南明离火
移动应用检测平台

ANDROID 静态分析报告

Delta Chat • v1.58.3

本报告由南明离火移动安全分析平台生成

分析日期: 2025-08-26 22:11:49

应用概览

文件名称:	Delta Chat v1.58.3.apk
文件大小:	25.65MB
应用名称:	Delta Chat
软件包名:	com.b44t.messenger
主活动:	org.thoughtcrime.securesms.ConversationListActivity
版本号:	1.58.3
最小SDK:	21
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	53/100 (中风险)
杀软检测:	经检测，该文件安全
MD5:	06dacf51cb043f54d3ff536d1882d6d1
SHA1:	10584e180077f58bb71cb1c780a5c2d8aa9920eb
SHA256:	312583a956a9dabeab7522a2575c9c775bf26ea1c80f6f6a887630b22968b3cf

分析结果严重性分布

高危	中危	信息	安全	关注
1	23	2	2	0

四大组件导出状态统计

Activity组件：34个，其中export的有： 8个
Service组件：10个，其中export的有： 3个
Receiver组件：13个，其中export的有： 4个
Provider组件：3个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
签名算法: rsassa_pkcs1v15
有效期自: 2017-02-02 14:32:04+00:00
有效期至: 2044-06-20 14:32:04+00:00
发行人: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
序列号: 0x1729b2d4
哈希算法: sha256
证书MD5: 9d362f50c5949184d1635145d5e78312
证书SHA1: b3ef0539b8a6dedf47b4e149747fbf97f7559133
证书SHA256: 9db6678ed74c88124b825e8f90502b76cd97c5eccc9aa92f4033027102d9aa9d
证书SHA512:
52d19ddbea687a53f8f2a5c7c94fcb54c64d73a1acc56b41febc56449811bb265412e2f1478bdfc1a6b508b6a02bbbed91aa430eb3837c9f9d78f0e384273e16

公钥算法: rsa
密钥长度: 2048
指纹: 1c60361523c78f97fc28ad8d0b2aa0b62018d068d7fae2f7efad3a3a06507def
共检测到 1 个唯一证书

权限声明与风险分级

权限名称	安全等级	权限内容	权限描述
android.permission.READ_CONTACTS	危险	读取联系人信息	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储。
android.permission.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.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.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.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。

android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.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_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
android.permission.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.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.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.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.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.INSTALL_SHORTCUT	普通	允许在启动器中安装快捷方式	允许应用程序在Launcher中安装快捷方。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
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.RAISED_THREAD_PRIORITY	未知	未知权限	来自 android 引用的未知权限。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.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_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.FOREGROUND_SERVICE_DATA_SYNC	普通	允许前台服务进行数据同步	允许常规应用程序使用类型为“dataSync”的 Service.startForeground。
com.b44t.messenger.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
com.sec.android.provider.badge.permission.READ	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。

com.htc.launcher.permission.UPDATE_SHORTCUT	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	普通	在应用程序上显示通知计数	在apex的应用程序启动图标上显示通知计数或徽章。
com.majeur.launcher.permission.UPDATE_BADGE	普通	在应用程序上显示通知计数	在solid的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
android.permission.READ_APP_BADGE	普通	显示应用程序通知	允许应用程序显示应用程序图标徽章。
com.oppo.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章
me.everything.badger.permission.BADGE_COUNT_READ	未知	未知权限	来自 android 引用的未知权限。
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
org.thoughtcrime.securesms.ShareActivity	Schemes: mailto://, Mime Types: audio/*, image/*, text/plain, video/*, application/*, text/*, */*,
org.thoughtcrime.securesms.RoutingActivity	Schemes: openpgp4fpr://, OPENPGP4FPR://, OpenPGP4FPR://, OpenPGP4Fpr://, OpenPGP4fpr://, https://, Hosts: i.delta.chat,
org.thoughtcrime.securesms.NewConversationActivity	Schemes: mailto://,
org.thoughtcrime.securesms.RegistrationActivity	Schemes: chat.delta://, Paths: /com.b44t.messenger/auth, /auth,

org.thoughtcrime.securesms.proxy.ProxySettingsActivity	Schemes: ss://, socks5://, SOCKS5://, SS://,
org.thoughtcrime.securesms.InstantOnboardingActivity	Schemes: DCACCOUNT://, dcaccount://, DCLOGIN://, dclogin://,

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **0** | 警告: **15** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	Activity (org.thoughtcrime.securesms.ShareActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
2	Activity (org.thoughtcrime.securesms.ConversationListActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
3	Activity-Alias (org.thoughtcrime.securesms.RoutingActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。
4	Activity (org.thoughtcrime.securesms.NewConversationActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
5	Activity (org.thoughtcrime.securesms.RegistrationActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
6	Activity (org.thoughtcrime.securesms.proxy.ProxySettingsActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

7	Activity (org.thoughtcrime.securesms.InstantOnboardingActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
8	Activity (org.thoughtcrime.securesms.WebxdcActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
9	Service (org.thoughtcrime.securesms.service.IPCAddAccountsService) 未受保护。 [android:exported=true]	警告	检测到 Service 已导出，未受任何权限保护，任意应用均可访问。
10	Broadcast Receiver (org.thoughtcrime.securesms.service.BootReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
11	Broadcast Receiver (org.thoughtcrime.securesms.service.PanicResponderListener) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
12	Service (androidx.sharetarget.ChooserTargetServiceCompat) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_CHOOSER_TARGET_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
13	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
14	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

15	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

代码安全漏洞检测

高危: **1** | 警告: **7** | 信息: **2** | 安全: **0** | 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	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
3	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
4	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
5	应用程序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
6	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

7	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
8	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
9	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
10	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

Native 库安全加固检测

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED(裁剪符号表)

1	x86/libnative-utils.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程（ROP）攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
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
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
00036	从 res/raw 目录获取资源文件	反射	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
00183	获取当前相机参数并更改设置	相机	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
00192	获取短信收件箱中的消息	短信	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
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
00054	从文件安装其他APK	反射	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
00028	从assets目录中读取文件	文件	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	10/30	android.permission.READ_CONTACTS android.permission.CAMERA android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.RECEIVE_BOOT_COMPLETED android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	11/46	android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_BACKGROUND_LOCATION android.permission.ACCESS_NETWORK_STATE android.permission.INTERNET com.android.launcher.permission.INSTALL_SHORTCUT android.permission.ACCESS_WIFI_STATE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.FOREGROUND_SERVICE

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

恶意域名威胁检测

域名	状态	中国境内	位置信息
index.html	安全	否	No Geolocation information available.
journeyapps.com	安全	否	**IP地址:** 216.137.39.6 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
www.smpte-ra.org	安全	否	**IP地址:** 52.20.185.129 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
din-server.org	安全	否	No Geolocation information available.

your-server.org	安全	否	**IP地址:** 95.216.70.207 **国家:** 芬兰 **地区:** 新地省 **城市:** 赫尔辛基 **纬度:** 60.169521 **经度:** 24.935450 **查看:** Google 地图
el-vostre-servidor.org	安全	否	No Geolocation information available.
tu-servidor.org	安全	否	No Geolocation information available.
get.delta.chat	安全	否	**IP地址:** 37.218.242.41 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
meet.jit.si	安全	否	**IP地址:** 104.18.21.227 **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
webxdc.org	安全	否	**IP地址:** 37.218.242.41 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
delta.chat	安全	否	**IP地址:** 37.218.242.41 **国家:** 荷兰（王国） **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
docs.rs	安全	否	**IP地址:** 18.154.206.60 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• https://accounts.google.com/	com/b44t/messenger/DcContext.java

• http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt	com/googlecode/mp4parser/authoring/tracks/SMPTETTTrackImpl.java
• https://github.com/deltachat/deltachat-android/issues/1639:	org/thoughtcrime/securesms/ContactSelectionListFragment.java
• https://github.com/deltachat/deltachat-android/issues!! • https://github.com/deltachat/deltachat-android/issues • https://get.delta.chat/#changelogs	org/thoughtcrime/securesms/ConversationListActivity.java
• file://index.html	org/thoughtcrime/securesms/FullMsgActivity.java
• https://delta.chat/contribute • https://delta.chat • https://delta.chat/gdpr • https://github.com/deltachat/deltachat-android/issues	org/thoughtcrime/securesms/LocalHelpActivity.java
• https://delta.chat/chatmail	org/thoughtcrime/securesms/InstantOnboardingActivity.java
• https://webxdc.org/apps/	org/thoughtcrime/securesms/util/Prefs.java
• https://github.com/journeyapps/zxing-android-embedded • https://el-vostre-servidor.org/$sala • https://github.com/vinc3m1/roundedimageview.git • https://your-server • https://meet.jit.si/$room • https://din-server.org/$rum • https://github.com/vinc3m1/roundedimageview • https://your-server.org/$room • https://journeyapps.com/ • https://tu-servidor.org/$room • https://get.delta.chat • https://github.com/vinc3m1	自研引擎-S
• 1.3.101.112 • 239.255.255.250 • 1.3.101.110 • 1.3.101.111 • https://github.com/tailscale/tailscale/issues/188mismatching • 1.3.101.113 • https://docs.rs/getrandom#nodejs-es-module-support • data::deletemessages	lib/x86/libnative-utils.so

Firebase 配置安全检测

标题	严重程度	描述信息

本报告由南明离火移动安全分析平台生成

Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/922391085500/namespaces/firebase:fetch?key=AIzaSyBYH8Iznh8btYX7g_udv_bu68VH30zzxho ） 已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
ZXing Android Embedded	JourneyApps	Barcode scanning library for Android, using ZXing for decoding.
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。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。
Jetpack ProfileInstaller	Google	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
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。
Jetpack ShareTarget	Google	提供向后兼容性，可以将快捷方式用作直接共享目标。

敏感凭证泄露检测

可能的密钥
"password" : "Palavra-chave"
"login_smtp_password" : "SMTP-passord"
"password" : "Passwort"
"login_auth_method" : "Auktoriseringsmetod"
"login_auth_method" : "Autorisationsmetode"
"login_smtp_password" : "SMTP-Passwort"

"password" : "Contrasinal"
"login_auth_method" : "Autorisatiemethode"
"library_zxingandroidembedded_author" : "JourneyApps"
"password" : "Parol"
"password" : "Pasvorto"
"login_auth_method" : "Autoriseringsmetode"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"password" : "Salasana"
"password" : "Wachtwoord"
"pref_incognito_keyboard" : "Inkognito-tastatur"
"login_smtp_password" : "SMTP-wachtwoord"
"password" : "Heslo"
"password" : "Lozinka"
"password" : "Pasahitza"
"pref_incognito_keyboard" : "Inkognito-Tastatur"
"password" : "Adgangskode"
"login_auth_method" : "Autorisierungsmethode"
"password" : "Passord"
"google_api_key" : "AIzaSyBYH8Iznh8btYX7g_udv_bu68VH30zzxho"
"google_app_id" : "1:922391085500:android:92b4cf12669cc083e2bb9"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"pref_password_and_account_settings" : "Kontoinnstillinger"
"pref_incognito_keyboard" : "Inkognito-tangentbord"
"password" : "Parola"
"password" : "Senha"
"google_crash_reporting_api_key" : "AIzaSyBYH8Iznh8btYX7g_udv_bu68VH30zzxho"
"password" : "Contrasenya"
"password" : "Password"
A2B55680-6F43-11E0-9A3F-0002A5D5C51B

9A04F079-9840-4286-AB92-E65BE0885F95

免责声明及风险提示:

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。