ANDROID STATIC ANALYSIS REPORT

Breeze (1.9.4)

File Name:	Breeze_ mental health_1.9.4_Apkpure.apk
Package Name:	com.basenjiapps.breeze
Scan Date:	Nov. 28, 2023, 7:11 p.m.
App Security Score:	39/100 (HIGH RISK)
Grade:	C
Trackers Detection:	7/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
8	14	2	2	1

FILE INFORMATION

File Name: Breeze_ mental health_1.9.4_Apkpure.apk
Size: 83.76MB
MD5: 9dbf25540828744c097f73dc684e649b
SHA1: 2eca6989e68add657229559f1a9745ea069a07f4
SHA256: 062567340b01c94f0b0ffc85362e6bd8ffcc4f2aed808832ec4366d4c0526ab1

APP INFORMATION

App Name: Breeze
Package Name: com.basenjiapps.breeze
Main Activity: com.basenjiapps.breeze.MainActivity
Target SDK: 33
Min SDK: 21
Max SDK:
Android Version Name: 1.9.4

Android Version Code: 70

APP COMPONENTS

Activities: 10
Services: 10
Receivers: 9
Providers: 5
Exported Activities: 2
Exported Services: 1
Exported Receivers: 3
Exported Providers: 1

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: 2021-04-13 13:53:58+00:00
Valid To: 2051-04-13 13:53:58+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xaa9307f5f822980380f64f2256bd80481afbaca0
Hash Algorithm: sha256
md5: ea6980ee7d346569bdb2b580b6b0ca5f
sha1: abbe52419aa0f6571fe641121a659d6171514b41
sha256: 027e4ad1ef85f5a73f0340e3693d8434a502c06808aad529ffe65844fd05a7c3
sha512: 4609cc629501283638c8044345331866706bdef9a837e085b8b2a0d63475f645c113cfcbe03c762086dced4b2773c52ef656df95ab30e297e95bd5ac549c7c61
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: e0ce8bade94d593e210e824a836b782efa08c213db27d482d690ec506dd0eca0
Found 1 unique certificates
```

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.SCHEDULE_EXACT_ALARM	normal		Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
com.android.alarm.permission.SET_ALARM	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous		Allows an app to post notifications
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
com.basenjiapps.breeze.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

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
network operator name check
ro.kernel.qemu check</td></tr>
<tr><td>Compiler</td><td>r8</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>dx</td></tr>
</table>
</td></tr>
<tr><td>classes3.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</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.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.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>
</table>
</td></tr>
<tr><td>classes5.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>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.basenjiapps.breeze,

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: **6** | WARNING: **3** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=21]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Broadcast Receiver (com.appsflyer.SingleInstallBroadcastReceiver) is not Protected. [android:exported=true]	high	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.
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	Content Provider (com.yandex.metrica.PreloadInfoContentProvider) is not Protected. [android:exported=true]	high	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.
6	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	high	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	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	high	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
8	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [android:exported=true]	high	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 (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: **1** | WARNING: **9** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a2/h0.java a3/c.java b4/c.java cg/a.java ch/b0.java ch/e1.java ch/f.java ch/k0.java ch/r.java ch/s.java ch/t.java com/airbnb/lottie/LottieAnimationView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				iew.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/appsflyer/AFLogger.java com/basenjiapps/auth_android/presentation/AuthActivity.java com/basenjiapps/breeze/MainActivityViewModel.java com/yandex/metrica/gpllibrary/a.java com/yandex/metrica/impl/ob/C1475h2.java com/yandex/metrica/impl/ob/Cf.java com/yandex/metrica/impl/ob/If.java com/yandex/metrica/impl/ob/Jf.java com/yandex/metrica/impl/ob/R1.java com/yandex/metrica/impl/ob/T2.java df/c.java df/g.java df/q.java df/r.java df/t.java df/w.java df/x.java df/z.java dg/a.java dm/c.java e3/c.java e4/a.java ee/c.java ef/d0.java ef/e.java ef/h0.java ef/i.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	ef/j.java ef/l.java ef/t.java ef/x.java f4/h0.java f4/x.java f5/g.java fd/c0.java fd/g.java fd/i0.java fd/s0.java fe/t.java fe/w.java fg/h.java g2/c.java gd/c.java gd/d0.java gd/f.java gd/m.java gd/q.java gf/z.java gh/a.java gh/b.java gh/d.java gh/h.java gh/l.java gh/o.java gh/p.java hf/a.java hf/a0.java hf/c.java hf/d0.java hf/f1.java hf/i1.java hf/s0.java hf/v0.java hf/w0.java hf/x0.java hf/z0.java i5/c.java jd/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				k/g.java k0/b.java k2/p.java k5/c.java kd/c.java kd/d.java kh/c.java l/c.java lf/a.java m3/a.java md/a.java mf/g.java mf/o.java mf/p.java od/f.java od/h.java od/k.java oh/g.java oh/n.java ph/b.java qe/i.java qf/b.java rd/a.java se/a.java sf/l.java sg/d.java si/a.java t3/a.java tg/b.java u3/a.java u3/b.java v1/s.java v3/a.java v3/m.java vd/a0.java vd/g0.java vd/h0.java vg/g.java w0/c.java w0/g.java xf/a.java

NO	ISSUE	SEVERITY	STANDARDS	z3/b.java z4/c.java FILES
				c4/a.java com/yandex/metrica/impl/ob/A8.java com/yandex/metrica/impl/ob/B8.java com/yandex/metrica/impl/ob/C1327b.java com/yandex/metrica/impl/ob/C1457g8.java com/yandex/metrica/impl/ob/C1481h8.java com/yandex/metrica/impl/ob/C1505i8.java com/yandex/metrica/impl/ob/C1528j8.java com/yandex/metrica/impl/ob/C1552k8.java com/yandex/metrica/impl/ob/C1576l8.java com/yandex/metrica/impl/ob/C1600m8.java com/yandex/metrica/impl/ob/C1624n8.java com/yandex/metrica/impl/ob/C1648o8.java com/yandex/metrica/impl/ob/C1672p8.java com/yandex/metrica/impl/ob/C1696q8.java com/yandex/metrica/impl/ob/C1719r8.java com/yandex/metrica/impl/ob/C1743s8.java com/yandex/metrica/impl/ob/C1767t8.java com/yandex/metrica/impl/ob/C1791u8.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	com/yandex/metrica/impl/ob/C1815v8.java com/yandex/metrica/impl/ob/C1839w8.java com/yandex/metrica/impl/ob/C1863x8.java com/yandex/metrica/impl/ob/C1887y8.java com/yandex/metrica/impl/ob/C1911z8.java com/yandex/metrica/impl/ob/C8.java com/yandex/metrica/impl/ob/D8.java com/yandex/metrica/impl/ob/E7.java com/yandex/metrica/impl/ob/E8.java com/yandex/metrica/impl/ob/F7.java com/yandex/metrica/impl/ob/F8.java com/yandex/metrica/impl/ob/G7.java com/yandex/metrica/impl/ob/G8.java com/yandex/metrica/impl/ob/H8.java com/yandex/metrica/impl/ob/I8.java com/yandex/metrica/impl/ob/K8.java com/yandex/metrica/impl/ob/L8.java com/yandex/metrica/impl/ob/M8.java com/yandex/metrica/impl/ob/N8.java com/yandex/metrica/impl/ob/O8.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/yandex/metrica/impl/ob/P8.java com/yandex/metrica/impl/ob/Q7.java com/yandex/metrica/impl/ob/Q8.java com/yandex/metrica/impl/ob/R8.java we/b0.java we/e0.java we/h0.java
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	com/airbnb/lottie/compose/RememberLottieCompositionKt.java com/appsflyer/AppsFlyerProperties.java com/yandex/metrica/impl/ob/C1501i4.java com/yandex/metrica/impl/ob/C1895yg.java com/yandex/metrica/impl/ob/D4.java com/yandex/metrica/impl/ob/yn.java g0/i0.java id/d.java k0/m1.java k0/m2.java ol/j0.java s4/h.java s4/i.java s4/l.java ta/g.java x4/j.java z1/h.java z1/u0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	com/appsflyer/internal/ai.java com/yandex/metrica/impl/ob/Cl.java com/yandex/metrica/impl/ob/Gl.java gd/d.java od/k.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/basenjiapps/auth_android/presentation/AuthActivity.java
6	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/basenjiapps/auth_android/presentation/AuthActivity.java
7	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/basenjiapps/auth_android/presentation/AuthActivity.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	com/appsflyer/internal/ai.java com/yandex/metrica/impl/ob/H.java ee/a.java si/a.java
9	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	fd/m.java j$/util/concurrent/ThreadLocalRandom.java ma/b.java vd/g0.java yk/a.java yk/b.java zk/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	com/basenjiapps/breeze/h.java e6/c.java vd/g0.java
11	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	e6/c.java u3/b.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	ch/t0.java com/yandex/metrica/impl/ob/X1.java
13	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	fd/b.java fd/h0.java fd/j0.java fd/s0.java fe/v.java md/j.java sd/b.java
14	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	cm/c.java cm/d.java cm/g.java cm/h.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
smonitorsdk.s	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
staging.sso.basenjiapps.com	ok	**IP:** 3.216.198.114 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
plus.google.com	ok	**IP:** 172.217.13.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
startup.mobile.yandex.net	ok	**IP:** 213.180.204.244 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
basenjiapps.com	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.google.com	ok	**IP:** 172.217.13.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
update.crashlytics.com	ok	**IP:** 172.217.13.99 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
accounts.google	ok	No Geolocation information available.
payments.basenjiapps.net	ok	**IP:** 3.212.244.36 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
svalidate.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
m.facebook	ok	No Geolocation information available.
sstats.s	ok	No Geolocation information available.
reports.crashlytics.com	ok	No Geolocation information available.
developers.facebook.com	ok	**IP:** 31.13.80.8 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map
developer.android.com	ok	**IP:** 172.217.13.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sso.basenjiapps.com	ok	**IP:** 34.204.214.107 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.betterhelp.com	ok	**IP:** 44.210.192.121 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
graph.s	ok	No Geolocation information available.
moodtracker-8c9ae.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
instagram.com	ok	**IP:** 31.13.80.174 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
graph-video.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
ssdk-services.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
play.google.com	ok	**IP:** 172.217.13.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
issuetracker.google.com	ok	**IP:** 172.217.13.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
facebook.com	ok	**IP:** 31.13.80.36 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map
sonelink.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.tiktok.com	ok	**IP:** 23.43.243.154 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.80.36 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map
sapp.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
yandex.com	ok	**IP:** 5.255.255.88 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
.facebook.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
firebase-settings.crashlytics.com	ok	**IP:** 172.217.13.131 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://moodtracker-8c9ae.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
ssss@gmail.com	p5/a.java
u0013android@android.com0 u0013android@android.com	ef/s.java

TRACKERS

TRACKER	CATEGORIES	URL
AppMetrica		https://reports.exodus-privacy.eu.org/trackers/140
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 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
"facebook_client_token" : "3ad8d6675d42f93ed2746908a8413305"
"firebase_database_url" : "https://moodtracker-8c9ae.firebaseio.com"
"google_api_key" : "AIzaSyALTZ7iZYBHJyXHBy4ZzOrGC0yVoZIA4sI"
"google_crash_reporting_api_key" : "AIzaSyALTZ7iZYBHJyXHBy4ZzOrGC0yVoZIA4sI"
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b>□□□□□□□□□□□□□□□□□□□□□□□□"

POSSIBLE SECRETS
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b>□□□□□□□□□□□□□"
0e5e9c33-f8c3-4568-86c5-2e4f57523f72
67bb016b-be40-4c08-a190-96a3f3b503d3
e992f2d927d84bf75b39ce6f64a79c76
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
4e610cd2-753f-4bfc-9b05-772ce8905c5e
7d962ba4-a392-449a-a02d-6c5be5613928
060534688f659efab287bd516a3a4aad
c56fb7d591ba6704df047fd98f535372fea00211
470fa2b4ae81cd56ecbcda9735803434cec591fa
cc2751449a350f668590264ed76692694a80308a
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
9f89db6f04ec319c99b89df2ff4a0fb8
7c244332ab06451ab2d97138b127d684

POSSIBLE SECRETS
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
e4250327-8d3c-4d35-b9e8-3c1720a64b91
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
20799a27-fa80-4b36-b2db-0f8141f24180
d8207821e5bd3005d40eae37cd21c5cd
b41172c29ef7ce778371c1fb58601578
3cff08d6cf392ff4f1514d0d2f5599f3
9b8f518b086098de3d77736f9458a3d2f6f95a37
01528cc0-dd34-494d-9218-24af1317e1ee
e44a8b69c7d76049d312caec6fb8a01b60982d8f
nRxJubTvK0kSMPeVGnFCATOR8UjpcXbk37UprgM6e4Q
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
6c5f504e-8928-47b5-bfb5-73af8d8bf4b4

POSSIBLE SECRETS
f07afdd2e03b98916ba7f9b771175a8f

PLAYSTORE INFORMATION

Title: Breeze: mental health

Score: 3.4556115 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.basenjiapps.breeze

Developer Details: Basenji Apps, 7066327292294031026, Florinis 7, Greg Tower, Floor 2, 1065, Nicosia, Cyprus, http://basenjiapps.com, support@basenjiapps.com,

Release Date: May 12, 2021 **Privacy Policy:** Privacy link

Description:

If you need an awesome tool to keep a diary and improve your mental well-being, then look no further. Meet Breeze — a mood tracker that is here to become your faithful ally in strengthening your mental health. Feelings to track, detailed stats to check, tests to do, and courses to learn — let us provide you with the features that will help you grow! Breeze doesn’t aim to replace a therapist. The mission is to help you improve your self-assessment and raise your awareness about depression, anxiety, bipolar disorder, extreme mood swings, and other mental disorders. The app is based on several concepts from cognitive-behavioral psychotherapy and contains four main features described below. Mood tracker Journal your mood daily to better understand the nature of your feelings and learn to be more in control of your emotions. Create a map of your emotional conditions and be aware of people and activities that make you happy or bring you down. Negative thoughts tracker The concept of automatic negative thoughts comes from cognitive behavioral therapy. The idea is that even minor negative thoughts that automatically appear in our consciousness influence our mood and psychological conditions. We provide you with several interactive techniques that help recognize and fight such negative patterns in thinking. Tracker of cognitive distortions Is it depression that makes you feel low? How to cope with panic attacks and anxiety? How to take care of people with bipolar disorder? We give some useful insights into popular cognitive distortions and teach you how to identify flaws in your thinking and behavior. Tests and self-assessments to discover your inner self The concept of psychological testing helps a lot to understand certain behaviors. We offer a great variety of tests: the Beck Anxiety Inventory Test, Beck Depression Inventory Test, Personality test, Mood Disorder Test, Test on Positive outlook, and many more. Advice from a psychotherapist (in future updates) Some practical advice from an acknowledged psychotherapist — he will cover widespread topics and issues people usually have in different areas of life. Breeze contains the following subscription options: - Weekly (with 3-days free trial) at $4 ; - Subscription automatically renews unless auto-renew is turned off at least 24-hours before the end of the current period. Account will be charged at the full price of the chosen subscription period. Account will be charged for renewal within 24-hours prior to the end of the current period - Any unused portion of a free trial period, if offered, will be forfeited when the user purchases a subscription to that publication. - Subscriptions may be managed by the user and auto-renewal may be turned off by going to the user’s Account Settings after purchase.

Report Generated by - MobSF v3.7.9 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment

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.