ANDROID STATIC ANALYSIS REPORT

Dateability (53)

File Name:	Dateability.apk
Package Name:	com.dateabilityapp
Scan Date:	Nov. 17, 2024, 11:39 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
1	18	1	2	1

FILE INFORMATION

File Name: Dateability.apk
Size: 23.38MB
MD5: 1474f05e75204fc94f406d8de9de5fab
SHA1: 8745d997efe1169505ef4fd05dfd5660dc8b2035
SHA256: 5a666b1fa661e4c92912902f5f97a170c30a6c7e62f94cd31337e46e52f2779a

APP INFORMATION

App Name: Dateability
Package Name: com.dateabilityapp
Main Activity: com.dateabilityapp.MainActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 53

Android Version Code: 53

APP COMPONENTS

Activities: 8
Services: 13
Receivers: 13
Providers: 4
Exported Activities: 0
Exported Services: 2
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: 2022-10-10 16:37:21+00:00
Valid To: 2052-10-10 16:37:21+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x168dacad2320ca51f130b0d48f918a8c7b155185
Hash Algorithm: sha256
md5: 9b1ab2c6d9978ff96962177f8e5e5230
sha1: 8b637f2e642b7201f63b9e901ee1a067fc2af56d
sha256: 490dc0c7b8e6b71dcc9b756d01763fd3cf7c93ca58f26d2a0a42bb500a863911
sha512: 5fdbef41f01f3ddfaf8aee24ab09919f34864ee4a8efda13e5edb5dfec1a57c5845be6bec3e123311a24b47e8fd6901073041b4f342377c531bb5107bc6c0248
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 81b3e9c7e227dcf09a17d27f8022a120a5dee27e8254998a851475cb8872a1e8
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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	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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.dateabilityapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<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.BOARD 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 Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></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: **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: **7** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched 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=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

NO	ISSUE	SEVERITY	DESCRIPTION
3	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.
4	Broadcast Receiver (com.amazon.device.iap.ResponseReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.inapp.purchasing.Permission.NOTIFY [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 (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
6	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.
7	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.
8	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: **8** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/c.java a6/e.java c1/j.java c4/a.java c5/c.java com/amazon/a/a/g/d.java com/amazon/a/a/o/c.java com/amazon/c/a/a/d.java com/amazon/device/drm/LicensingService.java com/amazon/device/drm/a/d/c.java com/amazon/device/iap/PurchasingService.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/BroadcastHandler.java com/amazon/device/simplesignin/SimpleSignInService.java com/amazon/device/simplesignin/a/a/c/b.java com/amazon/device/simplesignin/a/c.java com/amazon/device/simplesignin/a/c/b.java com/codetrixstudio/capacitor/GoogleAuth/GoogleAuth.java com/getcapacitor/m0.java com/revenuecat/purchases/capacitor/PurchasesPlugin.java com/revenuecat/purchases/common/DefaultLogHandler.java com/revenuecat/purchases/hybridcommon/CommonKt.java com/revenuecat/purchases/hybridcommon

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	com/revenuecat/purchases/hybridcommon/mappers/PurchasesPeriod.java d3/r1.java d4/b.java d6/g.java d6/o.java e0/c.java e4/h.java e4/s.java e4/t.java g0/a.java i2/k.java i4/d.java j0/c.java j8/p.java k4/l.java l2/a.java o0/c.java o5/d.java p5/b.java q/f.java q4/b0.java q4/d1.java q4/g2.java q4/h0.java q4/l.java q4/n.java q4/o0.java q4/s1.java q4/u1.java q6/b.java r5/g.java r6/c.java t3/h.java u0/c.java v1/i.java v3/b.java v3/c.java v3/g.java v3/q.java v3/r.java v3/t.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				v3/t.java v3/w.java v3/x.java w3/a0.java w3/f.java w3/f0.java w3/j.java w3/k.java w3/k0.java w3/n.java w3/w.java x/g.java x0/b.java x1/a.java x2/a.java x2/d.java y0/m0.java y3/c0.java y4/a.java z3/a.java z3/a1.java z3/c.java z3/d0.java z3/d1.java z3/e1.java z3/f1.java z3/g0.java z3/h1.java z3/n1.java z3/r1.java z4/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/getcapacitor/v0.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/capacitor/PurchasesPlugin.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/BackgroundAwareCallbackCacheKey.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsHelper.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/common/verification/SigningManager.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	q4/z0.java
4	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/amazon/a/a/o/b/a.java com/revenuecat/purchases/common/UtilsKt.java q6/b.java
5	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	b3/v.java com/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java m4/a.java p7/a.java p7/b.java q7/a.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/amazon/device/drm/LicensingService.java com/amazon/device/iap/PurchasingService.java
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	p2/m0.java p2/t0.java v0/a.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amazon/a/a/o/b/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	com/capacitorjs/plugins/camera/l.java com/getcapacitor/b0.java q6/c.java
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/capacitorjs/plugins/camera/l.java com/getcapacitor/b0.java com/getcapacitor/e0.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	com/amazon/c/a/a/c.java com/getcapacitor/a.java com/revenuecat/purchases/common/FileHelper.java q6/c.java s0/c.java
00012	Read data and put it into a buffer stream	file	com/amazon/c/a/a/c.java
00034	Query the current data network type	collection network	d3/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/getcapacitor/h1.java com/revenuecat/purchases/common/HTTPClient.java q4/g2.java r6/c.java
00089	Connect to a URL and receive input stream from the server	command network	com/codetrixstudio/capacitor/GoogleAuth/GoogleAuth.java com/getcapacitor/h1.java com/revenuecat/purchases/common/HTTPClient.java q4/g2.java r6/c.java
00109	Connect to a URL and get the response code	network command	com/revenuecat/purchases/common/HTTPClient.java q4/g2.java r6/c.java t3/e.java x2/d.java
00094	Connect to a URL and read data from it	command network	com/getcapacitor/h1.java d2/d.java
00108	Read the input stream from given URL	network command	com/getcapacitor/h1.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	a3/s.java c3/a.java com/amazon/a/a/i/a.java com/amazon/a/a/i/g.java com/amazon/device/iap/internal/a/a.java com/capacitorjs/plugins/applauncher/AppLauncherPlugin.java com/capacitorjs/plugins/camera/CameraPlugin.java com/getcapacitor/i.java q4/o0.java w3/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/amazon/device/drm/a/d/c.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/a/c/b.java com/capacitorjs/plugins/camera/CameraPlugin.java com/capacitorjs/plugins/pushnotifications/PushNotificationsPlugin.java com/getcapacitor/i.java d3/f2.java
00125	Check if the given file path exist	file	com/capacitorjs/plugins/camera/CameraPlugin.java com/getcapacitor/i.java
00036	Get resource file from res/raw directory	reflection	com/amazon/a/a/i/g.java com/capacitorjs/plugins/pushnotifications/v.java com/getcapacitor/i.java w3/g.java
00022	Open a file from given absolute path of the file	file	com/amazon/a/a/b/b.java com/capacitorjs/plugins/camera/CameraPlugin.java com/getcapacitor/e0.java s0/a.java v0/b.java
00075	Get location of the device	collection location	com/capacitorjs/plugins/geolocation/c.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	a3/s.java c3/a.java com/capacitorjs/plugins/applauncher/AppLauncherPlugin.java w3/g.java
00014	Read file into a stream and put it into a JSON object	file	q6/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00123	Save the response to JSON after connecting to the remote server	network command	d2/c.java
00153	Send binary data over HTTP	http	d2/c.java
00003	Put the compressed bitmap data into JSON object	camera	q4/o0.java
00054	Install other APKs from file	reflection	com/capacitorjs/plugins/camera/CameraPlugin.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/capacitorjs/plugins/camera/CameraPlugin.java
00024	Write file after Base64 decoding	reflection file	com/capacitorjs/plugins/camera/CameraPlugin.java
00192	Get messages in the SMS inbox	sms	com/getcapacitor/e0.java
00028	Read file from assets directory	file	com/getcapacitor/e0.java
00191	Get messages in the SMS inbox	sms	com/getcapacitor/e0.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/985220208374/namespaces/firebase:fetch?key=AIzaSyCaVLpQnSUwuwSCFsX4LUZmPtD81XkxocQ. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.WAKE_LOCK
Other Common Permissions	5/44	android.permission.BLUETOOTH, 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

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
play.google.com	ok	**IP:** 142.251.33.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
fundingchoicesmessages.google.com	ok	**IP:** 142.250.69.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
accounts.google.com	ok	**IP:** 142.251.111.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.amazon.com	ok	**IP:** 13.225.185.31 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
errors.rev.cat	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
support.google.com	ok	**IP:** 142.251.32.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
googlemobileadssdk.page.link	ok	**IP:** 142.250.69.97 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.googleapis.com	ok	**IP:** 142.251.33.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.250.69.36 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api-diagnostics.revenuecat.com	ok	**IP:** 34.224.198.224 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.69.98 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.revenuecat.com	ok	**IP:** 3.162.3.15 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api-paywalls.revenuecat.com	ok	**IP:** 18.211.236.74 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
api.revenuecat.com	ok	**IP:** 52.5.137.207 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
capacitorjs.com	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

✉ EMAILS

EMAIL	FILE
u0013android@android.com u0013android@android.com0	w3/v.java

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyCaVLpQnSUwuwSCFsX4LUZmPtD81XkxocQ"
"google_crash_reporting_api_key" : "AIzaSyCaVLpQnSUwuwSCFsX4LUZmPtD81XkxocQ"
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d003082010802820101000ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a

POSSIBLE SECRETS
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e04160414d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
BkxOKZDOMH8NUFJEmpCq1X+PtIP0kLI1Ua0ujwsrkUE=
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
ttuIHg/yfWDxJlotLoMLf9WBnVTbWFFKY03C8KHR8FAhIQHccw4LaDLJatYkpo23
fxU2A2MjpZ4aJWGzXeMNURilSCaKosw3oXImrqnhSVmXB+tMi32JakdNlHCV3t0c
1eWk7vHD3Ee+FybzKEoWLH07Pvdxo5flYR768ntLvpJZNSFjE7xgNzi+al9tiZC4
B3EEABB8EE11C2BE770B684D95219ECB
iibTgWRTbrwM2W7HZGJP5cjM0DLiCyA9TVVy1genRaa4nvgE3+CiRN/Fx87DVDsO

POSSIBLE SECRETS
7qOZVP58PfP3kLkbSBo98onihlohkIEpZC40FvE5nnCJ8ryn0NERK9JAnlww55zq
I5l5b06e/m6OPcJVryww5aceHDWuWNMRDm4mYVrBvJQ=
bObXLZFRWAdU6+me08AeNX2ciqxi45ddv3QSqAplzos=
NOrE2caDXO4nkFR2Fjy7NgGPKtPlIg1WAorknI/US68=
3PwoDnm3HnsskB+3ZnJHoZ7BzV0InxUqaAwJBlSwKFs=
ZVHCdOeJUA1S4bCrFb9VMsUCP8Sf65wDnbBE+q4M36k=
nIX5dAPvXYWFIvHlyxyLt0TnZ91UnAjFxZwf2qcoWSGcs+p5B5p88VCOzepPfMpE
y+BEEb1lYOUGwTehZ9VIg/2gibmtEOjDZzKXHhs5BV0=
1ZhioNexfONxLbr8oNixHPTbX/qv3RsJiyYoeeb0m+g=
MIrDuKB7N0O22daoYjLtFOJg5TtVRHK1+0ktwmGNtdU=
1OxyLDHu2cwu0U7XKtDO3q+DghLeQ8xcTgpGCDWDuEeCcfs+HPxSt8kldIfiq1K0
w5tjCRfZfXWJzckDvIkXwf5aGJEVejLzfxhnwyqJH5E=
8UC+BMIoCN+KAKrN9TZmuJsGMmo3RUHS+FjVMSp9QfgjxjGZ10kqO/oSdOn5Rw29
xLOAO7msIR4UFUyldUn5stL2wwbLdISu2CSlTLg4f6Q=
SMfJnKfhfLLyTw7dzHC+3CXVRNFLWK4N2mQHKB3gm/o=

POSSIBLE SECRETS
beFEMZ/YBSUug4MSXb2BKymKiM6ZxOOlxExWa37jMlM=
gL88T2vBvJS+jBemUvhPpVS5IeaU7cU4wFVgyT6PJl7pFldWXOd3mZxVZlQUSll5
Ee4p/yPQz67p3LoSNbpt1G8K9rDuoWxBYT8E4CbWyr8=
c103703e120ae8cc73c9248622f3cd1e
RSyr2AK130nKbepDTsaNV0Uv17TWUb4O6ebIiV3GgVs=
Q+fOnDUQnIPH75lusFutOgWOI4DeJ6z7X13oo1pZ5m19Kfyi56UOJglWSBqO3AzA
gzR6fJL0MpYPfJ/UkFL9UHjS7jlytQ+eyVRsQJTsxzK4yqDaskM4UtldyBDUp+Z9
zahwJ4oRFMB+Gn9BGkfZDZ8TzDEfKTB8Y6I4bT4vlwkVFXvqlnkWd7htbiUzWQyR
s7rU1m4XsqJ83s2reIjdkboWJYkg+gYouDrDcn3Ghpw=
s1ejGoWFNJedDDJqGqL3B22F5ZMvy0oaymBcWJepS9Hv4/6KtsHBpmbtFfwgqqen
aC7c3pDenGsdb0eFildzKOBrhobw8fKkmd52rTlBEKM=
9mv9Ihk+HlE8P3WJWSjhrxWrdB7cEu1gaxdteA5kBJ6DKumpWYk1Q5Vf8aocVg4i
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
ZHFOx+FjaOsul7gEkIcfA8auDnyRWXmT0qbiHVEO6U1RLulNSOFK3tPEgm+pvQxr
r6m9xWOlfK6iHuNH3QiJQf71aQCKDM6NhABQId+yaKg=

POSSIBLE SECRETS
sK9i540XcONymgaiZVMKYXr1VbNcwMhjwo2LFhhSCFg=
tfuuP59pzWN+H8zv1geT3jADiBKBGMQRjmCPoIvL5f45Lvl5qgJ0PgBqZF4WPnQj
zmLnsak1Fo/LHy30EeWswBCxcOoFKuH08l3DkSTUgzb476o6nI+C8ZUC+d8tLJwZ
A3EfeXObjqx38Tdc4wdTZSQNpfpw6YVck+944M4A/m0=
MbAcGuLi+XGl3MsgqAiQYLikemL120ZFxn+dIhaD+rHWJuTeO/M8+1c58cczHjCs
Y0trGqGVEUAa7A3LYgSQFKe4N9h1BuTC7OKFYCHfLSg=
qUEdP6yfmpdCkPVqoE8EyrX/MPjGh4YKRo5g3kOeMoc=
XCj6cS5OVeEeObzd394PGDbjTuQh+vSye2UT6221ugsKtO2/oznWOSes2cnebrVR
hMVcCX1S6+m7rVEDNdCHhVgXRFILMOQ9RgLSmTdPHeNgAU8CbmBsymKBuqLQcQaU
Jz2tk/JKeGJKcc4wwXH5Pf6ZM64fYgV4wWxByPOgNQE=
Eg2eC3eNesWzbAUINzxj1mXRcYgmzS654CxZFoVQbAM=
KHu8Xbxzr2mu9S25CNgKE5zXBf18Zj2waiAPYoFRjyhOXCyg+mYLv2x/JjCH7GjX
49f946663a8deb7054212b8adda248c6

PLAYSTORE INFORMATION

Title: Dateability

Score: 2.387097 **Installs:** 5,000+ **Price:** 0 **Android Version Support:** **Category:** Dating **Play Store URL:** com.dateabilityapp

Developer Details: Dateability, 8420511857358700422, 1312 17th Street Unit 2258 Denver, CO 80202, https://www.dateabilityapp.com, dateabilityapp@gmail.com,

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

Description:

Dateability is here to make love accessible. Dateability is the dating app designed for people with disabilities and chronic illnesses. We welcome people with physical, intellectual, and psychiatric disabilities to join and find their connection. Our inclusive dating app is LGBTQ+ friendly! At Dateability, we value inclusion, respect, and the importance of creating meaningful and healthy connections and we expect our members to act accordingly. We support each user and their individualized needs and preferences. Your profile includes common descriptors (height, political affiliation, education, etc.), but it also includes a section titled “Dateability Deets,” where you can include information about your disability, if desired. Dateability is free to use. Questions, concerns, or requests? Email support@dateabilityapp.com

SCAN LOGS

Timestamp	Event	Error
2024-11-17 23:39:49	Generating Hashes	OK
2024-11-17 23:39:49	Extracting APK	OK
2024-11-17 23:39:49	Unzipping	OK
2024-11-17 23:39:49	Getting Hardcoded Certificates/Keystores	OK
2024-11-17 23:39:49	Parsing APK with androguard	OK

2024-11-17 23:39:52	Parsing AndroidManifest.xml	OK
2024-11-17 23:39:52	Extracting Manifest Data	OK
2024-11-17 23:39:52	Performing Static Analysis on: Dateability (com.dateabilityapp)	OK
2024-11-17 23:39:52	Fetching Details from Play Store: com.dateabilityapp	OK
2024-11-17 23:39:52	Manifest Analysis Started	OK
2024-11-17 23:39:52	Checking for Malware Permissions	OK
2024-11-17 23:39:53	Fetching icon path	OK
2024-11-17 23:39:53	Library Binary Analysis Started	OK
2024-11-17 23:39:53	Reading Code Signing Certificate	OK
2024-11-17 23:39:53	Running APKiD 2.1.5	OK
2024-11-17 23:39:57	Detecting Trackers	OK

2024-11-17 23:40:00	Decompiling APK to Java with JADX	OK
2024-11-17 23:40:12	Converting DEX to Smali	OK
2024-11-17 23:40:12	Code Analysis Started on - java_source	OK
2024-11-17 23:40:15	Android SAST Completed	OK
2024-11-17 23:40:15	Android API Analysis Started	OK
2024-11-17 23:40:17	Android API Analysis Completed	OK
2024-11-17 23:40:17	Android Permission Mapping Started	OK
2024-11-17 23:40:21	Android Permission Mapping Completed	OK
2024-11-17 23:40:22	Email and URL Extraction Completed	OK
2024-11-17 23:40:22	Android Behaviour Analysis Started	OK
2024-11-17 23:40:24	Android Behaviour Analysis Completed	OK

2024-11-17 23:40:24	Extracting String data from APK	OK
2024-11-17 23:40:24	Extracting String data from Code	OK
2024-11-17 23:40:24	Extracting String values and entropies from Code	OK
2024-11-17 23:40:26	Performing Malware check on extracted domains	OK
2024-11-17 23:40:28	Saving to Database	OK

Report Generated by - MobSF v4.1.9

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.