission.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.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.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.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.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.BATTERY_STATS	普通	修改电池统计	允许对手机电池统计信息进行修改
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.CANCEL_NOTIFICATIONS	未知	未知权限	来自 android 引用的未知权限。
android.permission.BIND_NOTIFICATION_LISTENER_SERVICE	签名	NotificationListenerServices 需要用于系统绑定	必须是NotificationListenerService, 以确保只有系统可以绑定到。

android.permission.ACTION_NOTIFICATION_LISTENER_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
android.permission.INSTALL_PACKAGES	签名(系统)	请求安装APP	允许应用程序安装全新的或更新的 Android 包。恶意应用程序可能会借此添加其具有任意权限的新应用程序。
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.KILL_BACKGROUND_PROCESSES	普通	结束进程	允许应用程序结束其他应用程序的后台进程。
android.permission.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
android.permission.REBOOT	签名(系统)	强行重新启动手机	允许应用程序强行重新启动手机。
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私密信息。
android.permission.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
com.idormy.sms.forwarder.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序装载和卸载可移动存储器的文件系统。
android.permission.BLUETOOTH_ADMIN	危险	管理蓝牙	允许程序发现和配对新的蓝牙设备。
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.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.READ_CALENDAR	危险	读取日历活动	允许应用程序读取您手机上存储的所有日历活动。恶意应用程序可借此将您的日历活动发送给其他人。
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.MODIFY_PHONE_STATE	签名(系统)	修改手机状态	允许应用程序控制设备的电话功能。拥有此权限的应用程序可自行切换网络、打开和关闭无线通信等，而不会通知您。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
android.permission.EXPAND_STATUS_BAR	普通	展开/收拢状态栏	允许应用程序展开或折叠状态条。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.idormy.sms.forwarder.core.webview.AgentWebActivity	Schemes: http://, https://, about://, javascript://, inline://, Mime Types: text/html, text/plain, application/xhtml+xml, application/vnd.wap.xhtml+xml,

网络通信安全风险分析

高危: **1** | 警告: **0** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。

证书安全合规分析

高危: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名

Manifest 配置安全分析

高危: **3** | 警告: **23** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	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。
2	应用程序支持直接启动 [android:directBootAware=true]	信息	这个应用程序可以在用户解锁设备之前运行。如果你使用的是Application的自定义子类，并且你的应用程序中的任何组件都支持直接启动，那么你的整个自定义应用程序都被认为是支持直接启动的。在直接启动期间，你的应用程序只能访问存储在设备受保护存储中的数据。
3	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/network_security_config]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
4	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。
5	Activity设置了TaskAffinity属性 (com.idormy.sms.forwarder.activity.SplashActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
6	Activity (com.idormy.sms.forwarder.activity.MainActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

7	Activity (com.idormy.sms.forwarder.activity.ClientActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
8	Activity (com.idormy.sms.forwarder.activity.ClientActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
9	Activity (com.idormy.sms.forwarder.activity.TaskActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
10	Activity (com.idormy.sms.forwarder.activity.TaskActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
11	Activity (com.idormy.sms.forwarder.core.webview.AgentWebActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
12	Activity (com.idormy.sms.forwarder.core.BaseActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
13	Activity (com.idormy.sms.forwarder.utils.update.UpdateTipDialog) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
14	Activity (com.idormy.sms.forwarder.core.webview.WebViewInterceptDialog) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
15	Activity (com.idormy.sms.forwarder.core.XPageTransferActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
16	Broadcast Receiver (com.idormy.sms.forwarder.receiver.BatteryReceiver) 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。
17	Broadcast Receiver (com.idormy.sms.forwarder.receiver.BootCompletedReceiver) 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。
18	Broadcast Receiver (com.idormy.sms.forwarder.receiver.CallReceiver) 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。

本报告由南明离火移动安全分析平台生成

19	Broadcast Receiver (com.idormy.sms.forwarder.receiver.LockScreenReceiver) 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。
20	Broadcast Receiver (com.idormy.sms.forwarder.receiver.NetworkChangeReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.READ_PHONE_STATE [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。
21	Broadcast Receiver (com.idormy.sms.forwarder.receiver.SimStateReceiver) 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。
22	Broadcast Receiver (com.idormy.sms.forwarder.receiver.SmsReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BROADCAST_SMS [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。
23	Activity (com.gyf.cactus.pix.OnePixActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为"singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
24	Service (com.gyf.cactus.service.LocalService) 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。
25	Service (com.gyf.cactus.service.RemoteService) 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。
26	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
27	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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。

28	高优先级的Intent（2147483647） - {3} 个命中 [android:priority]	警告	通过设置一个比另一个Intent更高的优先级，应用程序有效地覆盖了其他请求。

代码安全漏洞检测

高危: **3** | 警告: **8** | 信息: **2** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	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
2	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
3	MD5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
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	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
6	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
7	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
8	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限

9	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
10	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
11	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
12	使用弱加密算法	高危	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
13	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
14	已启用远程WebView调试	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限

应用行为分析

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
00031	检查当前正在运行的应用程序列表	反射 信息收集	升级会员：解锁高级权限
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

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
00047	查询本地IP地址	网络 信息收集	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
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	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
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	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
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00058	连接到特定的WIFI网络	WiFi 控制	升级会员：解锁高级权限
00023	从当前应用程序启动另一个应用程序	反射 控制	升级会员：解锁高级权限
00079	隐藏当前应用程序的图标	规避	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
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	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
00028	从assets目录中读取文件	文件	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
00193	发送短信	短信	升级会员：解锁高级权限
00040	发送短信	短信	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	22/30	android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.RECEIVE_BOOT_COMPLETED android.permission.RECEIVE_SMS android.permission.RECEIVE_MMS android.permission.READ_SMS android.permission.SEND_SMS android.permission.CALL_PHONE android.permission.READ_PHONE_STATE android.permission.READ_CALL_LOG android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.GET_ACCOUNTS android.permission.WRITE_SETTINGS android.permission.GET_TASKS android.permission.WAKE_LOCK android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES android.permission.VIBRATE android.permission.READ_CALENDAR android.permission.RECORD_AUDIO android.permission.CAMERA
其它常用权限	15/46	android.permission.ACCESS_BACKGROUND_LOCATION android.permission.CHANGE_WIFI_STATE android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_NETWORK_STATE android.permission.INTERNET android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.BATTERY_STATS com.google.android.gms.permission.AD_ID android.permission.BLUETOOTH_ADMIN android.permission.BLUETOOTH android.permission.FLASHLIGHT

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
xupdate.ppps.cn	安全	是	**IP地址:** 47.98.123.17 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
publish.twitter.com	安全	否	**IP地址:** 162.159.140.229 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
api.ipify.org	安全	否	**IP地址:** 104.26.13.205 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
oapi.dingtalk.com	安全	是	**IP地址:** 117.69.71.61 **国家:** 中国 **地区:** 湖南 **城市:** 长沙 **纬度:** 28.200001 **经度:** 112.966667 **查看:** 高德地图
smsf.demo.com	安全	否	No Geolocation information available.
push.ppps.cn	安全	是	**IP地址:** 47.98.123.17 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
cdnjs.cloudflare.com	安全	否	**IP地址:** 104.17.25.14 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

sctapi.ftqq.com	安全	是	**IP地址:** 121.228.130.156 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
open.feishu.cn	安全	是	**IP地址:** 117.69.71.61 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
api.dingtalk.com	安全	是	**IP地址:** 117.69.71.61 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
api6.ipify.org	安全	否	No Geolocation information available.
api.telegram.org	安全	否	**IP地址:** 149.154.167.220 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图
twitter.com	安全	否	**IP地址:** 162.159.140.229 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
platform.twitter.com	安全	否	**IP地址:** 104.26.13.205 **国家:** 瑞典 **地区:** 西约塔兰省 **城市:** 哥德堡 **纬度:** 57.707409 **经度:** 11.966732 **查看:** Google 地图
a.b.com	安全	否	No Geolocation information available.
www.coolapk.com	安全	是	**IP地址:** 117.69.71.61 **国家:** 中国 **地区:** 安徽 **城市:** 苏州 **纬度:** 33.636440 **经度:** 116.978851 **查看:** 高德地图

gitee.com	安全	是	**IP地址:** 121.40.246.120 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
www.pushplus.plus	安全	是	**IP地址:** 47.98.123.17 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161582 **查看:** 高德地图
api.day.app	安全	是	**IP地址:** 43.155.109.24 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://t.me/ • https://gitee.com/pp/SmsForwarder/wikis/pages • https://gitee.com/pp/SmsForwarder/wikis/pages?sort_id=4912151&doc_id=1821427 • https://gitee.com/pp/SmsForwarder/wikis/pages?sort_id=4877445&doc_id=1821427 • https://qun.qq.com/qqweb/qunpro/share?_wv=3&_wwv=128&appChannel=share&inviteCode=1W5aewP&appChannel=share&businessType=9&from=246610&biz=ka	自研引擎-A
• https://api.telegram.org/bot	com/idormy/sms/forwarder/utils/sender/TelegramUtils.java
• https://gitee.com/	com/idormy/sms/forwarder/utils/sdkinit/XBasicLibInit.java
• https://github.com/xuexiangjys/	com/idormy/sms/forwarder/core/webview/AgentWebFragment.java
• https://twitter.com/%s • https://publish.twitter.com/oembed?url=https://twitter.com/twitter/status/%s&hide_media=true • https://publish.twitter.com/oembed?url=https://twitter.com/twitter/status/%s • https://platform.twitter.com/widgets.js	br/tiagohm/markdownview/ext/twitter/internal/TwitterNodeRenderer.java
• https://qyapi.weixin.qq.com	com/idormy/sms/forwarder/utils/sender/WeworkAgentUtils.java
• https://sctapi.ftqq.com/%s.send	com/idormy/sms/forwarder/utils/sender/ServerchanUtils.java
• https://xupdate.ppps.cn/update/checkversion	com/idormy/sms/forwarder/utils/sdkinit/XUpdateInit.java
• www.pushplus.plus	com/idormy/sms/forwarder/entity/setting/PushplusSetting.java

本报告由南明离火移动安全分析平台生成

• 88.88.88.88 • http://smsf.demo.com • http://88.88.88.88:5000 • 127.0.0.1	com/idormy/sms/forwarder/database/AppDatabase$Companion$buildDatabase$builder$1.java
• http://127.0.0.1:5000	com/idormy/sms/forwarder/utils/HttpServerUtils.java
• https://github.com/xuexiangjys	com/idormy/sms/forwarder/core/webview/XPageWebViewFragment.java
• https://open.feishu.cn/open-apis/im/v1/messages?receive_id_type= • https://github.com/pppscn/smsforwarder • https://open.feishu.cn/open-apis/auth/v3/tenant_access_token/internal	com/idormy/sms/forwarder/utils/sender/FeishuAppUtils.java
• https://github.com/pppscn/smsforwarder	com/idormy/sms/forwarder/utils/sender/FeishuUtils.java
• https://api.dingtalk.com/v1.0/oauth2/accesstoken • https://api.dingtalk.com/v1.0/robot/otomessages/batchsend	com/idormy/sms/forwarder/utils/sender/DingtalkInnerRobotUtils.java
• https://oapi.dingtalk.com/robot/send?access_token=	com/idormy/sms/forwarder/utils/sender/DingtalkGroupRobotUtils.java
• 88.88.88.88 • http://smsf.demo.com • http://88.88.88.88:5000 • 127.0.0.1	com/idormy/sms/forwarder/database/AppDatabase$Companion$MIGRATION_9_10$1.java
• https://api.ipify.org/ • https://api6.ipify.org/	com/idormy/sms/forwarder/workers/NetworkWorker.java
• https://cdnjs.cloudflare.com/ajax/libs/mathjax/2.7.2/MathJax.js?config=tex-mml-am_chtml	br/tiagohm/markdownview/MarkdownView.java
• 127.0.0.1	com/idormy/sms/forwarder/fragment/ServerFragment.java
• https://gitee.com/pp/smsforwarder/raw/main/privacy	com/idormy/sms/forwarder/utils/CommonUtils.java
• 255.255.255.255	com/idormy/sms/forwarder/server/controller/WolController.java
• https://www.coolapk.com/apk/com.idormy.sms.forwarder	com/idormy/sms/forwarder/utils/update/UpdateTipDialog.java
• 223.5.5.5	com/xuexiang/xutil/net/NetworkUtils.java
• https://qyapi.weixin.qq.com	com/idormy/sms/forwarder/entity/setting/WeworkAgentSetting.java

• https://gitee.com/pp/smsforwarder • https://gitee.com/pp/smsforwarder/wikis/pages • https://smsf.demo.com • 192.168.1.255 • https://push.ppps.cn/message?token= • https://qyapi.weixin.qq.com/cgixx?key=xxx • https://gitee.com/pp/smsforwarder/raw/main/pic/wechat_miniprogram.jpg • https://api.day.app/xxxxxxxx/ • www.pushplus.plus • https://a.b.com/msg?token=xyz • https://github.com/pppscn/smsforwarder • https://oapi.dingtalk.com/robot/send?access_token=xxx • 192.168.168.168 • http://127.0.0.1:5000 • https://gitee.com/pp/smsforwarder.wiki/raw/master/%e6%89%93%e8%b5%8f%e5%90%8d%e5%8d%95.md	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
Conscrypt	Google	Conscrypt 是一个 Java 安全提供程序 (JSP)。它实现了部分 Java 加密扩展 (JCE) 和 Java 安全套接字扩展 (JSSE)。 它使用 BoringSSL 为 Android 和 OpenJDK 上的 Java 应用程序提供加密原语和传输层安全性 (TLS)。 有关所提供内容的详细信息，请参阅功能文档。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
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。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
AndroidAutoSize	JessYanCoding	今日头条屏幕适配方案终极版，一个极低成本的 Android 屏幕适配方案。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
Jetpack Room	Google	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。

邮箱地址敏感信息提取

EMAIL	源码文件
aaa@bbb.ccc	自研引擎-S

第三方追踪器检测

名称	类别	网址
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

敏感凭证泄露检测

可能的密钥
"App_Secret" : "Secret"
"appkey" : "AppKey"
"appsecret" : "AppSecret"
"dingtalk_token" : "Webhook"
"header_key" : "Key"
"pushplus_webhook" : "webhook"
"regex_password" : "^(?:(?=.*[a-zA-Z])(?=.*[0-9])).{8,18}$"
"server_chan_send_key" : "SendKey"
"webhook" : "Webhook"
"App_Secret" : "Secret"
"appkey" : "AppKey"
"appsecret" : "AppSecret"
"dingtalk_token" : "Webhook"
"header_key" : "Key"
"pushplus_webhook" : "webhook"
"regex_password" : "^(?:(?=.*[a-zA-Z])(?=.*[0-9])).{8,18}$"
"server_chan_send_key" : "SendKey"
"webhook" : "Webhook"
"App_Secret" : "Secret"
"appkey" : "AppKey"
"appsecret" : "AppSecret"
"dingtalk_token" : "Webhook"
"header_key" : "Key"
"pushplus_webhook" : "webhook"
"regex_password" : "^(?:(?=.*[a-zA-Z])(?=.*[0-9])).{8,18}$"

"server_chan_send_key" : "SendKey"
"webhook" : "Webhook"
"App_Secret" : "Secret"
"api_location" : "Location"
"appkey" : "AppKey"
"appsecret" : "AppSecret"
"bark_encryption_key_regex" : "^[a-zA-Z0-9]{16}"
"copy_public_key" : "Copy"
"dingtalk_secret" : "Secret"
"dingtalk_token" : "Webhook"
"feishu_webhook" : "Webhook"
"generate_key" : "Generate"
"header_key" : "Key"
"password" : "Password"
"pushplus_token" : "Token"
"regex_password" : "^(?:(?=.*[a-zA-Z])(?=.*[0-9])).{8,18}$"
"server_chan_send_key" : "SendKey"
"username" : "Username"
"webhook" : "Webhook"
"webhook_params" : "Params"
"wework_webHook" : "WebHook"
2a21a1eb02fe950993991fb671c3416a
AAEGDgolrP2h2kXbSIrtO5rsTKRLfTdYb
60254fc7425ec2bf10f4293e
44d9c5ff34ab39f0193ef92bf4835f95

免责声明及风险提示: