南明离火
移动应用检测平台

ANDROID 静态分析报告

LPD CHECK • v5.01.23

分析日期: 2025-03-11 10:01:56

应用概览

文件名称:	57d3a79ba52cafd0ba7f6dbc05e9e1588b3f6aca51c508e04c802acd0869bf04.apk
文件大小:	11.05MB
应用名称:	LPD CHECK
软件包名:	com.frzinapps.smsforward
主活动:	com.frzinapps.smsforward.MainActivity
版本号:	5.01.23
最小SDK:	21
目标SDK:	31
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	46/100 (中风险)
跟踪器检测:	5/432
杀软检测:	12 个杀毒软件报毒
MD5:	76a79ffefcae95dccae41143e82ac735
SHA1:	8379492ffb8898af28fa23041176bdd9c5cd084
SHA256:	57d3a79ba52cafd0ba7f6dbc05e9e1588b3f6aca51c508e04c802acd0869bf04

分析结果严重性

高危	中危	信息	安全	关注
4	10	3	2	0

四大组件信息

Activity组件：25个，其中export的有： 0个
Service组件：15个，其中export的有： 3个
Receiver组件：12个，其中export的有： 1个
Provider组件：6个，其中export的有： 0个

证书信息

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977a72d17958704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
android.permission.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.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）
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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.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.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.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.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_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
android.provider.Telephony.SMS_RECEIVED	未知	未知权限	来自 android 引用的未知权限。

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.Manifest.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_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.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.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。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
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.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.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。

网络通信安全

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。

证书安全分析

高危: **0** | 警告: **1** | 信息: **1**

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

MANIFEST分析

高危: **0** | 警告: **4** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用程序具有网络安全配置 [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。
2	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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。

3	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。
4	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。
5	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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。

</> 安全漏洞检测

高危: **2** | 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	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
2	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
3	应用程序记录日志信息，不应记录敏感信息	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
4	应用程序可以写入应用程序目录。敏感信息应加密。	信息	CWE: CWE-276: 默认权限不正确 OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限

5	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
6	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
7	该文件是World Readable。任何应用程序都可以读取文件	高危	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
8	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
9	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
10	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

行为分析

编号	行为	标签	文件
00047	查询本地IP地址	网络 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
00162	创建 InetSocketAddress 对象并连接到它	socket	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
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

00013	读取文件并将其放入流中	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
00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00038	查询电话号码	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
00126	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
00188	获取短信地址	短信	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
00025	监视要执行的一般操作	反射	升级会员：解锁高级权限
00049	查询短信发送者的电话号码	短信 信息收集	升级会员：解锁高级权限
00050	Q查询短信服务中心时间戳	短信 信息收集	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
00129	获取短信内容	短信 信息收集	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
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	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
00040	发送短信	短信	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

敏感权限分析

类型	匹配	权限

恶意软件常用权限	10/30	android.permission.RECEIVE_BOOT_COMPLETED android.permission.GET_ACCOUNTS android.permission.SEND_SMS android.permission.READ_SMS android.permission.RECEIVE_SMS android.permission.RECEIVE_MMS android.permission.READ_PHONE_STATE android.permission.READ_CONTACTS android.permission.VIBRATE android.permission.WAKE_LOCK
其它常用权限	8/46	android.permission.INTERNET android.permission.FOREGROUND_SERVICE android.permission.ACCESS_NETWORK_STATE android.permission.CHANGE_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE com.google.android.gms.permission.AD_ID com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

域名检测

域名	状态	中国境内	位置信息
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
smsforward-b2198.firebaseio.com	安全	否	**IP地址:** 35.201.97.85 **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
frzinapps.com	安全	否	**IP地址:** 183.111.199.191 **国家:** 大韩民国 **地区:** 京畿道 **城市:** 城南市 **纬度:** 37.420624 **经度:** 127.126717 **查看:** Google 地图
website.com	安全	否	**IP地址:** 104.22.66.195 **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

URL链接分析

URL信息	源码文件
• https://play.google.com/store/apps/details?id=	com/frzinapps/smsforward/localad/LocalAdView.java
• https://frzinapps.com/refund.php	com/frzinapps/smsforward/bill/h.java
• https://frzinapps.com/url/help.php	com/frzinapps/smsforward/MainActivity.java
• https://frzinapps.com/url/help.php	com/frzinapps/smsforward/ui/FilterSettingHelpActivity.java
• https://github.com/frzinapps/smsforwarder_language • https://frzinapps.com/url/privacy.php	com/frzinapps/smsforward/ui/settings/SettingsActivity.java
• https://play.google.com/store/account/subscriptions?package=com.frzinapps.smsforward	com/frzinapps/smsforward/bill/RemoveAdActivity.java
• https://frzinapps.com/url/help.php • https://frzinapps.com/url/krhelp.php	com/frzinapps/smsforward/NoticeView.java
• https://api.telegram.org/bot	com/frzinapps/smsforward/httplib/d.java
• https://smsforward-b2198.firebaseio.com • https://website.com/send.php • https://website.com/send.php?msg=	自研引擎-S

FIREBASE数据库分析

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://smsforward-b2198.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/571413090288/namespaces/firebase:fetch?key=AIzaSyBZvwzsAFwGQ753OoOtoZwHHHre8yUs3Gg ） 已禁用。响应内容如下所示： 响应码是 403

第三方SDK

SDK名称	开发者	描述信息
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
Audience Network SDK	Facebook	The Audience Network allows you to monetize your Android apps with Facebook ads. An interstitial ad is a full screen ad that you can show in your app. Typically interstitial ads are shown when there is a transition in your app. For example -- after finishing a level in a game or after loading a story in a news app.

Google Sign-In	Google	提供使用 Google 登录的 API。
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。
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。
Audience Network	Facebook	通过 Facebook 广告使您通过移动媒体资源获利
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，以助您快速采取行动并专注于您的用户。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
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

EMAIL	源码文件
frzinapps@gmail.com	com/frzinapps/smsforward/MainActivity.java
frzinapps@naver.com	自研引擎-S

追踪器

名称	类别	网址
Facebook Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/65
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OpenTelemetry (OpenCensus, OpenTracing)	Analytics	https://reports.exodus-privacy.eu.org/trackers/412

密钥凭证

可能的密钥
AdMob广告平台的=> "com.google.android.gms.ads.APPLICATION_ID" : "ca-app-pub-6829342112730870~5890691146"
"admob_app_id" : "ca-app-pub-6829342112730870~5890691146"

"firebase_database_url" : "https://smsforward-b2198.firebaseio.com"
"google_api_key" : "AIzaSyBZvwzsAFwGQ753OoOtoZwHHHre8yUs3Gg"
"google_app_id" : "1:571413090288:android:76c7ace3b5611d8b"
"google_crash_reporting_api_key" : "AIzaSyBZvwzsAFwGQ753OoOtoZwHHHre8yUs3Gg"
"password" : "Password"
"str_key_guides_title" : "Notice"
"telegram_token" : "Token"
"str_key_guides_title" : "Notiz"
"str_key_guides_title" : "aviso"
yHTAZeApn5rh6Uzfx06Gv6eHdM34YL
nfX6Qz6PZwxyhhyb2yfCFSMMrxktpP5hRWZC+jZA+yNheXUXwKGmCUaKNr8zbWMElOHhprn9nAz[illegible]
W1zcp5YuPDw8mIQDVCH2uQY7qs2ejdZj5LIgIz4CbQ0wg53rlwE7DDQM6MNUgZLnzNmMSM[illegible]
nFkDpKOGSOA5El09S3somsRL+viClREZysmNu3WJrXFT8lMnBSP5CLNLguYQI7sqCSwm[illegible]UE4
81c858e5602f7b16a0a75ad51643f87d
61c7f7f8fea789040d837dc24f801265
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmf7dd[illegible]XYNCzAhufWfVgH2[illegible]
nXNZ4CH83egZuCVEomC02EwDMFK4p9+x/eT+tPcBAZvE[illegible]NSEW[illegible]a+NKCMQ8+A[illegible]c5yU[illegible]dnMuZ
eyJhbGciOiJSUzI1NiIsIng1YyI6WyJNSUlDNlRDQ0Fk[illegible]NBU29[illegible]RFFZSktvWklodm[illegible]OQVFFT[illegible]RQXdEekVOTUFzR0ExVUVBd3dFVW05dmREQWVGdzB4T kRFeE1UZ3hOalUwTUROYUZ3MHpOREV4TVRNe[illegible]E5hTUdZeEN6QUp[illegible]VQkFZVEFsVlRNUk13RVFZRFZRUUlEQXBEWVd4cFptOXlibWxoT VJZd0ZBWURWUVFIREExTmIzVnVkR0ZwYmlCV[illegible]NUlF3RWdZRFZRU[illegible]XRIY[illegible]5bmJHVWdTVzVqTGpFVU1CSUdBMVVFQXd3TFptOXZMbUpoY 2k1amIyMHdnZ0VpTUEwR0NTcUdTSWIz[illegible]UFBNElCRHdBd2d[illegible]CQVFDekZWS0pPa3FUbXl5ak1IV0JPckxkcFltYzBFY3ZHM01vaGFWK 1VKclZySTJTRHlrWThZV1NrVEt6OUJLb[illegible]pQUERzMzE4NE[illegible]XZWQjhSajNndUgzb0wrc0pUM3U5VjJ5NHp5bzV4TzZGV01CWUVRNl g4RGtHbFl0VHA1dGhlWWJSclhORU[illegible]RitMdEhUQ2FBQU5[illegible]DBORW9MYTZCUmhPRzY4Z0ZmSUF4eDVsVDhSRUU5dXR2UHV5K3JDYUJIb mZIT1BmOHBuMExTdmNlQmlqU0l[illegible]WTVjcmpQVmp5aVBB[illegible]V25IVEZBaWxmSG5wTEJsR3hwQ3lsZVBRaE1LclBjZ3ZEb0Q5bmQwTEE2eFlMRj dEUFhYU2E4RkxPK2ZQVjhDTk[illegible]XE5UmxmMlR0M[illegible]THRXUil1aDVMdWN0UDdBZ01CQUFFd0RRWUpLb1pJaHZjTkFRRUxCUUFEZ2dFQkFFc 01BQlpsKzhSbGswaHFCa3Rz[illegible]0bkYvMDdDblNCZ[illegible]UaVloTXByN1ZSSURsSExvZTVsc2xMaWxmWHp2YXltY01GZUgxdUJ4TndoZjdJTzdX dkl3UWVVSFNWK3JIe[illegible]VPMEpuOEh3Kz[illegible]9oSE[illegible]kTXZENXVXRXduM0x2K1c0eTdPaGFTYnpsaFZDVkNuRkxWS2ljQmF5VVhIdGRKWEpJQ 29rUjQraC9XTk03ZzB[illegible]taT3lmYjhoMXBo[illegible]bFBGS3JjVkRvNW05K0dodFBDNFBOakdMb2s2ci9qeDlDSU9DYXBJcWk4ZlhKRU94S3Zpb FllQVlxZmpXdmb[illegible]VVQkhycENROH[illegible]xsSTAyY1J6NXJ4VzRGUUF6MU5kb0c5SFpEWldhK05ORlRaZEFtdFdQSk1MZCs4TDhzbDQ9Iiwi TUlJQzhUQ0N[illegible]XdJQkFnSUpBTU5J[illegible]bGtNQTBHQ1NxR1NJYjNEUUVCQ3dVQU1BOHhEVEFMQmdOVkJBTU1CRkp2YjNRd0hoY05NVFF 4TVRFNE1UW[illegible]V2hjTk16UXhNV[illegible]U5EQXpXakFQTVEwd0N3WURWUVFEREFSU2IyOTBNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBQU 9DQVE4[illegible]USUJD20tDQVFFQXplVU[illegible]V0hoT1RVKzVNUS9sT21talFXcGZCaStGSnV4dm9lT21Rd2k2ZnJQS0tzYUtLWUdmQ1RQbEtFMGRtckVQOT Vibmkv[illegible]EFwUDE3b3JqVWU2S[illegible]Rk5JNUVaYWRJZmpiaC9xKzg1QzFDcDJCUzJZbXVaUXpYWkhQNjN5eUJwMDVZY2JNS3dDQkhYYUFnWW JtVFRrKzQ[illegible]MXBqTnBIUDZZaU[illegible]Nmem9rR3loYnZCcW5QYm5UZEk5dzZmak5CWUFici91Qk9UVTB2SzRrdHpsV2s1bHZzbTUxZTh2c0xTcVdob0 hBRHEwQXJpQWVsVTRTSHN[illegible]VRU3hXVjBLNWh6VHY0ZWN2Q2JHOWRza2lEQ3dXZyt1VFJTb0FGZVpPaE9OTDAwMHE3VmV5M0RaVGNMbD gvTzROUVZhWlI1aUFn[illegible]EQVFBQm8xQXdUakFkQmdOVkhRNEVGZ1FVc2ltbElSRGNKUjBvZlI3b004S3dIRk9IK3NJd0h3WURWUjBqQkJnd0Z vQVVzaW1sSVJEY0pS[illegible]idvTThLd0hGT0grc0l3REFZRFZSMFRCQVV3QXdFQi96QU5CZ2txaGtpRzl3MEJBUXNGQUFPQ0FRRUFXUWw4U21iUW9C VjN0ak9KOHpNb[illegible]UHBTU05ieDBnN0VML2RRZ0pwZXQwTWNXNjJSSGxnUUFPS2JTM1BSZW8ybnNSQi9aUnlZRHU0aTEzWkhaOGJNc0dPR VM0QlFwejEz[illegible]c5UmhzWHFMMGVEWWZCY2pqdGxydVVieGhuQUxwNFZOMXpWZHlXQVBDajBldTNNeHBnTVdjeW41MFFtaUpTai9FcXUvbEx odmUvd0t2akc[illegible]Vjh1UktSdUZiRmN0MERIQUhNblpxRkhjR1M1U28wY1luU2ZLNWZiQlJOZWxHZmxocGJiUHAwVjBhWGlxaW5xRDBZZTNPYVpkR nErMnJQ[illegible]W9DL2[illegible]L091NExzcFkzYjVvRDlyRU5keTdicTBLZXdQRnRnUHZVa0pySjNUemJpd3ZwZ2haN3pHMjZibko1STd1YzR5MVZ1anFhT0E9PSJdfQ
eWzIsJF4P[illegible]xQap9HK6Vlz8DGlgGwoiLCtyOEK0Bfu
tgLRb4bjuZVA8xvQ9uHNs8UtpBIOiUcagzvtKyyfCofk5U5sNb54GgVVYxa6p4A1ObdJv1jjlUOnzR8keX5LsAM4Ia7xeqiFh0GER4l0ulVChy

本报告由南明离火移动安全分析平台生成

nG4neteU1Pax2gtZVs3FLKv4daVNJMGApEAy36yz99dFtXu0FzIob0yeZn+WSorv3BSI6WsL8sjUx

GooglePlay应用信息

标题: SMS Forwarder

评分: 4.603133 **安装:** 1,000,000+ **价格:** 0 **Android版本支持:** **分类:** 工具 **Play Store URL:** com.frzinapps.smsforward

开发者信息: zerogic, 6270500602590978911, □□□ □□□ □□□ □□□ 136, 4□ 414-C19□, https://zerogic.com, cs@zerogic.com,

发布日期: 2012年7月24日 **隐私政策:** Privacy link

关于此应用:

这是一个可以在多个设备（PC、手机）之间同步短信或通知的应用程序。 小心！ 如果其他人要求您安装此应用程序，请小心，因为他/她可能是骗子。 如何使用 1. 首先，添加过滤器以设置收件人。 2. 输入收件人电话号码、电子邮件、URL、电报、推送服务 ID。您可以添加多个。 3. 您可以将电话号码或消息正文中出现的关键字设置为条件，或者如果您只想转发所有内容，则将其留空。 4. 您可以自定义转发消息的模板。 特点 - 将短信或通知转发到电子邮件、电话、URL、电报、推送服务。 - 为各种选项添加过滤器。 - 支持 Gmail 和 SMTP。 - 支持双 SIM 卡设置。 - 支持设置运行时间。 - 支持过滤器备份/恢复。 此应用程序不提供从未安装该应用程序的设备获取消息的功能。 请求的权限 仅在使用该功能时才请求所有权限。 1.接收短信、接收彩信、读取短信、发送短信 这是读取和发送短信所必需的。 2. 读取联系人 这是读取您的 Gmail 帐户和联系人姓名所必需的。 隐私 - 此应用程序需要阅读或发送短信的权限。 - 此应用程序不会在服务器上保存短信或联系人。 - 当您删除此应用程序时，所有数据将无条件删除。 （但是，在删除此应用程序之前，请先从应用程序中删除推送服务帐户。）

免责声明及风险提示: