ANDROID STATIC ANALYSIS REPORT

app_icon

Health Connect

(2024.11.28.00.release)

File Name:	com.google.android.apps.healthdata_167158.apk
Package Name:	com.google.android.apps.healthdata
Scan Date:	Aug. 29, 2025, 11:15 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	24	2	2	1

FILE INFORMATION

File Name: com.google.android.apps.healthdata_167158.apk
Size: 6.99MB
MD5: c8f6ea1435602abde1e0f063213f831e
SHA1: 3159a7c95b039a21d79ca7e56aa19f79f0ca12f5
SHA256: f033d0e5975e4d937a22695cdc618121d4c3572fb7a4e3f8ef4b64a18d753668

APP INFORMATION

App Name: Health Connect
Package Name: com.google.android.apps.healthdata
Main Activity:
Target SDK: 35
Min SDK: 28
Max SDK:
Android Version Name: 2024.11.28.00.release

Android Version Code: 167158

APP COMPONENTS

Activities: 12
Services: 16
Receivers: 18
Providers: 2
Exported Activities: 6
Exported Services: 4
Exported Receivers: 4
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
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: 2021-11-01 17:26:21+00:00
Valid To: 2051-11-01 17:26:21+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x46d28279dd7450ba04446457757075d9ed254181
Hash Algorithm: sha256
md5: e387b32a00620d7770b4ac3dc2c99370
sha1: 2e14d810f4f0246f4b6612a011933e0a3164b8d4
sha256: b2c0a80e485934bfb08f902ca27505813df3159e4e6dd4a4df078d66cb1c2003
sha512: 4a0177d82bd6c2fcaed1ee73c1ddf0481ac7e41771baabeeec93a62f5dd8c693a8ab6d3e804a3c65199591e37904311eb94c6b3af72ef005e31ff1afde6afce7
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 2816674776396b093f7d2be6fb078d041bc720c04d4a7220075ebf77728c928d
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.GET_PACKAGE_SIZE	normal	measure application storage space	Allows an application to find out the space used by any package.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.MIGRATE_HEALTH_CONNECT_DATA	unknown	Unknown permission	Unknown permission from android reference
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.google.android.apps.healthdata.permission.START_ONBOARDING	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
c8f6ea1435602abde1e0f063213f831e.apk	FINDINGS: Anti Disassembly Code — DETAILS: illegal class name

<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.MANUFACTURER check
Build.HARDWARE check
Build.TAGS 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>
<tr><td>Anti Disassembly Code</td><td>illegal class name</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

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: 17 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
3	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Service (com.google.android.apps.healthdata.home.phone.quicksettings.QuickSettingsService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_QUICK_SETTINGS_TILE [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-Alias (com.google.android.apps.healthdata.SettingsActivity1) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Activity-Alias (com.google.android.apps.healthdata.SettingsActivity2) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Content Provider (com.google.android.apps.healthdata.home.phone.searchindexables.HealthConnectSearchIndexablesProvider) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.READ_SEARCH_INDEXABLES [android:exported=true]	warning	A Content Provider 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
8	Service (com.google.android.apps.healthdata.service.androidx.HealthCoreService) is not Protected. [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.
9	Broadcast Receiver (com.google.android.libraries.phenotype.client.stable.AccountRemovedBroadcastReceiver) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
10	Broadcast Receiver (com.google.android.libraries.phenotype.client.stable.PhenotypeUpdateBackgroundBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.PHENOTYPE_UPDATE_BROADCAST [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.
11	Activity (com.google.android.libraries.social.licenses.LicenseMenuActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
12	Broadcast Receiver (com.google.apps.tiktok.experiments.phenotype.ConfigurationUpdatedReceiver_Receiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.PHENOTYPE_UPDATE_BROADCAST [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.
13	Activity (com.google.apps.tiktok.nav.gateway.GatewayActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
14	Activity-Alias (com.google.android.apps.healthdata.deeplink.DefaultGateway) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
15	Activity-Alias (com.google.android.apps.healthdata.deeplink.ShowMigrationInfo) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.MANAGE_HEALTH_DATA [android:exported=true]	warning	An Activity-Alias 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
16	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
17	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: **0** | WARNING: **6** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/aa.java defpackage/aac.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/aga.java defpackage/agi.java defpackage/agl.java defpackage/agy.java defpackage/akb.java defpackage/ako.java defpackage/akz.java defpackage/anj.java defpackage/anu.java defpackage/anz.java defpackage/aqg.java defpackage/arg.java defpackage/atm.java defpackage/auz.java defpackage/aze.java defpackage/bdw.java defpackage/beg.java defpackage/beo.java defpackage/bfd.java defpackage/bhm.java defpackage/bht.java defpackage/biu.java defpackage/bja.java defpackage/bkb.java defpackage/bks.java defpackage/bn.java defpackage/bty.java defpackage/bw.java defpackage/bwg.java defpackage/bwu.java defpackage/bxy.java defpackage/cle.java defpackage/cnk.java defpackage/co.java defpackage/dbp.java defpackage/dcx.java defpackage/dhg.java defpackage/di.java defpackage/dir.java defpackage/dis.java defpackage/djk.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/djl.java defpackage/djz.java defpackage/dka.java defpackage/dkl.java defpackage/dko.java defpackage/dks.java defpackage/dkt.java defpackage/dle.java defpackage/dlq.java defpackage/dmc.java defpackage/dmj.java defpackage/dmm.java defpackage/dnd.java defpackage/dni.java defpackage/dnn.java defpackage/dnp.java defpackage/dns.java defpackage/dnx.java defpackage/dny.java defpackage/doc.java defpackage/dod.java defpackage/doj.java defpackage/dol.java defpackage/dpn.java defpackage/dpu.java defpackage/dpx.java defpackage/dqe.java defpackage/dqm.java defpackage/dqn.java defpackage/dqs.java defpackage/drb.java defpackage/dro.java defpackage/dry.java defpackage/dsc.java defpackage/dse.java defpackage/dsm.java defpackage/dsn.java defpackage/dtw.java defpackage/due.java defpackage/dvw.java defpackage/dyz.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	defpackage/dyp.java defpackage/dyq.java defpackage/dyy.java defpackage/dz.java defpackage/dzm.java defpackage/dzz.java defpackage/ebo.java defpackage/edm.java defpackage/edn.java defpackage/eed.java defpackage/efq.java defpackage/eht.java defpackage/ekh.java defpackage/emw.java defpackage/enq.java defpackage/etg.java defpackage/etp.java defpackage/eus.java defpackage/eux.java defpackage/euz.java defpackage/evh.java defpackage/evk.java defpackage/ewa.java defpackage/ex.java defpackage/ey.java defpackage/ezj.java defpackage/ezm.java defpackage/ezn.java defpackage/ezo.java defpackage/ezp.java defpackage/fct.java defpackage/fed.java defpackage/fhv.java defpackage/fiw.java defpackage/flo.java defpackage/fnb.java defpackage/fq.java defpackage/fqv.java defpackage/ftw.java defpackage/fwu.java defpackage/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/gaw.java defpackage/gbh.java defpackage/gbu.java defpackage/gch.java defpackage/gci.java defpackage/gcy.java defpackage/gdu.java defpackage/gdz.java defpackage/gfa.java defpackage/ggm.java defpackage/gjk.java defpackage/gtu.java defpackage/gwt.java defpackage/gxc.java defpackage/gxf.java defpackage/gxg.java defpackage/gxm.java defpackage/gym.java defpackage/hfe.java defpackage/hff.java defpackage/hfg.java defpackage/hix.java defpackage/ht.java defpackage/ig.java defpackage/ike.java defpackage/ikp.java defpackage/ikr.java defpackage/ikv.java defpackage/jq.java defpackage/kg.java defpackage/kp.java defpackage/kr.java defpackage/kv.java defpackage/li.java defpackage/lz.java defpackage/mh.java defpackage/nf.java defpackage/pk.java defpackage/qm.java defpackage/qs.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				defpackage/rc.java defpackage/rl.java defpackage/sa.java defpackage/sd.java defpackage/so.java defpackage/ss.java defpackage/su.java defpackage/sv.java defpackage/sx.java defpackage/ta.java defpackage/tr.java defpackage/ug.java defpackage/vp.java defpackage/vv.java defpackage/w.java defpackage/wq.java defpackage/xq.java defpackage/xr.java defpackage/z.java defpackage/zi.java defpackage/zk.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	defpackage/cby.java defpackage/cla.java defpackage/clc.java defpackage/clt.java defpackage/clu.java defpackage/ddz.java defpackage/edx.java defpackage/ehc.java defpackage/ejx.java defpackage/ejz.java defpackage/elc.java defpackage/epm.java defpackage/ero.java defpackage/erq.java defpackage/ert.java defpackage/esb.java defpackage/esc.java defpackage/gjk.java defpackage/glv.java defpackage/glw.java defpackage/glx.java defpackage/gua.java defpackage/gvb.java defpackage/hxx.java defpackage/hxy.java defpackage/hxz.java defpackage/hyd.java j$/util/concurrent/ThreadLocalRandom.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	defpackage/awe.java defpackage/bav.java defpackage/bcf.java defpackage/bcz.java defpackage/bdh.java defpackage/bop.java defpackage/epa.java defpackage/evr.java defpackage/fvx.java defpackage/fxs.java
4	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	defpackage/anr.java defpackage/cpr.java defpackage/cvn.java defpackage/fcc.java
5	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	defpackage/ajt.java
6	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	defpackage/heq.java
7	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	defpackage/ezx.java
8	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	defpackage/atn.java defpackage/dqs.java defpackage/z.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	defpackage/eoh.java defpackage/etg.java defpackage/fot.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	defpackage/aa.java defpackage/bab.java defpackage/bao.java defpackage/bap.java defpackage/bfh.java defpackage/ecf.java defpackage/enb.java defpackage/enx.java defpackage/eqn.java defpackage/etg.java defpackage/faa.java defpackage/fah.java defpackage/faz.java defpackage/su.java defpackage/sv.java defpackage/zk.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	defpackage/agk.java defpackage/agl.java defpackage/bze.java defpackage/ctj.java defpackage/cux.java defpackage/cyu.java defpackage/dkb.java defpackage/dyp.java defpackage/geu.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	defpackage/agk.java defpackage/agl.java defpackage/bze.java defpackage/ctj.java defpackage/cux.java defpackage/dkb.java
00036	Get resource file from res/raw directory	reflection	defpackage/agk.java defpackage/bfd.java defpackage/ctj.java defpackage/dkb.java defpackage/eti.java defpackage/geu.java
00091	Retrieve data from broadcast	collection	defpackage/auf.java
00079	Hide the current app's icon	evasion	defpackage/aya.java defpackage/cnt.java
00022	Open a file from given absolute path of the file	file	defpackage/alm.java defpackage/esn.java defpackage/ezx.java defpackage/z.java

RULE ID	BEHAVIOUR	LABEL	FILES
00075	Get location of the device	collection location	defpackage/bvo.java
00137	Get last known location of the device	location collection	defpackage/bvo.java
00187	Query a URI and check the result	collection sms calllog calendar	defpackage/djk.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	defpackage/djk.java
00024	Write file after Base64 decoding	reflection file	defpackage/rl.java
00012	Read data and put it into a buffer stream	file	defpackage/zk.java
00089	Connect to a URL and receive input stream from the server	command network	defpackage/bbo.java
00030	Connect to the remote server through the given URL	network	defpackage/bbo.java
00109	Connect to a URL and get the response code	network command	defpackage/bbo.java
00044	Query the last time this package's activity was used	collection reflection	defpackage/ctz.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET
Other Common Permissions	2/44	android.permission.FOREGROUND_SERVICE, android.permission.PACKAGE_USAGE_STATS

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
developer.android.com	ok	**IP:** 64.233.176.113 **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.
support.google.com	ok	**IP:** 64.233.177.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
plus.google.com	ok	**IP:** 64.233.185.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	defpackage/dkh.java

HARDCODED SECRETS

POSSIBLE SECRETS
"mindful_session_label" : "Mindfulness"
"sleep_session_with_one_field" : "%1$s"
06e4dca59c10391acc89a9514e9775f2f049a657-
CnQKMmNvbS5nb29nbGUuYW5kcm9pZC5hcHBzLmhlYWx0aGRhdGEudGVzdGluZy50ZXN0YXBwEj4KBwjnDxAIGAoSM2h0dHBzOi8vc3VwcG9ydC5nb29nbGUuY29tL2FuZHJvaWQ/cD1nZXRfc3RhcnRlZF9oYw
1cbd3130fa23b59692c061c594c16cc0
a-95ed6082-b8e9-46e8-a73f-ff56f00f5d9d
Ci1jb20uZ29vZ2xlLmFuZHJvaWQucHJpbWVzLWphbmstJVBBQ0tBR0VfTkFNRSUSIwgCEh9KPCVFVkVOVF9OQU1FJT4jbWlzc2VkQXBwRnJhbWVzEh8IAxIbSjwlRVZFTlRfTkFNRSU+I3RvdGFsRnJhbWVzEiYIBRIiSjwlRVZFTlRfTkFNRSU+I21heEZyYW1lVGltZU1pbGxpcw
86254750241babac4b8d52996a675549

POSSIBLE SECRETS

Ch9jb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5maXRuZXNzChtjb20uc2VjLmFuZHJvaWQuYXBwLnNoZWFsdGgKF2NvbS5maXRiaXQuRml0Yml0TW9iaWxlChFjb20ub3VyYXJpbmcub3VyYQoVY29tLndpdGhpbmdzLndpc2NhbGUyChdjb20ub25lcGVsb3Rvbi5jYWxsaXN0bwoZY29tLndlaWdodHdhdGNoZXJzLm1vYmlsZQoXY29tLnNpbGxlbnMuc2hhcGV1cGNsdWIKFWNvbS5oZWFsdGhpZnltZS5iYXNpYwoYY29tLm15Zml0bmVzc3BhbC5hbmRyb2lkChdubC5hcHB5aGFwcHMuaGVhbHRoc3luYwoTY29tLm9jdWx1cy50d2lsaWdodA

Ch4KE0NhcmUuY2FyaXR5LmFwcF9kZXYSBxoFBB0eBxEKIQoaSnAuam95Zml0LmpveWZpdGFwcGFuZHJvaWQSAxoBBgojChxKcC5ub2J1Y29ycG9yYXRpb24uaGVpYW53YWxrEgMaAQYKGgoPYWUubTQyLnN1cGVyYXBwEgcaBRsEGQYRCikKFWFwcC5hZXN0aGV0aWNzYWR2aXNvchIQGgkBCgIdDRkGIxEiAwEdIwopCg9hcHAuYnBqcy5tb2JpbGUSFhoUAQkaGwocAgQFHQ0XGB8gIiUGIxEKFQoOYXBwLm1vdmV2by5wc3oSAxoBBgofChBhcHAubW92ZXZvLnNhcHBpEgsaCQIDBCcFJCUGCAofChVhcHAud2VpZ2h0Zml0LmFuZHJvaWQSBhoEBSIBEQojChlhc2lhLmNyb2l4LmFwcC5yZWxheHdvcmxkEgYaBAEEGQYKFQoNYmlrZS5jb2JpLmFwcBIEIgICBAovCiVici5jb20ucmRzYXVkZS5oZWFsdGhQbGF0Zm9ybS5hbmRyb2lkEgYaBAINBhEKHgoTY2FzZS5jYXJpdHkuYXBwX2RldhIHGgUEHR4HEQoaCg9jYXJlLmdvb2RheS5hcHASBxoFAQIEBiMKGAoMY2MuaXNz aW4uc2JtEggaAgYRIgIGEQoZCg5jYy5pc3Npbi5zcG9ydBIHGgIdBiIBHQodChZjby5jaG9vc2VicmlnaHQuY2xpZW50EgMaAQYKKgoPY28ud2VsbC53ZWxsYXBwEhcaFQEJGhsKAgQFHR4NFxgkIhklBiMHEQoqCh9jb20uYWJzb2x1dGVseWRpZ2l0YWwuc3RlcGNoYWluEgcaAgEGIgEGChgKEGNvbS5hZGFlZmZzZTIwMjESBBoCAgYKGAoRY29tLmFkYWVqdXJpczIwMjESAxoBBgoXChBjb20uYWRhZW5mbGkyMDIxEgMaAQYKNAoaY29tLmFkdm1lZHMubXBocmFwcF90YWluYW4SFhoUASEJGhsKHAsMHR4NHyAiGSUGIxEKFQoOY29tLmFsYW5tb2JpbGUSAxoBBgoPCghjb20uYWxppeBIDGgEGChcKDGNvbS5hbHRlcl92MhIHGgERIgIEHQoeChZjb20uYW5hbW5lLm91Y2hpYnlnvdWluEgQaAhkGCiIKGmNvbS5hbmFtbmUub3VjaGlieW91aW4uc3RnEgQaAhkGChoKDmNvbS5hcHAuZml0YWdlEggiBgkKCwwdEQoWCgpjb20uYXBwLmdlEggiBgkKCwwdEQosCiVjb20uYXBwLnJlYWxmaXR6Y2xpZW50YW5kcm9pZC5maXRuZXNzEgMaAQYKLgoeY29tLmJlbmVmaXR0ZWNobm9sb2dpZXMuYmVmaXQEgwaBAQdBhEiBAQdBhEKIAoYY29tLmJld HRlcmxpZmUuU3RlcG9ncmFtEgQaAgIGChcKDmNvbS5iZXR0ZXJ0aW1lEgUaAwQZBgodCg9jb20uYmV4b21lLmVnaGkSChoIARsKHB0ZBhEKJQoaY29tLmJyaXNrbG9uZ2V2aXR5LmFuZHJvaWQSBxoFAgQdGQYKLQoTY29tLmJ1enVkLmdmYWlmdmljZRIWGhQBIQkaGwocAgQdHg0PHyAiGQYjEQorCg1jb20uYndzLmFwcHYyEhoaGAEJGCgsMAgEECAwQnBR0eDRcPGB8kICIZBiMHEQomChhjb20uY2FsbGNhcmUuYW5kcm9pZC5mcGhvbmVpcGNhAgEGCgYKGAoRY29tLmNhbGxvcmllLmRlbW8SBhoEBQYRCj gYKG4wKBMHEQoXCj4KHWNvbS5jaGFwbWVjaC5ocGZ0aGNhcmUuaGxkZWx0YV9zdGFnZRIHGgQBCgcBAgcKJQoZY29tLmNoYXJ0aW5nLnZkcmlrb21vYWxlEgQaAhkGCiMKHGNvbS5jaGVja21hdGUuYW5kcm9pZBIDGgEGCiIKHGNvbS5jaW1i

Ch4KE0NhcmUuY2FyaXR5LmFwcF9kZXYSBxoFBB0eBxEKIQoaSnAuam95Zml0LmpveWZpdGFwcGFuZHJvaWQSAxoBBgojChxKcC5ub2J1Y29ycG9yYXRpb24uaGVpYW53
YWxrEgMaAQYKGgoPYWUubTQyLnN1cGVyYXBwEgcaBRsEGQYRCikKFWFwcC5hZXN0aGV0aWNzYWR2aXNvchIQGgkBCgIdDRkGIxEiAwEdIwopCg9hcHAuYnBqcy5tb2Jpb
GUSFhoUAQkaGwocAgQFHQ0XGB8gIiUGIxEKFQoOYXBwLm1vdmV2by5wc3oSAxoBBgofChBhcHAubW92ZXZvLnNhcHBpEgsaCQIDBCcFJCUGCAofChVhcHAud2VpZ2h0
Zml0LmFuZHJvaWQSBhoEBSIBEQojChlhc2lhLmNyb2l4LmFwcC5yZWxheHdvcmxkEgYaBAEEGQYKFQoNYmlrZS5jb2JpLmFwcBIEIgICBAovCiVici5jb20ucmRzYXVkZS5oZW
FsdGhQbGF0Zm9ybS5hbmRyb2lkEgYaBAINBhEKHgoTY2FzZS5jYXJpdHkuYXBwX2RldhIHGgUEHR4HEQoaCg9jYXJlLmdvb2RheS5hcHASBxoFAQIEBiMKGAoMY2MuaXNz
aW4uc2JtEggaAgYRIgIGEQoZCg5jYy5pc3Npbi5zcG9ydBIHGgIdBiIBHQodChZjby5jaG9vc2VicmlnaHQuY2xpZW50EgMaAQYKKgoPY28ud2VsbC53ZWxsYXBwEhcaFQEJGhs
KAgQFHR4NFxgkIhklBiMHEQoqCh9jb20uYWJzb2x1dGVseWRpZ2l0YWwuc3RlcGNoYWluEgcaAgEGIgEGChgKEGNvbS5hZGFlZmZzZTIwMjESBBoCAgYKGAoRY29tLmFkYW
VqdXJpczIwMjESAxoBBgoXChBjb20uYWRhZW5mbGkyMDIxEgMaAQYKNAoaY29tLmFkdm1lZHMubXBocmFwcF90YWluYW4SFhoUASEJGhsKHAsMHR4NHyAiGSUGIxEKF
QoOY29tLmFsYW5tb2JpbGUSAxoBBgoPCghjb20uYWxpeBIDGgEGChcKDGNvbS5hbHRlcl92MhIHGgERIgIEHQoeChZjb20uYW5hbW5lLm91Y2hpYnlvdWluEgQaAhkGCiIK
GmNvbS5hbmFtbmUub3VjaGlieW91aW4uc3RnEgQaAhkGChoKDmNvbS5hcHAuZml0YWdlEggiBgkKCwwdEQoWCgpjb20uYXBwLmdlEggiBgkKCwwdEQosCiVjb20uYXB
wLnJlYWxmaXR6Y2xpZW50YW5kcm9pZC5maXRuZXNzEgMaAQYKLgoeY29tLmJlbmVmaXR0ZWNobm9sb2dpZXMuYmVmaXQSBhoEBQdBhEiBAQdBhEKIAoYY29tLmJld
HRlcmxpZmUuU3RlcG9ncmFtEgQaAgIGChcKDmNvbS5iZXR0ZXJ0aW1lEgUaAwQZBgodCg9jb20uYmV4b21lLmVnaGkSChoIARsKHB0ZBhEKJQoaY29tLmJyaXNrbG9uZ2V
2aXR5LmFuZHJvaWQSBxoFAgQdGQYKLQoTY29tLmJ1enVkLmdmaWxlMDIxEgcaBRsEGQYRChYKEGNvbS5jYWxvcmllLmRlbW8SBBoCBQYKJAoeY29tLmNhbGxicmVla
GNvbS5jaGFwbWVjaC5ocGZ0aGNhcmUuaGxkZWx0YV9zdGFnZRIHGgQBCgcBAgcKJQoZY29tLmNoYXJ0aW5nLnZkcmlrb21vYWxlEgQaAhkGCiMKHGNvbS5jaGVja21hdGUuYW5kcm9pZBIDGgEGCiIKHGNvbS5jaW1i

IlIxEKKQoZY29tLmtha2FvaGVhbHRoY2FyZS5wYXN0YRIMGgoBAgQdHhklBiMRChcKEGNvbS5rZGRpLmtkbGEuanASAxoBBgopChVjb20ua2luZ3NtaXRoLnhpYW9qaW4SE
BoGAQIBJQYjIgYEBAgQIBMKPwoVY29tLmtpbmdzdGluY3QuaHVkZGxlEiYaJAEhCRobChwLDBICAwQnBR0eDRcmDxQYFR8kICIWGSUGIwcRCAojChNjb20ubGFuc2lrLmdsd
WNvZml0EgwaCgECBCcdHiIZBiMKGAoRY29tLmxlYm91Z2luZy5hcHASAxoBBgobChRjb20ubGVva2FyZS50cmFja2x5ZhIDGgEGCh8KGGNvbS5sZW9rYXJlLnRyYWNrbHlmL
mRldhIDGgEGCiEKGWNvbS5saWJlcmRhdC5saWJlcmRhdGJldGESBBoCBQYKGwoPY29tLmxpbnppLnNwb3J0EggiBgECBB0GIwojChxjb20ubGlxdWlkc3RhdGUucGVwaGVh
bHRoYXBwEgMaAQYKKAodY29tLmxtc3BvcnR0b3VyaXNtLnJ1bm5pbmNpdHkSBxoCAgYiAQYKJQoaY29tLm1vYmlsZTEuY2hhbGxlbmdlaG91bmQSBxoFAgMEJwYKHAoM
Y29tLm1yYy5sZWFuEgwaBAEYIxEiBAEYIxEKJAodY29tLm12ZW50dXMuc2VsZmNhcmUuYWN0aXZpdHkSAxoBBgoYCg1jb20ubXlkYXkuYXBwEgcaBQIdIhkGCh8KDWNvbS
5uYWlyYXdhbGsSDhoFAiclBiMiBQInJQYjCj0KFWNvbS5uZWNsYWJzLnRlbXBsZWRldhIkGiIBIQkaGwocCwwSAgMEJwUdHg0XJg8UGB8kICIZJQYjBxEICisKIWNvbS5ub19jcm
VhdGl2aXR5X2NvYWNoX29mX3Blb3BsZRIGGgEGIgEGChcKEGNvbS5ub3ZhYmVuZWZpdHMSAxoBBgoZCg9jb20ubnR0Lm1pZXJpaGESBhoEGx0GEQoWCg9jb20ubnVra3
VhYS5hcHASAxoBGQokChljb20ubnV0cmF0ZWNoLmFwcC5hbmRyb2lkEgcaBQECBAYjCjMKIGNvbS5udXRyaXRpb24udGVjaG5vbG9naWVzLkZpdGlhEg8aBQoEGCMRIgY
KBBcYIxEKMwogY29tLm9tcm9uaGVhbHRoY2FyZS5vbXJvbmNvbm5lY3QSDxoDAgYjIggbAh0NGQYjEQoaChBjb20ucGFyYW4ub3Vud2FuEgYaBAEEJwYKGAoNY29tLnBhc
mxheW1lZBIHGgUNFxgZEQoXCgxjb20ucGhtcC5hcHASBxoFAQIEBiMKIAoSY29tLnBpbGx5emUuaGVhbHRoEgoaCAEKAgQdBiMRCi0KIWNvbS5wcmVzc2ZvcndhcmRnYW
1lcy5jYXJkaW9xdWVzdBIIGgIdBiICHQYKGQoPY29tLnByb2FjdGl2ZWx5EgYaBAQZBhEKHQoPY29tLnByb2plY3RlY2hvEgoaBAEKIxEiAgoRCiAKFGNvbS5wdWppZS53YXRjaG
ZhY2VzEggaBgECBB0GIwocChRjb20ucWluZ25pdS5hcmJvbGVhZhIEIgIKEQobChNjb20ucWluZ25pdS5mZWVsZml0EgQiAgoRCiAKFmNvbS5yYWduYXJzdHVkaW9zLkFIR0
MSBhoBBiIBBgonChtjb20ucmFnbmFyc3R1ZGlvcy5zdGVwc2Vuc2USCBoCBQYiAgUGChgKDWNvbS5yZWFsLmdycnQSBxoFARodDQYKGwoTY29tLnJlY29kZS5icmFkZm9y
ZBIEGgICBgobChNjb20ucmVjb2RlLmZjY2NhcmVzEgQaAgIGCiEKGWNvbS5yZWNvZGUuZm91bmRhdGlvbndlbGwSBBoCAgYKIwobY29tLnJlY29kZS5pbm5vdmF0ZXJjb25u
ZWN0EgQaAgIGCiEKGWNvbS5yZWNvZGUubWNycmlmZmpvdXJuZXkSBBoCAgYKJgoeY29tLnJlY29kZS5tZXJpdG1lZGljYWxjb25uZWN0EgQaAgIGChoKEmNvbS5yZWNvZG
UucHJvc3BlchIEGgICBgoZChFjb20ucmVjb2RlLnR1c3RpbhIEGgICBgogChFjb20ucmVkaWdvLmRpZXRnbxILGgYKAh0NBhEiAREKHgoUY29tLnJldml2ZWRuYS5oZWFsdGgSB
hoEHSIZBgojChtjb20ucnViYW1hcHBzLmRyZWFtc2pvdXJuZXkSBBoCHRkKLwoVY29tLnJ1bnRhc3RpYy5hbmRyb2lkEhYaCQECAwQnHSUGIyIJAQIDBCcdJQYjCjUKGmNvbS
5yeGJyaWRnZS5zeW5hcHNlbW9iaWxlEhcaFQEJGhsKHAIEBR0NFxgfICIZJQYjEQoZChFjb20uc2FoaGEuYW5kcm9pZBIEGgIZBgorChxjb20uc2FrYXNzdHVkaW8uaGVkZWZs
ZXJpbWl6EgsaAgQGIgUBAgQGIwodChVjb20uc2NheWFuLmhhcHB5Y2VsbHMSBBoCGQYKMgopY29tLnNlbGZjYXJlLmRpYXJ5Lm1vb2QudHJhY2tlci5tb29kcHJlc3MSBRoD
HhkGCmQKFGNvbS5zaGFtcm9jay5yZWV3b3JrEkwaJAEhCRobChwLDBICAwQnBR0eDRcmDxQYFR8kICIWGSUGIwcRCCIkASEJGhsKHAsMEgIDBCcFHR4NFyYPFBgVHyQgI
hYZJQYjBxEIChsKD2NvbS5zbGltcGFsLmFwcBIIIgYJCgsMHREKIgoQY29tLnNuYXBhbmR0cmFjaxIOGggBCgIdDRkGESICAR0KIAoUY29tLnNvY2NlckZpdFlvdS5BcHASCBoGA
gQnHSUGCi4KHGNvbS5zb2Z0Y29uc3RydWN0LnZpZ29oZWFsdGgSDhoFAQIlBiMiBQECJQYjChgKD2NvbS5zcGFya2hhYml0cxIFGgMBAgYKSQonY29tLnNwb3J0YWJsZS5z
cG9ydGFibGVfd2hpdGVfbGFiZWxfYXBwEh4aHAEJCgsMEgIDBCcFHR4NFw8YHyQgIhklBiMHEQgKIAoSY29tLnNwb3J0c3Bhc3Nwb3J0EgoaCAEJCg0fBgcRCiYKG2NvbS5zc3
RlY2hzeXN0ZW0uaG9tZWZpdHBybxIHGgUBAh0GIwomChtjb20uc3RhcmhlYWx0aC5zdGFyd2VsbG5lc3MSBxoFAR0fBiMKIAoXY29tLnN0ZXAuaGVhbHRoLmFuZHJvaWQS
BRoDAgYjCiYKH2NvbS5zdXJwYXNzcG9ydC5wYXJ0aWNpcGF0ZS5rc3ASAxoBBgocChBjb20uc3p5ay5teWhlYXJ0EggaAhsdIgIbHQoXChBjb20udGFwYmVlLmRlbHRhEgMaA
QYKGwoRY29tLnRheWxvci50YXlsb3ISBhoBESIBEQoRCgpjb20udGVhbWNvEgMaAQYKJAoQY29tLnRnaS5hZ2V3aXNlchIQGggaGwIdHh8lBiIEGx0fBgooChtjb20udGltZXBy
b2R1Y3RzLmxpbWl0c21hcnQSCRoBBiIEHRkGEQokChJjb20udG9iaWFza3Vyei5hcHASDhoIAQoCHQ0ZBhEiAgEdCjYKJWNvbS50cmFpbmluZ2FtaWdvLnR1ZGlwLnRyYWlu
aW5nYW1pZ28SDRoFAQIEBiMiBAECBiMKJwoaY29tLnRyYW5zc2lvbi5vcmFpbW9oZWFsdGgSCSIHAQIdHyIZBgovChRjb20udHJpY29nLnRyaWNhcmVoZhIXGhUBCRobCh
wCBAUdDRcYHyAiGSUGIxEKJQoeY29tLnRyeWFwdC5Wb2xrc3dhZ2VuR2Vuc2VyQXBwEgMaAQYKFgoNY29tLnVidXJuLmFwcBIFGgMBBCMKJwoXY29tLnVkaGMucnBtc21
hcnRjbGluaXgSDBoKAh0NHyAZBiMHEQoeChNjb20udWhkYS5tb25pdG9yaW5nEgcaBQECHQYjCisKG2NvbS51bHRpbWF0ZXBlcmZvcm1hbmNlLnd3dxIMGgQXGQYRIgQ
XGQYRChoKDmNvbS51bWVub2tpLmpwEggaBhobHBkGEQokChRjb20udXJiYW5kcm9pZC5zbGVlcBIMGgQdHyIZIgQdHyIZChUKC2NvbS51cmluaWZ5EgYaBAEdGQYKQQ
oWY29tLnZvb3N0YWNrLm51dHJpbm90ZRInGh4BIQkaGwocCwwCAwQnBR0eDRcPGCQgIhklBiMHEQgiBQENFxgZChYKDmNvbS52dC52aXRhZml0EgQiAgoRChcKD2Nv
bS53YW0uYW5kcm9pZBIEGgIEBgobChBjb20ud2VsbGJheXQuYXBwEgcaBQECBQYjChwKEWNvbS53ZWxsbW8uY2xpZW50EgcaBRsEGQYRChsKEWNvbS53ZWxsc2hhcGU
uYXBwEgYaBAIdGQYKSgobY29tLndlbGx0b3J5LmNsaWVudC5hbmRyb2lkEisaIwEhCRobChwLDBICAwQFHR4NFyYPFBgVHyQgIhYZJQYjBxEIIgQbHR4RChQKCmNvbS53ZX
dhcmQSBhoEAQIFBgojChJjb20ud2lnZ2wud2lnZ2xhcHASDRoFAgQdBiMiBAIEBiMKIwoaY29tLndvbWJhdGFwcHMuY2FyYm1hbmFnZXISBRoDBAYRCiIKFmNvbS54ZGV2c3
Rhci5zbGVlcHRlcnkSCBoGHR4fIhkHCh0KDWNvbS55YXplbi5hcHASDBoKAQkCAwUdIgYjEQokChxjb20uem9jb251dC5hcm9neWFtbnV0cml0aW9uEgQaAgYjCiEKGWNvbS
56b2NvbnV0LmJhbGNhbG51dHJlZnkSBBoCBiMKGgoWY29tLnpvY29udXQuYm9keXNocmluZRIACiIKGmNvbS56b2NvbnV0LmJveGZ1bGxvZmJlYW5zEgQaAgYjChwKFGN
vbS56b2NvbnV0LmRyZmFybWVyEgQaAgYjChsKE2NvbS56b2NvbnV0LmZsYWJieWUSBBoCBiMKJgoeY29tLnpvY29udXQuaGVhbHRoYmVmb3Jld2VhbHRoEgQaAgYjCiAK
GGNvbS56b2NvbnV0LmhlYWx0aHR1bm5lbBIEGgIGIwomCh5jb20uem9jb251dC5oZWFsdGh5Znlzb2x1dGlvbnMSBBoCBiMKIQoZY29tLnpvY29udXQuaG9ybW9uZWNsa

POSSIBLE SECRETS

W5pYxIEGgIGIwodChVjb20uem9jb251dC5pY3VyZWRpZXQSBBoCBiMKIAoYY29tLnpvY29udXQuamJnZW5kdXJhMTAxEgQaAgYjCh8KF2NvbS56b2NvbnV0Lm1paGVhbHR
aAhSbhgQaAgYjCh0KE2NvbS56b2NvbnV0Lm5wZml0bmVzcxIEGgIGIwoZChFjb20uem9jb251dC5uc2tpbhIEGgIGIwokChxjb20uem9jb251dC5udXRyYWN5bGlmZXN0eW
xlEgQaAgYjChwKFGNvbS56b2NvbnV0Lm51dHJpZml0EgQaAgYjCiQKHGNvbS56b2NvbnV0Lm51dHJpdGlvbmRlZmluZWQSBBoCBiMKGwoTY29tLnpvY29udXQub2pvbGl
mZRIEGgIGIwobChNjb20uem9jb251dC5wYXJhZml0EgQaAgYjCh8KF2NvbS56b2NvbnV0LnBvb25hbXNhZ2FyEgQaAgYjCiAKGGNvbS56b2NvbnV0LnJ1c3RpY3dpc2RvbRIE
GgIGIwogChhjb20uem9jb251dC53b3djb21tdW5pdHkSBBoCBiMKIgobY3oudG1lc29sdXRpb25zLm5vdm9jYXJlYXBwEgMaAQYKJwoVZGUuZGVyZXJzdGVtdXNrZWwuYXB
wEg4aCAEKAh0NGQYRIgIBHQoeCgxkZS5naW5vc2luZ2gSDhoIAQoCHQ0ZBhEiAgEdChsKEmRlLnRvcnRpamEuYXBwLnR3YRIFGgMEBiMKIgoXZGV2LmFwcHRvZGF0ZS5tZ
W50YWlBcHASBxoFGwIdGQYKJwofZGV2LmxhYjkwLnNwYWNlRm9yTnV0cml0aW9uLmRldhIEGgIBAgorCiBkaWdpZml0LnZpcnR1YWd5bS5jbGllbnQuYW5kcm9pZBIHGg
UCBB0GIwosChVkaWdpdGFsLmxhbXAubWluZGxhbXASExoRAQkaGwocAh0eFxgfIBklBiMKQQoaZGsuY2FjaGV0LmNhcnBfc3R1ZGllc19hcHASIxohASEJGhsKHAsCAwQnB
R0eDRcmDxQYFR8kICIZJQYjBxEICi4KJGVkdS5vc3VtYy5yaXNlLm1oZWFsdGg2MTYzNjg2OTY1NzY2NRIGGgEGIgEGCiAKD2VzLnNwYy5zbWFydHlvdRINGgINESIHAgQdHxk
GIwpJChtldS5iZW91cmJlc3QuYm9iX21vYmlsZV9hcHASKhokASEJGhsKHAsMEgIDBCcFHR4NFyYPFBgVHyQgIhYZJQYjBxEIIgINEQoZChJldXMud2VsbGsud2VsbGthcHASAxo
BBgopChtmaS5wdW9sdXN0dXN2b2ltYXQubWFyc21hcnMSChoIAgQdGSUGIxEKGgoTZ292Lmd5ZW9uZ2dpLmdnY2FyZBIDGgEGCjcKE2hlYWx0aC5hbHlmLnBhdGllbnQ
SIBoeASEJGhsKHAsMAgMEJwUdHg0XDxgfJCAiGSUGIwcRCiQKEWhlYWx0aC5teWRpYWJldGVzEg8aBhobBBcGESIFGhsEFxEKGAoMaGsuamNmaXRjaXR5EggaBgECBRkGIw
oVCg5pbi5maXRwYWdlLmFwcBIDGgEGCh8KGGlvLmNvbm5lY3RlZGxpZmUuY2xocHJvZBIDGgEZCiUKHmlvLmNvbm5lY3RlZGxpZmUubWVkaWNsaW5pY3VhdBIDGgEZC
hsKCmlvLm1haWxpZmUSDRoLARobAgQdDRkGIxEKHwoXanAuYXNhaGlrYXdhLmhlYWx0aGNhcmUSBBoCAgYKHAoVanAuYmFsYW5jZWNoZWNrLnNhbndhEgMaAQYKN
QoYanAuY28uY2l0aXplbi5oZWFsdGhjYXJlEhkaDCEJGwocCwIdDQYjESIJIQkbChwLHQ0RCjkKHGpwLmNvLmNpdGl6ZW4uaGVhbHRoY2FyZS5zdGcSGRoMIQkbChwLAh0N
BiMRIgkhCRsKHAsdDREKQAoWanAuY28ubG9nc2hhcmUubG9nc2lydRImGhEBCRobChwMAh0NDxgiJQYjESIRAQkaGwocDAIdDQ8YIiUGIxEKIQoUanAuY28ubWVkaXJvbS
5tb3RoZXISCSIHASEcHRkGIwofChNqcC5jby5ydW5uZXJzLnRhdHRhEggaBgIDBCcGIworCiJqcC5jby50cmVlYmVsbC5hcHAuTWluZFRoZXJtb21ldGVyEgUaAx0ZBgogChdqcC
5oaWJpdG5lc3MuRml0bmVzc0FwcBIFGgMCBiMKGwoTanAuaW5hYmUuaGVhbHRoY2FyZRIEGgIGBgohChpqcC5qb3lmaXQuam95Zml0YXBwYW5kcm9pZBIDGgEGCiAK
E2pwLmxpbnFfcGFsZXR0ZS5scXASCRoHGhsKHB0GEQoXChBqcC5uZWNwcy5mdWt1b2thEgMaAQYKFQoOanAubmVjcHMuZ290b3USAxoBBgoVCg5qcC5uZWNwcy5zY
WxrbxIDGgEGCiMKHGpwLm5vYnVjb3Jwb3JhdGlvbi5oZWlhbndhbGsSAxoBBgoeChRqcC5wb2ludGkucG9pbnRpX2FwcBIGGgEGIgEGCiEKF2pwLnBva2Vtb24ucG9rZW1v
bnNsZWVwEgYaARkiARkKJgoaa3IuY28uYXJkcy5jYW5tb3JlcHJvLnByb2QSCBoGGhscHR8GCiUKFGtyLmNvLmZhbWlsaWNhcmUuZm1iEg0aCwEbAgQdHxklBiMHCi0KHGty
LmNvLmhjb25uZWN0LmhlYWx0aG9uLmdlbmESDRoLARobAgQdGBkGIxEKGgoTbGkueWFwcC5hcHA2ODgzMEEyQhIDGgEGChoKE2xpLnlhcHAuYXBwQURCQ0IxNDESA
xoBBgohChFubC5pdmlkby5pdmlkb3BnbxIMGgoaGxwdDR8gJQYRCh0KFW9ubGluZS5zbWFydF93ZWxsbmVzcxIEGgIGEQo8ChtvcmcuaWdneW1lZGlhLnBlcmlvZHRyYW
NrZXISHRoTASEcEgIEHR4NJhQVIhYZBiMRCCIGIRIVFhkRCjMKEXBsLmxpZmViaXRlLml5b25pEh4aDyEcEgQdHg0XJhQVFhkGESILIRwSDRcmFBUWGREKOQolcGwucGF3ZW
xza3J6eXBrb3dza2kuc2tpcHB5Zml0Lm1vYmlsZRIQGg4BCgsMAgQFHQ8fGQYjEQocChVydS5haXNhLmFuZHJvaWQuZWtwdjISAxoBBgoZCg1ydS5tdHMuY29zbW9zEggaA
glGIgICBgoaChJzZS5zbHNvLmhhbHNvbWV0ZXISBBoCAgYKFAoLdHYuZmlpdC5hcHASBSIDAQQdChkKDHdlbGx0aHkuY2FyZRIJGgcaGwQdHwYR

PLAYSTORE INFORMATION

Title: Health Connect

Score: 2.6471775 **Installs:** 500,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.google.android.apps.healthdata

Developer Details: Google LLC, 5700313618786177705, None, http://www.android.com/, health-connect-support@google.com,

Release Date: Nov 10, 2022 **Privacy Policy:** Privacy link

Description:

Health Connect by Android gives you a simple way to share data between your health, fitness, and wellbeing apps without compromising on privacy. Once you've

downloaded Health Connect, you can access it through your settings by going to Settings > Apps > Health Connect, or from your Quick Settings menu. Get more from your favorite apps. Whether you're focused on activity or sleep, nutrition or vitals, sharing data between your apps can help you better understand your health. Health Connect gives you simple controls, so you only share the data you want to. Keep your health and fitness data in one place. Health Connect stores the health and fitness data from your apps in one place, offline and on your device, so you can easily manage the data from your different apps. Update privacy settings in a few taps. Before a new app can access your data, you can review and choose what you want to share. If you change your mind, or want to see which apps recently accessed your data, find it all in Health Connect.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 23:15:12	Generating Hashes	OK
2025-08-29 23:15:12	Extracting APK	OK
2025-08-29 23:15:12	Unzipping	OK
2025-08-29 23:15:12	Parsing APK with androguard	OK
2025-08-29 23:15:13	Extracting APK features using aapt/aapt2	OK
2025-08-29 23:15:13	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 23:15:15	Parsing AndroidManifest.xml	OK

2025-08-29 23:15:15	Extracting Manifest Data	OK
2025-08-29 23:15:15	Manifest Analysis Started	OK
2025-08-29 23:15:15	Performing Static Analysis on: Health Connect (com.google.android.apps.healthdata)	OK
2025-08-29 23:15:16	Fetching Details from Play Store: com.google.android.apps.healthdata	OK
2025-08-29 23:15:16	Checking for Malware Permissions	OK
2025-08-29 23:15:16	Fetching icon path	OK
2025-08-29 23:15:17	Library Binary Analysis Started	OK
2025-08-29 23:15:17	Reading Code Signing Certificate	OK
2025-08-29 23:15:17	Running APKiD 2.1.5	OK
2025-08-29 23:15:19	Detecting Trackers	OK
2025-08-29 23:15:20	Decompiling APK to Java with JADX	OK

2025-08-29 23:15:28	Converting DEX to Smali	OK
2025-08-29 23:15:28	Code Analysis Started on - java_source	OK
2025-08-29 23:15:30	Android SBOM Analysis Completed	OK
2025-08-29 23:15:39	Android SAST Completed	OK
2025-08-29 23:15:39	Android API Analysis Started	OK
2025-08-29 23:15:48	Android API Analysis Completed	OK
2025-08-29 23:15:49	Android Permission Mapping Started	OK
2025-08-29 23:15:56	Android Permission Mapping Completed	OK
2025-08-29 23:15:56	Android Behaviour Analysis Started	OK
2025-08-29 23:16:08	Android Behaviour Analysis Completed	OK
2025-08-29 23:16:08	Extracting Emails and URLs from Source Code	OK

2025-08-29 23:16:10	Email and URL Extraction Completed	OK
2025-08-29 23:16:10	Extracting String data from APK	OK
2025-08-29 23:16:10	Extracting String data from Code	OK
2025-08-29 23:16:10	Extracting String values and entropies from Code	OK
2025-08-29 23:16:11	Performing Malware check on extracted domains	OK
2025-08-29 23:16:15	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.