ANDROID STATIC ANALYSIS REPORT

Health Monitor (1.0.3)

File Name:	com.gthreload.health.monitor.gp_4.apk
Package Name:	com.gthreload.health.monitor.gp
Scan Date:	Aug. 29, 2025, 11:22 p.m.
App Security Score:	51/100 (MEDIUM RISK)

Grade:	B
Trackers Detection:	7/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	17	2	2	2

FILE INFORMATION

File Name: com.gthreload.health.monitor.gp_4.apk
Size: 10.17MB
MD5: 1b9b127e606b8c710bf8c86a11af36d9
SHA1: d31be03365d5680af7b0df2552e4a3606cc4f35c
SHA256: e04fd21835a9a87bc862d8edf3cd0e56f90d397baa07f766ad1af336def87f37

APP INFORMATION

App Name: Health Monitor
Package Name: com.gthreload.health.monitor.gp

Main Activity: com.gthreload.health.monitor.gp.view.activity.SplashActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 1.0.3
Android Version Code: 4

APP COMPONENTS

Activities: 31
Services: 13
Receivers: 13
Providers: 4
Exported Activities: 3
Exported Services: 2
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-10-24 02:20:07+00:00
Valid To: 2054-10-24 02:20:07+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x9bfee50c809335d1f8da2a0ecdb0f9015c885819
Hash Algorithm: sha256
md5: e8ae04b4538ff6c4ac8d735ffc33aaa9
sha1: 4856ba7892022fb2a7546ca14d28bd24546a28c5
sha256: 690b8fb4ba296f340ffc0214829ec81665b327029f098bf2693d6332aadbbe00
sha512: f3f1e41513c931c9569fa7f270cb97b1d53b8d12827727ec4024d85883dbe2feb022f0e254b20854eed908bf0603aa24b51195e31b09f5c82174ff89a2bd6091
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 1a9ca801dfee27ccfe40aaca3c6fe91c549e310a442fb2621ca916abe93e2def
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_HEALTH	normal	enables foreground services with health-related functionality.	Allows a regular application to use Service.startForeground with the type "health".
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.HIGH_SAMPLING_RATE_SENSORS	normal	Access higher sampling rate sensor data	Allows an app to access sensor data with a sampling rate greater than 200 Hz.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.PRODUCT check
SIM operator check
network operator name check
ro.kernel.qemu check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.gthreload.health.monitor.gp,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **9** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
5	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

HIGH: **1** | WARNING: **6** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	a0/c.java a3/f.java b2/d.java c2/a.java com/appsflyer/internal/AFg1aSDK.java com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/data/LineDataSet.java com/github/mikephil/charting/data/PieEntry.java com/github/mikephil/charting/listener/a.java com/tencent/mmkv/MMKV.java com/tencent/mmkv/MMKVContentProvider.java d3/q.java d4/b0.java d4/c.java d4/c0.java d4/d0.java d4/e.java d4/g0.java d4/k0.java d4/l.java d4/m0.java d4/n.java d4/n0.java d4/o0.java d4/r0.java d4/s0.java d4/x.java d4/z.java d8/c.java f/b0.java f/f.java f/n0.java f0/c.java f1/i.java g/b.java g/d.java g/f0.java g/k.java h2/n.java h4/j.java i1/a.java i4/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				i4/e.java i4/l.java i4/q.java j/l.java j4/f.java k/c.java k/d.java k8/a.java k8/b.java l8/f.java m/a.java m2/e.java o/f.java o/h.java o/k.java org/libpag/HardwareDecoder.java org/libpag/PAGAnimator.java org/libpag/TraceImage.java org/libpag/b.java r/a.java r1/h.java s5/e.java u7/d.java v2/f0.java v2/n.java w/c0.java w/h.java w/l0.java w/n0.java w/u0.java w/v0.java w0/p.java w2/a0.java w2/d0.java w2/e0.java w2/f0.java w2/q0.java w2/r.java w2/z.java x2/f.java x2/n.java x3/b.java y0/i.java z3/a.java
2	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFb1tSDK.java
3	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	c7/a.java c7/b.java com/appsflyer/internal/AFb1cSDK.java com/gthreload/health/monitor/gp/view/widget/MaybeLikeLayout.java d7/a.java h4/o.java w/u0.java
4	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	f/a.java f/c0.java f/d0.java f/h.java f/n0.java m/j.java s/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	c8/c.java c8/d.java c8/g.java c8/h.java
6	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	d4/x.java f0/a.java z3/a.java
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	m1/m0.java m1/t0.java
8	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/libpag/PAGDiskCache.java w/u0.java
9	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/gthreload/health/monitor/gp/HealthApplication.java f3/e.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	h2/a0.java
11	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	o/k.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00003	Put the compressed bitmap data into JSON object	camera	j/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/appsflyer/internal/AFb1tSDK.java com/appsflyer/internal/AFc1dSDK.java com/appsflyer/internal/AFc1sSDK.java com/appsflyer/internal/AFf1nSDK.java com/gthreload/health/monitor/gp/comm/measure/HealthCameraManage.java com/gthreload/health/monitor/gp/ext/HealthExtKt.java d4/c.java w/b.java w/n0.java w/u0.java w/v0.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFb1tSDK.java com/appsflyer/internal/AFc1sSDK.java d4/b0.java w/n0.java
00036	Get resource file from res/raw directory	reflection	com/appsflyer/internal/AFb1tSDK.java com/appsflyer/internal/AFf1jSDK.java com/appsflyer/internal/AFi1bSDK.java com/appsflyer/internal/AFi1cSDK.java d4/c.java w/b.java w/u0.java w/v0.java
00094	Connect to a URL and read data from it	command network	h3/a.java org/libpag/b.java w/b0.java
00014	Read file into a stream and put it into a JSON object	file	e3/d.java i4/p.java k3/a.java p/i.java s/a.java w/y.java y/j.java
00013	Read file and put it into a stream	file	com/appsflyer/internal/AFb1jSDK.java d3/y.java e3/d.java g/d.java i3/e.java i4/p.java j8/i.java k3/a.java o/k.java org/libpag/PAGFont.java p/i.java s/a.java w/l0.java w/y.java y/j.java y6/e.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFj1wSDK.java w/n0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFj1wSDK.java w/n0.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1mSDK.java com/appsflyer/internal/AFj1wSDK.java w/n0.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1aSDK.java com/appsflyer/internal/AFi1bSDK.java com/appsflyer/internal/AFj1wSDK.java w/b.java w/n0.java w/u0.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFj1wSDK.java w/n0.java
00187	Query a URI and check the result	collection sms calllog calendar	w/n0.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFj1wSDK.java w/n0.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1mSDK.java com/appsflyer/internal/AFj1wSDK.java w/n0.java
00089	Connect to a URL and receive input stream from the server	command network	c1/d.java com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1nSDK.java f0/c.java org/libpag/b.java
00162	Create InetSocketAddress object and connecting to it	socket	c8/b.java c8/h.java
00163	Create new Socket and connecting to it	socket	c8/b.java c8/h.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFi1wSDK.java w/u0.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/gthreload/health/monitor/gp/comm/measure/HealthCameraManage.java com/gthreload/health/monitor/gp/ext/HealthExtKt.java d4/c.java w/u0.java w/v0.java
00015	Put buffer stream (data) to JSON object	file	w/u0.java w/y.java
00022	Open a file from given absolute path of the file	file	com/appsflyer/internal/AFg1eSDK.java e3/d.java i8/c.java m3/b.java w/y.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFg1eSDK.java e3/d.java w/y.java
00004	Get filename and put it to JSON object	file collection	c0/a.java w/y.java
00012	Read data and put it into a buffer stream	file	g/d.java o/k.java w/y.java
00096	Connect to a URL and set request method	command network	c1/d.java com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1nSDK.java org/libpag/b.java
00030	Connect to the remote server through the given URL	network	org/libpag/b.java
00109	Connect to a URL and get the response code	network command	c1/d.java com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1nSDK.java com/appsflyer/internal/AFf1iSDK.java org/libpag/b.java w/b0.java
00108	Read the input stream from given URL	network command	org/libpag/b.java
00009	Put data in cursor to JSON object	file	w/u0.java
00183	Get current camera parameters and change the setting.	camera	com/gthreload/health/monitor/gp/comm/measure/HealthCameraManage.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1mSDK.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/503978180382/namespaces/firebase:fetch?key=AIzaSyCT4rf6hgJqMGOjL2rh0E8Ch7lOcxEHpdY is enabled. Ensure that the configurations are not sensitive response: {'entries': {'HMGP101': '{"HM_Coldlaunch_time":"10","HM_Hotlaunch_time":"7","HM_InterAD_Showtimes":"4","HM_Open":"ca-app-pub-7855170407354960/5983691160","HM_Inter1":"ca-app-pub-7855170407354960/4322377679","HM_ 7855170407354960/7724018360","HM_Native1":"ca-app-pub-7855170407354960/6265436777","HM_Native2":"ca-app-pub-7855170407354960/4952355102","HM_Show_Native":"false","HM_First_Click_ShowAD":"false","HM_Measure_Start_ShowAD":"false","HM_Measure_Report_ShowAD":"false","HM_Splash_ShowAD":"false","HM_Audit_Mode":"false","HM_Earning_FB '{"HM_Coldlaunch_time":"10","HM_Hotlaunch_time":"7","HM_InterAD_Showtimes":"4","HM_Open":"ca-app-pub-7855170407354960/5983691160","HM_Inter1":"ca-app-pub-7855170407354960/2838653073","HM_Inter2":"ca-app-pub-7855170407354960/7724018360","HM_Native1":"ca-app-pub-7855170407354960/6265436777","HM_Native2":"ca-app-pub-7855170407354960/4952355102","HM_Show_Native":"false","HM_First_Click_ShowAD":"false","HM_Measure_Start_ShowAD":"false","HM_Measure_Report_ShowAD":"false","HM_Splash_ShowAD":"100","HM_Audit_Mode":"false","HM_Earning_FBs 'HMGP106': '{"HM_Coldlaunch_time":"10","HM_Hotlaunch_time":"7","HM_InterAD_Showtimes":"4","HM_Open":"ca-app-pub-7855170407354960/5983691160","HM_Inter1":"ca-app-pub-7855170407354960/2838653073","HM_Inter2":"ca-app-pub-7855170407354960/7724018360","HM_Native1":"ca-app-pub-7855170407354960/6265436777","HM_Native2":"ca-app-pub-7855170407354960/4952355102","HM_Show_Native":"false","HM_First_Click_ShowAD":"false","HM_Measure_Start_ShowAD":"false","HM_Measure_Report_ShowAD":"false","HM_Splash_ShowAD":"100","HM_Audit_Mode":"false","HM_Earning_FBs 'state': 'UPDATE', 'templateVersion': '18'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.CAMERA, android.permission.WAKE_LOCK, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	6/44	android.permission.FLASHLIGHT, android.permission.CHANGE_WIFI_STATE, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.c2dm.permission.RECEIVE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION
otheve.beacon.qq.com	IP: 129.226.106.210 Country: Hong Kong Region: Hong Kong City: Hong Kong

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
diabetes.org	ok	**IP:** 44.218.46.141 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
graph-video.s	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
otheve.beacon.qq.com	ok	**IP:** 129.226.106.210 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
graph.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sdlsdk.s	ok	No Geolocation information available.
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.9.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.mayoclinic.org	ok	**IP:** 23.222.206.33 **Country:** United States of America **Region:** Minnesota **City:** Minneapolis **Latitude:** 44.979969 **Longitude:** -93.263840 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
www.heart.org	ok	**IP:** 104.18.27.158 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
simpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sadrevenue.s	ok	No Geolocation information available.
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
sars.s	ok	No Geolocation information available.
www.youtube.com	ok	**IP:** 172.253.124.190 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sregister.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
n.healthmonitorgp.top	ok	**IP:** 104.21.48.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
aps-webhandler.appsflyer.com	ok	**IP:** 18.238.109.70 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
health-monitor-gp.web.app	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
slaunches.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
svalidate-and-log.s	ok	No Geolocation information available.
diabetesfoodhub.org	ok	**IP:** 3.231.20.35 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sapp.s	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
en.wikipedia.org	ok	**IP:** 198.35.26.96 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.791256 **Longitude:** -122.400810 **View:** Google Map
commons.wikimedia.org	ok	**IP:** 198.35.26.96 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.791256 **Longitude:** -122.400810 **View:** Google Map
svalidate.s	ok	No Geolocation information available.

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
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

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "8db8210676cd4ff2a4688567928b3f80"
"facebook_token" : "d04fc7b270aebf2a01f9f283acb082fe"
"google_api_key" : "AIzaSyCT4rf6hgJqMGOjL2rh0E8Ch7lOcxEHpdY"
"google_crash_reporting_api_key" : "AIzaSyCT4rf6hgJqMGOjL2rh0E8Ch7lOcxEHpdY"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
ki2ip3Sp4zD5u1iHxdI5CQP+nQytWboRZ8YxUMq1u4GDs7rHoXiw6vz07EKttNE7
5BsC37pqFx3Fp5Qtv0y+RSU8LVttAMXjX8aFccLrzxg=
49f946663a8deb7054212b8adda248c6
c56fb7d591ba6704df047fd98f535372fea00211
ZzhYXgKMhken/ic2sDR8A53WLOTMzsBN7DfnMjKoyhk=
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
36864200e0eaf5284d884a0e77d31646
J3qHQsXE9gxUWY3EQze3pD9LpRQkp3i0z4IBb3xvxMfPfsFZNBOU+l2pHi8zC3DO
Q0EftCh9LNoL/97bVNRGH4YGKN2mjVuI8Ruidx0q8xs=
9b8f518b086098de3d77736f9458a3d2f6f95a37
mLbfRIQxtPVbZphUgAhWqMeuqa25AIe/5rz8vv9YVkc=
WIPKXsZv2l0NBmLvWdV3TkucPJ5dkfbRYYrTASAxFfQ=
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
115792089210356248762697446949407573530086143415290314195533631308867097853951
somG6HzRa3YZJrwwnfL6K8d6jP9Npv493BtTLjfx2vaqxDUDPiPCNzpi42Jpggs8
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
PyZj3I+LGZvAhJ9n3OQrlENydgM2JwW0T6dRxf3as8iTDiIpqvAE/3692CSblz+3
AtCF0F/Ugi3KOt6zYtgfLSsd+8KzXVTsnhwfj9NoYBY=

POSSIBLE SECRETS
WQCGmUFTrgSOZ83nswxrNh39wVE6t1Ouq3E0zMLvIMA=
nK4MIXXv/sY+coqtAjalB6f9NiJ1zVnlRnfsJ++LIaOoNJXY+cpXhUK9rjjc0N2G
115792089210356248762697446949407573529996955224135760342422259061068512044369
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
zuOSwgzLq/YXiyJNPWGjICL0KrcqY8eXUxyiBgiihdg=
af60eb711bd85bc1e4d3e0a462e074eea428a8
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
nKZwK8oioxkTwDfG9V2sR2xNb9GbO72JaQ9OaUpmWGl7ZX+EiCwiESnhzEGly7cm
tJ+SvALjKnpAv9FF8u56pKKRS55/vzUDe+m9ct97Lx4=
gziBDgIPHk3UnbqAN9Ta9zRxJ8KBrTfiKBXyCZDQ588=
eEgPK4FD9N/fpMPwsM6h+Wvbqi3j4L5DBTwMY2KteC4=
hIbo0WHjc5N2XBD7HI+Mwh9BXu/nIzOhdTaHZ1DPjeizuR48SZNCpBdtOxY4cHlb
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
IcH9chIM8pdQBP/eeaIVQOxIkEFtHwPKwBzAXjYRdyw5KOKrZsfN3FYxHItVH2IL
JQeYWB/Ar5LqSSZ5i6IhxYZ+uXn8SEDYL9xPjgGTx2M=
CYcH4LBpiH+KaEScKuk48/IbmIORuaeHTHx2iwUA0vRWrbIkTWIgIbVYJ8eozDwX
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
bcd191accaa49d9ccc6e7b06598ffdb6
cc2751449a350f668590264ed76692694a80308a
AemuwIJaLmYE+nU5fadET3FINkdby4LnWDkawsC9pWk=
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
2ZUgS25mCfmBpvNAAnoop42ZvK9H4E17vIqHMHWBgDSruAgpJ0/PRWhyN3sqcUbC
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
FdxRYG9/HOndmgVdj1eVgDulreHUGSjsWl31nKn2TzY=

POSSIBLE SECRETS
6diiPm6leEU3dn6Yh3093iP+CyZAN47Ila9hmZbBOygAlbw7IfYBD8oUvevGhzQp
470fa2b4ae81cd56ecbcda9735803434cec591fa
0BurIdBwA1Yjcso9P1TmQgVgvpSOR3INLha4uP5JdYXgWQEacWBPKA8E9hy+9dAe
t0k+Q4WGODPCHlTh1fiMgaVG6LJXWEyq2lqorD4gMCo=
XE2927Ta6gTWmjrPmk4in7GLLwsXJnqTbhVN3N+/b3M=
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
8lD2ezwwsI93agi51tjtw1sdZVRU2vHPSc7HynOlFDE=
tk45mDotIpTZidmNYxxiIBsjVftw/e0h3Unlwpf2Me4=
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
U5Ngb8pPuPEbyAEAeNCt0wgGFK4YAtkNGCrOQKfD/ONzQcV8GTtSZ6EoO3NY8V1s
eISRjanjhAfdgJ9+lE3tGViJFRMvsuX1oVbmo+9k2XU=
0377caaa7ac435bea866027c1310860b
f+0D9BT8zkFXnX9yG742KHeQy11nhCJFb6PFndn+zMk=
W1peSRrFFzj+W6DyflucA6CQWTsphM4X4AkhjKjRy/o=
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
69psxaRqrIVZzPpt4pN0wGmA/kc6O8gjOJlblyEzW1E=
JHENilgoa32pdW2+FQZfbiKa1To+b6hAFc5hyxP6u/LWvHbIhkfTDC3kQMR4mpq3
lWYMNwupvIr4nCzhi63Y96rPhOxZK2U2oV0yQU5ISOuxDdywn/U6CBTwu78HOm4H
m4uJd6hJYeAUgFAUB1OT370Awen8YINd4hKC7XM/6ec=
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
d4INySQwKXrFgcw/Yp0O6t4YGx7HF+F75DncE44LSIy22mr4UP50R657OPRB1jqZ
F0+pSvx9GtXcjR12oFzzp5apK08MRky74IYez805WxvZBZTjFs672zxMax8w5kp9
df6b721c8b4d3b6eb44c861d4415007e5a35fc95

POSSIBLE SECRETS
hvOzu3pRF2dcNdvDy8db1rttL97bOQyvLLd+NabZhD5sRaprNsAQL2vdtDd+eY16
TOlHmdp8XsKJiprHSu957VTnJJL2Dj58ytcwt3QLHDQ=
wsk3Vojf7RmX+WtFiGWOJo7xhFKFeiDn9iUtTCe0eNY=
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
8UEA9TmdE+sqV3zcsNgnFI5Sf8uIsQHU61W37Ddl8zaNqY23x/FpuoK+mm9MWruA
m4BHDSYRnsEEIrYlgM0yy1C5NfyYnIIeJvwgjuCY5HY=
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
GZJYAQ87uqT/39Vw1xO4VkKaUA+BZKFiVkKasBC0VSw=
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
a1Na7bntM+sktGxZBhUnqailj8ITQ7piLQZ5OyqVU2HU4R0rOCZ63N/fUHG081A+
ChMYhePBDqkXl5DeRTg9cgSXXNPVEcIqgEVciYHEVlkZyx/HkVQXSnen8aw33G2s
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
CbnHJiUmcb7bV3nHtVfkQJESWUzuF9spYS2HkpVPEQ4sOQCQUFomcsL6vpMTm+JY
qlbJd0rViXaFpU2SvrkcezPlE/VtgXulMFWFUXmIBBg=
B3EEABB8EE11C2BE770B684D95219ECB
Q2oRzQFBrNQ6PISKRcfuekSxxMHiBiKCGVgSnsIVkCh9YR7J4L17zMBZU0VVyUEU
c103703e120ae8cc73c9248622f3cd1e
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333636353 65a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b

POSSIBLE SECRETS
pY1LPqV65osROa0AkcabhXHjwpz5nP0HOapDW2QtdtU=
ZqqofhkB4+yK9ARzF+IbcECpWBtuTXlqWFDkC/AVdcM=
Srq4/7DDafVhhxKPQvFzGwPCcbAxjsRhBUoTZMyZ8i1elMwCHCPiECib9I+dpg+U

PLAYSTORE INFORMATION

Title: Health Monitor: Sugar & BP

Score: 4.514563 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.gthreload.health.monitor.gp

Developer Details: DigitalSail (HK) Limited, 5910339767837763172, None, https://health-monitor-gp.web.app, gthreload@gmail.com,

Release Date: Oct 23, 2024 **Privacy Policy:** Privacy link

Description:

Discover a comprehensive wellness companion with Health Monitor: Sugar & BP Tracker. Empowers you to take control of your health with ease and convenience. Heart Rate Monitoring Measure your heart rate anytime, anywhere Blood Sugar Monitoring Keep track of your blood glucose levels. Blood Pressure Analysis Record and monitor your blood pressure. Blood Oxygen Recording Log your blood oxygen levels. Clear data analytics Analyze your heart rate, blood oxygen data and give you recommendations. Download now and start your journey to a healthier lifestyle today□ Privacy Policy□https://health-monitor-gp.web.app/privacy.txt Terms of Conditions□https://health-monitor-gp.web.app/privacy.txt Support Notes□https://health-monitor-gp.web.app/support.txt Disclaimer: All data and analyses provided by the app are for reference only and should not be used as a basis for medical diagnosis and treatment. We are not responsible for any consequences arising from the use of this app, including but not limited to health issues or inaccurate measurements.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 23:22:08	Generating Hashes	OK
2025-08-29 23:22:08	Extracting APK	OK
2025-08-29 23:22:08	Unzipping	OK
2025-08-29 23:22:09	Parsing APK with androguard	OK
2025-08-29 23:22:09	Extracting APK features using aapt/aapt2	OK
2025-08-29 23:22:09	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 23:22:11	Parsing AndroidManifest.xml	OK
2025-08-29 23:22:11	Extracting Manifest Data	OK

2025-08-29 23:22:11	Manifest Analysis Started	OK
2025-08-29 23:22:11	Performing Static Analysis on: Health Monitor (com.gthreload.health.monitor.gp)	OK
2025-08-29 23:22:11	Fetching Details from Play Store: com.gthreload.health.monitor.gp	OK
2025-08-29 23:22:12	Checking for Malware Permissions	OK
2025-08-29 23:22:12	Fetching icon path	OK
2025-08-29 23:22:12	Library Binary Analysis Started	OK
2025-08-29 23:22:12	Reading Code Signing Certificate	OK
2025-08-29 23:22:12	Running APKiD 2.1.5	OK
2025-08-29 23:22:16	Detecting Trackers	OK
2025-08-29 23:22:18	Decompiling APK to Java with JADX	OK
2025-08-29 23:22:32	Converting DEX to Smali	OK
2025-08-29 23:22:32	Code Analysis Started on - java_source	OK
2025-08-29 23:22:34	Android SBOM Analysis Completed	OK
2025-08-29 23:22:40	Android SAST Completed	OK
2025-08-29 23:22:40	Android API Analysis Started	OK
2025-08-29 23:22:45	Android API Analysis Completed	OK
2025-08-29 23:22:46	Android Permission Mapping Started	OK

2025-08-29 23:22:51	Android Permission Mapping Completed	OK
2025-08-29 23:22:51	Android Behaviour Analysis Started	OK
2025-08-29 23:22:57	Android Behaviour Analysis Completed	OK
2025-08-29 23:22:57	Extracting Emails and URLs from Source Code	OK
2025-08-29 23:22:58	Email and URL Extraction Completed	OK
2025-08-29 23:22:58	Extracting String data from APK	OK
2025-08-29 23:22:58	Extracting String data from Code	OK
2025-08-29 23:22:58	Extracting String values and entropies from Code	OK
2025-08-29 23:23:01	Performing Malware check on extracted domains	OK
2025-08-29 23:23:03	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.