南明离火
移动应用检测平台

ANDROID 静态分析报告

Subsidios

SubsidiosGLP • 1.0

分析日期: 2024-02-28 06:59:59

应用概览

文件名称:	SubsidiosGLP.apk
文件大小:	15.93MB
应用名称:	SubsidiosGLP
软件包名:	com.glp.subsidiosonline
主活动:	com.bexsoluciones.bexmovilprovigas.Home
版本号:	1.0
最小SDK:	23
目标SDK:	29
加固信息:	未加壳
应用程序安全分数:	44/100 (中风险)
跟踪器检测:	5/432
杀软检测:	3 个杀毒软件报毒
MD5:	f7d504a0a600815140778fc511bd3942
SHA1:	52ede025b324e99d2c7971ab87d2e3d180f4f5a
SHA256:	e3ab2b03ce8537a124c22697350517c3b8ebf453d91f39371db6d31fe7e8bd3

分析结果严重性分布

高危	中危	信息	安全	关注
4	20	2	1	1

四大组件导出状态统计

Activity组件：12个，其中export的有： 3个
Service组件：8个，其中export的有： 3个
Receiver组件：6个，其中export的有： 3个
Provider组件：1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=Andres, OU=Bex Soluciones, O=Bex, L=Medellin, ST=Colombia, C=57
签名算法: rsassa_pkcs1v15
有效期自: 2024-02-08 20:11:39+00:00
有效期至: 2049-02-01 20:11:39+00:00
发行人: CN=Andres, OU=Bex Soluciones, O=Bex, L=Medellin, ST=Colombia, C=57
序列号: 0x1
哈希算法: sha256
证书MD5: 77a9da7a7d4ddb4b6aa7c312451030bd
证书SHA1: 312fc30a6ac202ddfea0851cb2ec7ab96ac975b1
证书SHA256: 315d72210ce6659cd6b167a5247a6458068e96697b626d397fb5f3df904437c2
证书SHA512:
c2cd1d85117d37c308ad1d15cf01a2b3a926182eab1c2891ac8ca0781ed6fc91b4d181be7c6d942f61ea35ad56c333f66a5ac51ec04531cb2def7469efb89a15

公钥算法: rsa
密钥长度: 2048
指纹: 2e1b56d39d821ed98a215a1a2e29b2556ed2d7a2e4186611fd2bb67b5026d8dd
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.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_PRIVILEGED_PHONE_STATE	未知	未知权限	来自 android 引用的未知权限。
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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.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错略的经纬度信息，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_LOCATION_EXTRA_COMMANDS	普通	访问定位额外命令	访问额外位置提供程序命令，恶意应用程序可能会使用它来干扰GPS或其他位置源的操作。
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。
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
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.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.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.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.WRITE_MEDIA_STORAGE	签名(系统)	获取外置SD卡的写权限	允许应用程序在外置SD卡中进行写入操作。
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_INTERNAL_STORAGE	未知	未知权限	来自 android 引用的未知权限。
android.permission.READ_INTERNAL_STORAGE	未知	未知权限	来自 android 引用的未知权限。
com.glp.subsidiosonline.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.com.glp.subsidiosonline://,

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	应用程序已使用代码签名证书进行签名
应用程序存在Janus漏洞	警告	应用程序使用了v1签名方案进行签名，如果只使用v1签名方案，那么它就容易受到安卓5.0-8.0上的Janus漏洞的攻击。在安卓5.0-7.0上运行的使用了v1签名方案的应用程序，以及同时使用了v2/v3签名方案的应用程序也同样存在漏洞。

Manifest 配置安全分析

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

序号	问题	严重程度	描述信息
1	应用程序可以安装在存在漏洞的已更新 Android 版本上 Android 6.0-6.0.1, [minSdk=23]	警告	该应用程序可以安装在具有多个未修复漏洞的旧版本 Android 上。这些设备不会从 Google 接收合理的安全更新。支持 Android 版本 => 10、API 29 以接收合理的安全更新。
2	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。

3	程序可被任意调试 [android:debuggable=true]	高危	应用可调试标签被开启，这使得逆向工程师更容易将调试器挂接到应用程序上。这允许导出堆栈跟踪和访问调试助手类。
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	Broadcast Receiver (com.google.android.gms.gcm.GcmReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
6	Activity (com.bexsoluciones.bexmovilprovigas.InicioSubsidios) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
7	Activity (com.google.android.gms.appinvite.PreviewActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
8	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。
9	Service (com.google.firebase.messaging.FirebaseMessagingService) 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，因此使其对设备上的任何其他应用程序都可访问。
10	Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) 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，因此使其对设备上的任何其他应用程序都可访问。
11	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.INSTALL_PACKAGES [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。

本报告由南明离火移动安全分析平台生成

12	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [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。
13	Service (com.google.firebase.iid.FirebaseInstanceIdService) 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，因此使其对设备上的任何其他应用程序都可访问。

代码安全漏洞检测

高危: **2** | 警告: **6** | 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	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
4	应用程序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
5	使用弱加密算法	高危	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
6	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

7	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
8	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用已被攻破或存在风险的密码学算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
9	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
10	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
11	启用了调试配置。生产版本不能是可调试的	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

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	armeabi/libBlinkBarcode.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。		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	False warning 符号可用

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	5/30	android.permission.READ_PHONE_STATE android.permission.CAMERA android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.WAKE_LOCK
其它常用权限	10/46	android.permission.FLASHLIGHT android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_LOCATION_EXTRA_COMMANDS android.permission.ACCESS_WIFI_STATE com.google.android.c2dm.permission.RECEIVE android.permission.BLUETOOTH android.permission.BLUETOOTH_ADMIN android.permission.WRITE_EXTERNAL_STORAGE android.permission.READ_EXTERNAL_STORAGE

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

gcm-client-datagas.firebaseio.com	安全	否	**IP地址:** 34.120.206.254 **国家:** United States of America **地区:** Missouri **城市:** Kansas City **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
login.live.com	安全	否	**IP地址:** 20.190.144.166 **国家:** Korea (Republic of) **地区:** Seoul-teukbyeolsi **城市:** Seoul **纬度:** 37.566311 **经度:** 126.977942 **查看:** Google 地图
restlet.org	安全	否	**IP地址:** 47.75.40.150 **国家:** United States of America **地区:** New York **城市:** New York City **纬度:** 40.713516 **经度:** -74.008041 **查看:** Google 地图
goo.gl	安全	否	**IP地址:** 142.250.217.174 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
www.webdav.org	安全	否	**IP地址:** 140.211.9.38 **国家:** United States of America **地区:** Oregon **城市:** Eugene **纬度:** 44.036083 **经度:** -123.052429 **查看:** Google 地图
www.linkedin.com	安全	是	**IP地址:** 52.130.75.155 **国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.224333 **经度:** 121.469139 **查看:** 高德地图
www.paypal.com	安全	否	**IP地址:** 192.229.232.89 **国家:** Japan **地区:** Tokyo **城市:** Tokyo **纬度:** 35.689507 **经度:** 139.691696 **查看:** Google 地图
www.openmobilealliance.org	安全	否	**IP地址:** 104.26.8.105 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

pdf417.mobi	安全	否	**IP地址:** 172.67.134.202 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
provigas.bexsoluciones.com	安全	否	**IP地址:** 35.188.44.247 **国家:** United States of America **地区:** Iowa **城市:** Council Bluffs **纬度:** 41.261940 **经度:** -95.860832 **查看:** Google 地图
www.wireless-village.org	安全	否	**IP地址:** 172.67.131.214 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
schema.org	安全	否	**IP地址:** 192.178.50.46 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
twitter.com	安全	否	**IP地址:** 104.244.42.1 **国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.773968 **经度:** -122.410446 **查看:** Google 地图
login.yahoo.com	安全	否	**IP地址:** 106.10.248.157 **国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看:** Google 地图
pagead2.googlesyndication.com	安全	否	**IP地址:** 142.250.64.130 **国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
tools.ietf.org	安全	否	**IP地址:** 104.16.45.99 **国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.783058 **经度:** -96.806671 **查看:** Google 地图

webglp.minminas.gov.co	安全	否	**IP地址:** 179.1.211.143 **国家:** Colombia **地区:** Antioquia **城市:** Medellin **纬度:** 6.251840 **经度:** -75.563591 **查看:** Google 地图
schemas.xmlsoap.org	安全	否	**IP地址:** 13.107.213.58 **国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件
• http://webglp.minminas.gov.co:8081/libreria?idMovil=	co/gov/minminas/SubsidiosGLP/publico/Mediador.java
• https://provigas.bexsoluciones.com/bexmovil/api/	com/bexsoluciones/bexmovilprovigas/ApiClient.java
• https://provigas.bexsoluciones.com/bexmovil/api/datastock/?apikey=16e35825b92499c930a33be03f6f4ba597fd9e8b&method=getCalculoSubsidios&deviceid=	com/bexsoluciones/bexmovilprovigas/CalcularSubsidio.java
• https://provigas.bexsoluciones.com/bexmovil/api/	com/bexsoluciones/bexmovilprovigas/InicioSubsidios.java
• https://provigas.bexsoluciones.com/bexmovil/api/datastock/?apikey=16e35825b92499c930a33be03f6f4ba597fd9e8b&method=getCalculoSubsidios • http://3.223.225.176/api/v1/datagas/echo • https://provigas.bexsoluciones.com/bexmovil/api/datastock/?apikey=16e35825b92499c930a33be03f6f4ba597fd9e8b&method=	com/bexsoluciones/bexmovilprovigas/model/Constants.java
• http://pdf417.mobi	com/microblink/view/overlay/IIIIIIIIII.java
• file:///	org/kobjects/util/Util.java
• http://schemas.xmlsoap.org/soap/encoding/ • http://schemas.xmlsoap.org/soap/envelope/	org/ksoap2/SoapEnvelope.java
• http://xml.apache.org/xml-soap	org/ksoap2/serialization/MarshalHashtable.java
• http://www.wireless-village.org/CSP • http://www.wireless-village.org/PA • http://www.wireless-village.org/TRC • http://www.openmobilealliance.org/DTD/WV-CSP • http://www.openmobilealliance.org/DTD/WV-PA • http://www.openmobilealliance.org/DTD/WV-TRC • www.wireless-village.org	org/kxml2/wap/wv/WV.java

• http://www.webdav.org/specs/rfc2518.html • http://www.webdav.org/specs/rfc2518.html#METHOD_COPY • http://www.webdav.org/specs/rfc2518.html#METHOD_LOCK • http://www.webdav.org/specs/rfc2518.html#METHOD_MKCOL • http://www.webdav.org/specs/rfc2518.html#METHOD_MOVE • http://tools.ietf.org/html/rfc5789 • http://www.webdav.org/specs/rfc2518.html#METHOD_PROPFIND • http://www.webdav.org/specs/rfc2518.html#METHOD_PROPPATCH • http://www.webdav.org/specs/rfc2518.html#METHOD_UNLOCK	org/restlet/data/Method.java
• http://tools.ietf.org/html/rfc6585 • http://www.webdav.org/specs/rfc2518.html • http://restlet.org/learn/javadocs/2.3/ • http://www.webdav.org/specs/rfc2518.html#STATUS_102 • http://www.webdav.org/specs/rfc2518.html#STATUS_207 • http://www.webdav.org/specs/rfc2518.html#STATUS_422 • http://www.webdav.org/specs/rfc2518.html#STATUS_423 • http://www.webdav.org/specs/rfc2518.html#STATUS_424 • http://tools.ietf.org/html/rfc6585#section-4 • http://www.webdav.org/specs/rfc2518.html#STATUS_507	org/restlet/data/Status.java
• https://github.com/restlet/restlet-framework-java/issues/778),	org/restlet/representation/ObjectRepresentation.java
	自研引擎分析结果

- http://schema.org/ListenAction
- http://schema.org/SearchAction
- https://plus.google.com/
- http://schema.org/FilmAction
- https://accounts.google.com
- http://schema.org/PhotographAction
- http://schema.org/WantAction
- https://twitter.com
- https://www.googleapis.com/auth/drive.appdata
- https://www.facebook.com
- https://www.googleapis.com/auth/plus.login
- https://www.linkedin.com
- https://www.googleapis.com/auth/drive
- http://hostname/?
- https://www.googleapis.com/auth/fitness.body.write
- https://www.googleapis.com/auth/plus.me
- https://www.googleapis.com/auth/fitness.activity.write
- https://www.googleapis.com/auth/drive.apps
- https://www.googleapis.com/auth/drive.file
- https://gcm-client-datagas.firebaseio.com
- https://www.googleapis.com/auth/datastoremobile
- https://login.live.com
- http://goo.gl/8Rd3yj
- http://schema.org/CommunicateAction
- https://www.googleapis.com/auth/games
- https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps
- http://schema.org/ActiveActionStatus
- https://www.paypal.com
- http://schema.org/AddAction
- https://login.yahoo.com
- http://schema.org/FailedActionStatus
- https://www.googleapis.com/auth/fitness.body.read
- http://schema.org/ReserveAction
- https://www.googleapis.com/auth/fitness.location.read
- http://schema.org/BookmarkAction
- http://webglp.minminas.gov.co:8081/libreria?idMovil=
- http://schema.org/LikeAction
- https://www.googleapis.com/auth/appstate
- http://schema.org/ViewAction
-
- https://www.googleapis.com/auth/games_update
- https://www.googleapis.com/auth/fitness.nutrition.write
- https://www.googleapis.com/auth/fitness.location.write
- http://schema.org/CompletedActionStatus
- https://www.googleapis.com/auth/fitness.nutrition.read
- https://www.googleapis.com/auth/games.firstparty
- https://www.googleapis.com/auth/fitness.activity.read
- http://schema.org/ActivateAction
- http://schemas.org/MatchAction

Firebase 配置安全检测

标题	严重程度	描述信息

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Google Analytics	Google	提供各种 API，可帮助您收集、配置和报告用户与您的在线内容进行互动的数据。

Google Cast	Google	使用 Google Cast SDK，您可以扩展 Android，iOS 或 Chrome 应用，以将其流式视频和音频定向到电视或声音系统。 您的应用程序成为播放，暂停，搜索，倒带，停止和控制媒体的遥控器。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
android@android.com0	自研引擎分析结果
yay@y.u5vcghyy	lib/armeabi/libBlinkBarcode.so

第三方追踪器检测

名称	类别	网址
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105

敏感凭证泄露检测

可能的密钥
"google_api_key" : "AIzaSyBVEwb57re[illegible]LaisyMEa5KdCy6K2jk"
"firebase_database_url" : "https://gcm-client-datagas.firebaseio.com"
"google_crash_reporting_api_key" : "AIzaSyBVEwb57re0hhe8LaisyMEa5KdCy6K2jk"
16e35825b92499c930a33be03f6f4ba597fd9c8b

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动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。