MOBSF

ANDROID STATIC ANALYSIS REPORT

Blood Sugar & Pressure Tracker (1.3.2)

File Name:	net.magictool.bloodsugar_16.apk
Package Name:	net.magictool.bloodsugar
Scan Date:	Sept. 1, 2025, 2:50 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	15	2	1	1

FILE INFORMATION

File Name: net.magictool.bloodsugar_16.apk
Size: 16.52MB
MD5: 0e1bab485ca3a5d1f780dc765545fed7
SHA1: 8f43c3431657236342230e554f2b94e88a93b49d
SHA256: 0d3f91542739ea8fa5f866ba888520c4d1d765e4d2932b8e714e2867f721a557

APP INFORMATION

App Name: Blood Sugar & Pressure Tracker
Package Name: net.magictool.bloodsugar
Main Activity: net.magictool.bloodsugar.MainActivity
Target SDK: 34
Min SDK: 23

Max SDK:
Android Version Name: 1.3.2
Android Version Code: 16

APP COMPONENTS

Activities: 8
Services: 15
Receivers: 17
Providers: 5
Exported Activities: 0
Exported Services: 1
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
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: 2024-03-12 07:19:30+00:00
Valid To: 2054-03-12 07:19:30+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x6991eff8f7306115d97ea212b50f820d0499dfa9
Hash Algorithm: sha256
md5: b5241ecae8e8a8f802a246901b19ae4d
sha1: 6b6610385f3f36e9dc9f6bcf70b9fb7d233cccce
sha256: 760dc75cf891282b9511b37b7cd601ca855b30dc7453e2c4efe5f103e4fbe224
sha512: 71289bcc22a16242298093c417ed91517a9c116ed435195361e4d381e59955ff9bb2e83056ca54de4d582764adec2700a670a1f8707577acbe7da4d20357585b
PublicKey Algorithm: rsa
Bit Size: 4096

Fingerprint: 1279be21e8a983d89640b81ab9acc30bfe7cd7ecc20ac540840b453f2960eb65
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
net.magictool.bloodsugar.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator 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.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name 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>

FILE	DETAILS
classes3.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
net.magictool.bloodsugar.MainActivity	Schemes: bloodsugar://, https://, Hosts: open, aesji.app.link, aesji-alternate.app.link, aesji.test-app.link, aesji-alternate.test-app.link,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 6 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) 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.
4	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.
5	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
6	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.
7	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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: **0** | WARNING: **6** | INFO: **2** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a2/b.java c2/a0.java c2/b.java c2/o0.java c2/p1.java c2/r1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c2/f1.java c2/z1.java c5/b.java com/aliyun/sls/android/producer/LogProducerHttpTool.java com/dexterous/flutterlocalnotifications/ActionBroadcastReceiver.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/ScheduledNotificationReceiver.java d2/g.java d4/a.java d5/c0.java d5/e0.java d5/i.java e0/e1.java e0/w0.java e4/j.java f3/c.java g/d.java g0/s0.java g5/d.java h1/d.java i3/e.java i3/i.java io/flutter/plugins/camerax/k0.java io/flutter/plugins/camerax/p0.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundService.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java io/flutter/plugins/inapppurchase/e.java io/flutter/plugins/pathprovider/a.java io/flutter/plugins/sharedpreferences/a.java io/flutter/plugins/urllauncher/b.java io/flutter/plugins/webviewflutter/o.java j/e.java j/i.java j/j.java

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	j/i.java j8/e.java k1/f.java l6/n.java m1/a.java m3/c.java m6/a.java m6/d0.java m6/e.java n/g.java n1/j.java n5/d0.java n5/h.java o/c.java o1/a.java o6/b.java o6/e.java o6/f0.java o6/g0.java o6/j0.java o6/l.java o6/q.java o6/v.java o6/x.java o6/y.java p/e0.java p/h1.java p/i1.java p/k1.java p/r0.java p/u.java p/u0.java p/v0.java p/y0.java p/z0.java p3/a.java p5/c.java p6/a.java p6/d.java q1/e.java q1/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				q1/n.java q1/p.java q1/p1.java q1/t0.java q2/a.java q3/g.java q5/b.java q6/f.java r1/a.java r4/c.java s0/a0.java s1/c.java s1/d.java s1/h.java s2/f0.java s2/i0.java s2/k0.java s2/l0.java s2/n.java s2/n0.java s2/y.java t1/c.java t1/e.java t1/f.java t1/g.java t1/k.java t2/c.java t6/c0.java u/c.java u0/d.java u2/a.java u4/a.java v3/a.java v3/e.java v4/a.java v4/q.java v4/s.java v4/u.java v6/c.java y1/i.java y2/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				y3/f.java y3/g.java z1/e.java
2	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/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/isolate/IsolatePreferences.java com/dexterous/flutterlocalnotifications/models/NotificationDetails.java t6/b0.java u/b.java
3	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	d5/i.java n3/a.java
4	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	io/flutter/plugins/pathprovider/a.java r1/i.java s6/h.java
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	g0/u.java i3/i.java io/flutter/plugins/camerax/f1.java io/flutter/plugins/camerax/h0.java q2/a.java
6	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	j$/util/concurrent/ThreadLocalRandom.java o7/a.java o7/b.java p7/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/editing/d.java io/flutter/plugin/platform/g.java n5/t0.java
8	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	j5/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java g5/d.java io/flutter/plugins/urllauncher/a.java n5/d.java n5/n.java p5/b.java u/c.java v4/a.java v4/q.java v4/u.java
00022	Open a file from given absolute path of the file	file	g0/u.java i3/i.java io/flutter/plugins/camerax/h0.java io/flutter/plugins/pathprovider/a.java k3/a.java l2/l.java n3/b.java q2/a.java v5/f.java w0/s0.java
00013	Read file and put it into a stream	file	com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java g0/u.java i3/i.java i7/g.java k3/c.java l2/l.java q1/g.java q2/a.java t1/e.java t1/k.java
00209	Get pixels from the latest rendered image	collection	j8/e.java r5/p.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/aliyun/sls/android/producer/LogProducerHttpTool.java n5/q.java
00109	Connect to a URL and get the response code	network command	com/aliyun/sls/android/producer/LogProducerHttpTool.java n5/q.java
00153	Send binary data over HTTP	http	com/aliyun/sls/android/producer/LogProducerHttpTool.java
00029	Initialize class object dynamically	reflection	v2/h.java
00012	Read data and put it into a buffer stream	file	q2/a.java
00036	Get resource file from res/raw directory	reflection	com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java g5/d.java n5/d.java p/y0.java v4/a.java v4/q.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	io/flutter/plugins/urllauncher/a.java n5/d.java v4/a.java v4/q.java v4/u.java
00161	Perform accessibility service action on accessibility node info	accessibility service	d2/g.java io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/f.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	d2/g.java io/flutter/view/AccessibilityViewEmbedder.java

RULE ID	BEHAVIOUR	LABEL	FILES
00210	Copy pixels from the latest rendered image into a Bitmap	collection	r5/p.java
00202	Make a phone call	control	v4/u.java
00203	Put a phone number into an intent	control	v4/u.java
00091	Retrieve data from broadcast	collection	n5/d.java s4/v2.java
00123	Save the response to JSON after connecting to the remote server	network command	n5/q.java
00089	Connect to a URL and receive input stream from the server	command network	n5/q.java
00030	Connect to the remote server through the given URL	network	n5/q.java
00094	Connect to a URL and read data from it	command network	n5/q.java
00108	Read the input stream from given URL	network command	n5/q.java
00121	Create a directory	file command	r1/a.java
00125	Check if the given file path exist	file	r1/a.java
00078	Get the network operator name	collection telephony	n5/v0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00175	Get notification manager and cancel notifications	notification	q1/t0.java
00147	Get the time of current location	collection location	j/l.java
00075	Get location of the device	collection location	j/l.java
00115	Get last known location of the device	collection location	j/l.java
00191	Get messages in the SMS inbox	sms	p/y0.java
00079	Hide the current app's icon	evasion	o4/e.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/1016321674360/namespaces/firebase:fetch?key=AIzaSyCWPIYuRYB96pIb38zWWHLIpWbEQ3rXxJY. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.RECEIVE_BOOT_COMPLETED, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.VIBRATE
Other Common Permissions	4/44	com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE

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

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
help.branch.io	ok	**IP:** 104.18.20.218 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
docs.flutter.dev	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
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
bnc.lt	ok	**IP:** 18.238.109.50 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api2.branch.io	ok	**IP:** 18.238.96.83 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cdn.branch.io	ok	**IP:** 18.238.109.81 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
branch.app.link	ok	**IP:** 18.238.109.80 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
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
"google_api_key" : "AIzaSyCWPIYuRYB96pIb38zWWHLIpWbEQ3rXxJY"
"google_crash_reporting_api_key" : "AIzaSyCWPIYuRYB96pIb38zWWHLIpWbEQ3rXxJY"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
vDxCHtRyDtZtywG/lqG2i2wEAK0QRlsYMxcEu2Y9QxY=
yTyv47DW9aV6rpyU1wL04puCd80cKdCTVtCqLwFmVTX0TBccJdZ4Z0bBqZNN3F0R
fY7ocyET9PuMHUXxIlKP/PpFa5xsSzhwfB8mpep5FSQ=
uqJEUYtMC6igyTZFAAEE75NBgASQTYxYWvVnS4oyIqiXJPhpeFyV9nSFbcfeIJKd
470fa2b4ae81cd56ecbcda9735803434cec591fa
FlygBXZrpziR+Pp2xmzyZ9k6GUcrj9kWbY5XuUd40ERy2hxHTKqhUwfuGSusXUTd
1eASkBAriCqBxPWd4okyyc+CHCTvdkAuw8U5qBN0KobaC6TQVXZIuItjy1xo8n06
JFMtS6Z9bzmnMwoeWTxjTTnvJVVZDuewSTBrvx9CdBc=
NnIoFyYmTm9Yd/i5F1TZFAo2tPeZkpFEZBtgPBr60Ow=
8HOKLqLOucCjn3kWyyKimNsF6Dcutdd9y3ap015kDIWZNsgYbLJqzHSzKo+jDSQ4
TdQDsqdcAU8jyTN6NihYJULAUxAJpTfNWWUTPnMXLns=

POSSIBLE SECRETS
49f946663a8deb7054212b8adda248c6
UrsneQ7OIRNo8EjOO9YdieQqewqlcsXgRCgjv7EyHmQ=
Gt05wlkB9VlCQDpYnwS+bvW/Sf4rdLdhAuNRhSCvQ2I=
0kr13TIqRr0Mkim2K4wTtB+PeWlqdIn0V95/3g6ojAuM6jvjN6OT9QeeEcwm9v6h
pkxrOWj7zD1ScyeXlo8fp1m52MhBIE9QvURtfE4hxB81XVp6EbBK8CYQjvvhYlf1
sgSNHgqJ9EwYu8w2dMx3zRGSIiO9D1spUgPO3F51srA=
af60eb711bd85bc1e4d3e0a462e074eea428a8
5gR2Yi2k1qmqwB908rtZUebo4TzAbjEGSkWYIuNbRdnGPocO4kIxU9dsn2qP+c0J
3ikNbWzMTIqU222KtrzzFiiUcpXtNPU8upxs9wXDAJYxbW4sx23+rx4eBiJjRteZ
JZBFNEdYFhTFBTCRgtU3dDnkdlKXmKLHUW9VyRRgLZX35JOvzKEIQuHunyCpcG/w

POSSIBLE SECRETS
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
GajzmnIGCWKypTldGXdzGSwHW6ZZV69Bh6cWfmyAJmA=
36864200e0eaf5284d884a0e77d31646
5UR6HKB81c0cBAmhqUCkwnSn0PivsbvOC36lSRnvbJazdJtsmM3DNCGH8hJ11MS9
lVUtMgOC8oCk0OL1R8+dcIzJX9C75UT4Pn6J82++vFrHU4GwQD+682Yf0fGqttpS
OfZFeGMpPN4nP2QoVlOsW4kmNx194lMXDh8YPc+yAeg=
pwlWlXowmv5MgDBY81mya6zXLrSMULDo97qGgXQvfFI=
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f

POSSIBLE SECRETS
skGQhdInPY4sBMicxMlDA8FpM67X6t386GsGM5hjG6o=
B3EEABB8EE11C2BE770B684D95219ECB
qmKK3b5gFczPFV6EXQK4o/dThX0H+NXEfphwaNTcj5pJFkabLh1X9vORrSfnOkeV
3Dv+WIEpWKEbBzcuP3SgLUV0aXQTnDSdpPKu/RzIzoY=
7Ejn4kVFfkIwTENQCsQUmu0CsZi/nLRRU7QLVgsNDkU=
EByWffqzraQVS82Db2+ro2d9ZqC8EsuKj9igHJ6rpI4=
Q54q2JslusSv8X8AsH7nKgnoWyF6GsnL4uj/9o5E5cc=
t30h8UZEoZP8GE77k4AdlDjTvNQpvs7DHs10k6C9ZzU=
t4LignzpQnyAJJAZeU8P3GGD0dgmuTMT4n9grwU+EMc=
c103703e120ae8cc73c9248622f3cd1e
RRAtLSPp4UfCvUq8TqKgqVcK2MQ98P/X8fWWJOdf6yU=
gWtAtoadyS/0GQFYvFINsjkt4bRjT5fE+w3tC36yAJU=
bVq06mwryvswJ9TEv8eKHMxwi9DjT7SQH2xL+admUqskqroPQT0vVkasNMzV5jv7
b4xBpY1Zr7toyC1sOTTNBO4ImhCct0sLu70B1nFUAHo=

POSSIBLE SECRETS
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071 30d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b13 07416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613 616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930 3132333336353 65a308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301 406035504071307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031 307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636 f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314 dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990 c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee 165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf 2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76 c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe 5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e69613116301406035504071307416e64726f69643110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d01010405000382010010019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
8mLoio5zXFzLNZDTURhMAugjCGrSPBhh3GCaf2t8mPk=
s/IaC73MjD9vpfzZvssIGR7eelXzGompBCRU9Px19GF39ZofYoD29ElcUTZqSvpM
ikPkuPQbpnIYaQGo6Ao4zzPX0Qaf9HhmEZeT4ZfFQOg=
19nlSd1PMyXKl1niHXaxZmvGyLnyitkJHQnkLHtPHLj6n1sor4NdBFlTmnlba7BL
flTy8eyNabiNCHuPyNX0x482LGXuzWIuGD/71SlN2nKRI9kSJNQ0LUuMwsl06lrx
a0784d7a4716f3feb4f64e7f4b39bf04
AjndXp1s5xIDXysf7TNVubDac7r00lcAtHKozpGmJzQ=

POSSIBLE SECRETS
nCcHhBJ+r5jDr0ERNbOfBIJ/pDQFZIqvHaO2vAiQNRE=
bae8e37fc83441b16034566b
MyezUX/G4B4IwyhTDkP3w1lDN+jx4NQ6UyU5K5beVZyubOhn8Q7qD9UAXT+3eaCC
nv6PiabX0G4RLHtriKodA9C0rOBToujvB9ySFMp3wxE=

PLAYSTORE INFORMATION

Title: Blood Sugar & Pressure Tracker

Score: 4.4224424 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** net.magictool.bloodsugar

Developer Details: Hangzhou Suoyi Network Technology Co., Ltd., Hangzhou+Suoyi+Network+Technology+Co.,+Ltd., None, https://magictool.net/bloodsugar/protocol/privacy.html, sharploit@gmail.com,

Release Date: Mar 12, 2024 **Privacy Policy:** Privacy link

Description:

With Blood Sugar & Blood Pressure Tracker APP, you'll monitor and record your blood pressure and blood sugar levels easily.empowering you to take control of your health. Here's what Blood Sugar & Blood Pressure Tracker APP can do for you: Comprehensive Blood Sugar Tracking - Easily log your blood sugar and measurements, ensuring you stay informed about your glucose levels. - Track both fasting and post-meal blood sugar readings effortlessly. Efficient Blood Pressure Monitoring - Gain a deeper understanding of your cardiovascular well-being by seamlessly logging your blood pressure measurements. - Effortlessly monitor your systolic and diastolic blood pressure readings, ensuring a holistic approach to managing your overall health and wellness. In-depth Analysis: - Analyze your blood sugar trends over time with detailed charts and graphs, allowing you to make informed decisions about your health. Timely Medication Alerts - Customize medication reminders to ensure you never miss a dose. Set up personalized alerts to prompt timely intake of medications, ensuring adherence to your treatment plan. Health Information - Expand your knowledge of health-related topics including blood pressure and blood glucose management. Access valuable information to support your journey towards better health. NOTE: - This app supports the recording of health indicators and does not directly measure blood pressure or glucose levels. - Tips provided in the app are for reference purposes only. - This app is not a substitute for professional medical equipment. - If you have any medical concerns or suspect a heart condition, please consult a doctor promptly. We value your feedback! Download Blood Sugar & Blood Pressure Tracker APP and let us know how we can improve your experience. Your health is our priority!

SCAN LOGS

Timestamp	Event	Error
2025-09-01 14:50:16	Generating Hashes	OK
2025-09-01 14:50:16	Extracting APK	OK
2025-09-01 14:50:16	Unzipping	OK
2025-09-01 14:50:16	Parsing APK with androguard	OK
2025-09-01 14:50:17	Extracting APK features using aapt/aapt2	OK
2025-09-01 14:50:17	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 14:50:18	Parsing AndroidManifest.xml	OK
2025-09-01 14:50:18	Extracting Manifest Data	OK
2025-09-01 14:50:18	Manifest Analysis Started	OK

2025-09-01 14:50:19	Performing Static Analysis on: Blood Sugar & Pressure Tracker (net.magictool.bloodsugar)	OK
2025-09-01 14:50:21	Fetching Details from Play Store: net.magictool.bloodsugar	OK
2025-09-01 14:50:22	Checking for Malware Permissions	OK
2025-09-01 14:50:22	Fetching icon path	OK
2025-09-01 14:50:22	Library Binary Analysis Started	OK
2025-09-01 14:50:22	Reading Code Signing Certificate	OK
2025-09-01 14:50:23	Running APKiD 2.1.5	OK
2025-09-01 14:50:27	Detecting Trackers	OK
2025-09-01 14:50:30	Decompiling APK to Java with JADX	OK
2025-09-01 14:50:59	Decompiling with JADX failed, attempting on all DEX files	OK

2025-09-01 14:50:59	Decompiling classes2.dex with JADX	OK
2025-09-01 14:51:07	Decompiling classes.dex with JADX	OK
2025-09-01 14:51:15	Decompiling classes3.dex with JADX	OK
2025-09-01 14:51:17	Decompiling classes2.dex with JADX	OK
2025-09-01 14:51:24	Decompiling classes.dex with JADX	OK
2025-09-01 14:51:32	Decompiling classes3.dex with JADX	OK
2025-09-01 14:51:34	Converting DEX to Smali	OK
2025-09-01 14:51:34	Code Analysis Started on - java_source	OK
2025-09-01 14:51:36	Android SBOM Analysis Completed	OK
2025-09-01 14:51:41	Android SAST Completed	OK

2025-09-01 14:51:41	Android API Analysis Started	OK
2025-09-01 14:51:45	Android API Analysis Completed	OK
2025-09-01 14:51:45	Android Permission Mapping Started	OK
2025-09-01 14:51:49	Android Permission Mapping Completed	OK
2025-09-01 14:51:50	Android Behaviour Analysis Started	OK
2025-09-01 14:51:57	Android Behaviour Analysis Completed	OK
2025-09-01 14:51:57	Extracting Emails and URLs from Source Code	OK
2025-09-01 14:51:58	Email and URL Extraction Completed	OK
2025-09-01 14:51:58	Extracting String data from APK	OK
2025-09-01 14:51:58	Extracting String data from Code	OK
2025-09-01 14:51:58	Extracting String values and entropies from Code	OK

2025-09-01 14:52:01	Performing Malware check on extracted domains	OK
2025-09-01 14:52:02	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.