ANDROID STATIC ANALYSIS REPORT

LifeMD (1.48.0)

File Name:	com.lifemd.care_134597615.apk
Package Name:	com.lifemd.care
Scan Date:	Aug. 30, 2025, 11:43 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	19	3	3	1

FILE INFORMATION

File Name: com.lifemd.care_134597615.apk
Size: 43.5MB
MD5: ccd369d4aa715a731a90ec2d797b9076
SHA1: a88cdaaa2a443aaa087a6cc5f36d812af22dc081
SHA256: 5214a933cae17f9250d135cd29ab65f350352f997276dfbae33db9582022e81f

APP INFORMATION

App Name: LifeMD
Package Name: com.lifemd.care
Main Activity: com.lifemd.care.MainActivity
Target SDK: 34
Min SDK: 29
Max SDK:
Android Version Name: 1.48.0

Android Version Code: 134597615

APP COMPONENTS

Activities: 15
Services: 16
Receivers: 17
Providers: 5
Exported Activities: 1
Exported Services: 2
Exported Receivers: 4
Exported Providers: 0

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: 2022-01-27 17:20:23+00:00
Valid To: 2052-01-27 17:20:23+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xafaaaca66c80f0352ec33c0c6a9fe99cea472437
Hash Algorithm: sha256
md5: 5153160b1a3b28fecc6c81f440dc9965
sha1: 9c8b447ed7c49f1b6df6d553fdf5237ccd983b3c
sha256: 940787f31e48d4cee538a71e73393a362d81dcf85aecf2739bc75fcb34ea407e
sha512: 7fa78f5fb3b485d238589be5da8c73450bb6b5fac29e4148cb2f73031ecb60c82646b998014cefffac4db36fcba7abbe2c1a0ebd6fbe124b9530819789c6d4f0
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 48b9467d9a26b9cda66c2a36fd9606bfdabade0f448746c09485e62e767e4590
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.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
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.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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_PHONE_CALL	normal	enables foreground services during phone calls.	Allows a regular application to use Service.startForeground with the type "phoneCall".
android.permission.MANAGE_OWN_CALLS	normal	enables a calling app to manage its own calls.	Allows a calling application which manages it own calls through the self-managed ConnectionService APIs.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
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.lifemd.care.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.samsung.android.mapsagent.permission.READ_APP_INFO	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
SIM operator check
network operator name check
ro.kernel.qemu check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.lifemd.care.MainActivity	Schemes: https://, Hosts: lifemd.page.link, *.lifemd.com, Path Prefixes: /f/a,
com.aboutyou.dart_packages.sign_in_with_apple.SignInWithAppleCallback	Schemes: signinwithapple://, Paths: /callback,

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
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	Activity (com.aboutyou.dart_packages.sign_in_with_apple.SignInWithAppleCallback) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Broadcast Receiver (flutter.moum.headset_event.HeadsetBroadcastReceiver) 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.
5	TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
6	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
7	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
9	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
10	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: **8** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A4/a.java A7/e.java C0/n.java D2/a.java D5/j.java E2/e.java E2/h.java E2/i.java E2/j.java F4/a.java G/u.java G4/i.java G4/j.java G8/c.java H0/i.java I/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				I2/d.java I5/d.java J4/f.java J7/m.java J7/n.java K4/b.java K7/a.java K7/c.java K7/j.java O7/C0556c0.java P8/c.java Q1/e.java R7/C0616i.java R7/g0.java T/d.java T1/f.java T1/l.java T7/b.java T7/o.java V/f.java V1/a.java V5/a.java V5/b.java V5/c.java V6/a.java V6/e.java V7/b.java W6/h.java W7/a.java W7/k.java W8/a.java X1/c.java X4/e.java X7/d.java Y/a.java Y1/d.java Y4/H.java Y7/n.java Z1/a.java Z4/C0707e.java Z6/b.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	Z8/a.java a7/C0746a.java c/AbstractC1031d.java com/aboutyou/dart_packages/sign_in_with_apple/SignInWithAppleCallback.java com/appsflyer/internal/AFg1aSDK.java com/baseflow/geolocator/GeolocatorLocationService.java com/baseflow/geolocator/b.java com/baseflow/geolocator/e.java com/baseflow/geolocator/f.java com/braze/support/BrazeLogger.java com/datadog/android/ndk/internal/NdkCrashLog.java com/datadog/android/rum/DdRumContentProvider.java com/datadog/android/rum/internal/domain/scope/RumViewScope.java com/pichillilorenzo/flutter_inappwebview_android/Util.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserActivity.java com/pichillilorenzo/flutter_inappwebview_android/service_worker/ServiceWorkerManager.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/FlutterWebView.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InputAwareWebView.java com/zipow/cmmlib/Logger.java d0/C1555e.java d3/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				e2/n.java e5/C1622a.java e6/e.java e7/b.java e7/e.java f0/C1635c.java g2/C1667a.java g3/C1670a.java h5/C1722h.java h6/e.java h6/m.java i0/C1730b.java i4/n.java io/flutter/embedding/engine/FlutterJNI.java io/flutter/embedding/engine/renderer/FlutterRenderer.java io/flutter/plugin/editing/d.java io/flutter/plugin/editing/f.java io/flutter/plugin/platform/SingleViewPresentation.java io/flutter/plugin/platform/c.java io/flutter/plugin/platform/l.java io/flutter/plugin/platform/r.java io/flutter/plugin/platform/t.java io/flutter/view/AccessibilityViewEmbedder.java j2/q.java j7/C1776E.java j7/C1787j.java j7/RunnableC1775D.java k/C1808m.java k/C1809n.java k/C1810o.java k/C1812q.java k/C1813r.java k/C1815t.java k0/C1821b.java l4/C1900a.java l4/C1901b.java l7/e.java m4/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				m4/l.java o2/C2037a.java r5/C2183a.java t4/C2246e.java u/C2266d0.java u/C2280k0.java u/Y.java u/r0.java u4/AbstractC2320b.java u4/C.java u4/C2321c.java u4/D.java u4/k.java u4/r.java u4/w.java u4/x.java u4/z.java u5/d.java us/zoom/internal/NativeBitmap.java v6/C2393b.java w/T.java w0/AbstractC2437a.java w6/C2474c.java x4/AbstractDialogInterfaceOnClickListenerC2575v.java x4/C2547F.java x4/C2552K.java x4/C2572s.java x5/C2586g.java x7/h.java x7/j.java x7/k.java x7/l.java x7/n.java x7/s.java x7/t.java y0/AbstractC2604c.java y7/C2622a.java y7/C2624c.java z2/e.java z2/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	V7/a.java V7/b.java com/zipow/cmmlib/AppUtil.java e7/b.java e7/e.java us/zoom/video_sdk/i.java
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	Y1/c.java com/pichillilorenzo/flutter_inappwebview_android/credential_database/CredentialDatabaseHelper.java j3/C1754A.java j3/p.java j3/t.java j7/C1787j.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	O8/c.java O8/d.java O8/g.java O8/h.java us/zoom/video_sdk/z.java
5	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	v6/C2393b.java w6/C2474c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	bo/app/e50.java bo/app/fv.java bo/app/gy.java bo/app/i70.java bo/app/jr.java bo/app/ju.java bo/app/kn.java bo/app/la0.java bo/app/q.java bo/app/rc.java bo/app/uh0.java bo/app/y60.java bo/app/zq.java
7	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	O7/D0.java T7/k.java e7/e.java i7/b.java us/zoom/reflection/utils/AppUtilsReflection.java v6/C2394c.java w/C2436u.java
8	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	U3/a.java W6/h.java k/C1813r.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	D0/a.java W7/j.java com/appsflyer/appsflyersdk/AppsFlyerConstants.java com/braze/configuration/BrazeConfig.java com/datadog/android/api/net/RequestFactory.java com/datadog/android/log/internal/LogsFeature.java com/datadog/android/rum/internal/FeaturesContextResolver.java com/datadog/android/rum/internal/domain/event/RumEventMeta.java com/datadog/android/rum/internal/domain/scope/ExternalResourceTimingsKt.java com/datadog/android/rum/internal/domain/scope/RumRawEvent.java com/datadog/android/rum/internal/domain/scope/RumSessionScope.java com/datadog/android/rum/internal/domain/scope/RumViewInfo.java com/datadog/android/rum/internal/metric/SessionEndedMetric.java com/pichillilorenzo/flutter_inappwebview_android/credential_database/URLCredentialContract.java com/pichillilorenzo/flutter_inappwebview_android/types/ClientCertResponse.java com/pichillilorenzo/flutter_inappwebview_android/types/HttpAuthResponse.java t2/d.java us/zoom/libtools/storage/PreferenceUtil.java us/zoom/libtools/storage/ZmSharePreferenceHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	D5/a.java I5/o.java
11	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	J0/b.java P3/L.java S3/b.java U0/T.java bo/app/w30.java com/appsflyer/internal/AFa1vSDK.java com/appsflyer/internal/AFi1fSDK.java com/braze/support/IntentUtils.java q8/C2160a.java
12	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	us/zoom/net/dns/DnsServersDetector.java us/zoom/video_sdk/z.java
13	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/braze/support/StringUtils.java us/zoom/video_sdk/z.java
14	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/editing/b.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFc1kSDK.java com/datadog/android/rum/tracking/ActivityLifecycleTrackingStrategy.java com/lifemd/care/services/CallNotificationService.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ActionBroadcastReceiver.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	A7/d.java T7/k.java V7/b.java Y1/d.java Z1/a.java Z8/a.java bo/app/bj0.java bo/app/ea.java bo/app/fa.java bo/app/gp.java bo/app/yd0.java bo/app/zc.java com/braze/e0.java com/braze/support/BrazeImageUtils.java com/datadog/android/core/internal/persistence/BatchId.java com/datadog/android/ndk/internal/NdkCrashReportsFeature.java com/zipow/cmmlib/AppContext.java e7/b.java e7/e.java l0/C1885p.java l0/C1886q.java l0/C1891v.java us/zoom/video_sdk/i.java w/C2436u.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	E2/e.java E2/h.java E2/j.java T7/k.java X7/c.java com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1kSDK.java com/baseflow/geolocator/e.java com/braze/ui/inappmessage/views/InAppMessageHtmlBaseView.java com/braze/ui/support/UriUtils.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsChannelDelegate.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/TrustedWebActivity.java e7/b.java us/zoom/video_sdk/l0.java y2/C2613a.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	E2/e.java E2/h.java E2/j.java X7/c.java com/baseflow/geolocator/e.java us/zoom/video_sdk/l0.java y2/C2613a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	E0/t.java E2/e.java E2/h.java com/appsflyer/internal/AFj1tSDK.java com/appsflyer/internal/AFj1wSDK.java com/appsflyer/internal/AFj1xSDK.java com/baseflow/geolocator/e.java com/braze/ui/support/UriUtils.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java h4/F.java us/zoom/video_sdk/i.java
00096	Connect to a URL and set request method	command network	E0/j.java com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1lSDK.java com/pichillilorenzo/flutter_inappwebview_android/Util.java h4/r.java w6/C2474c.java
00089	Connect to a URL and receive input stream from the server	command network	E0/j.java com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1lSDK.java h4/r.java w6/C2474c.java
00109	Connect to a URL and get the response code	network command	E0/j.java com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1lSDK.java com/appsflyer/internal/AFf1kSDK.java h4/r.java l4/C1901b.java t4/RunnableC2245d.java w6/C2474c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	E0/c.java E0/t.java S8/p.java Z8/a.java bo/app/pr.java bo/app/wc0.java com/appsflyer/internal/AFa1ySDK.java com/appsflyer/internal/AFb1jSDK.java com/braze/support/BrazeImageUtils.java com/datadog/android/core/internal/persistence/file/batch/PlainBatchFileReaderWriter.java com/pichillilorenzo/flutter_inappwebview_android/Util.java com/zipow/annotate/ImageUtil.java com/zipow/cmmlib/AppContext.java e7/e.java h4/C1709g.java h4/F.java k8/C1844g.java l0/C1885p.java l0/InterfaceC1883n.java n0/C1944e.java s7/C2216d.java us/zoom/internal/NativeBitmap.java us/zoom/video_effects/b.java us/zoom/video_sdk/i.java us/zoom/video_sdk/l0.java us/zoom/video_sdk/r.java us/zoom/video_sdk/t.java v6/C2394c.java w/C2436u.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFj1tSDK.java com/appsflyer/internal/AFj1vSDK.java com/appsflyer/internal/AFj1xSDK.java us/zoom/video_sdk/i.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFi1rSDK.java
00030	Connect to the remote server through the given URL	network	E0/j.java com/pichillilorenzo/flutter_inappwebview_android/Util.java h4/r.java
00094	Connect to a URL and read data from it	command network	E0/j.java com/pichillilorenzo/flutter_inappwebview_android/Util.java h4/r.java
00108	Read the input stream from given URL	network command	E0/j.java h4/r.java
00102	Set the phone speaker on	command	f7/e.java org/webrtc/voiceengine/AudioDeviceAndroidAAudio.java org/webrtc/voiceengine/AudioDeviceAndroidOpenSLESHelper.java
00056	Modify voice volume	control	f7/e.java org/webrtc/voiceengine/AudioDeviceAndroidOpenSLESHelper.java
00002	Open the camera and take picture	camera	com/zipow/nydus/camera/CameraCaptureImplV1.java
00183	Get current camera parameters and change the setting.	camera	com/zipow/nydus/camera/CameraCaptureImplV1.java com/zipow/nydus/camera/CameraMgrV1.java

RULE ID	BEHAVIOUR	LABEL	FILES
00028	Read file from assets directory	file	E0/a.java h4/C1705c.java
00132	Query The ISO country code	telephony collection	Y0/h.java h4/p.java
00161	Perform accessibility service action on accessibility node info	accessibility service	f0/C1635c.java io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/c.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	f0/C1635c.java io/flutter/view/AccessibilityViewEmbedder.java
00012	Read data and put it into a buffer stream	file	com/datadog/android/core/internal/persistence/file/batch/PlainBatchFileReaderWriter.java e7/e.java us/zoom/video_sdk/i.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	B0/a.java com/zipow/annotate/ImageUtil.java
00079	Hide the current app's icon	evasion	u2/m.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1lSDK.java us/zoom/video_sdk/i.java
00123	Save the response to JSON after connecting to the remote server	network command	com/pichillilorenzo/flutter_inappwebview_android/Util.java

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	O8/b.java O8/h.java
00163	Create new Socket and connecting to it	socket	O8/b.java O8/h.java
00014	Read file into a stream and put it into a JSON object	file	v6/C2394c.java
00202	Make a phone call	control	E2/j.java
00203	Put a phone number into an intent	control	E2/j.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1lSDK.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1lSDK.java
00208	Capture the contents of the device screen	collection screen	us/zoom/internal/share/ScreenShareServer.java
00209	Get pixels from the latest rendered image	collection	us/zoom/internal/share/ScreenShareServer.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/861261954957/namespaces/firebase:fetch?key=AIzaSyDyiyGhF2qqJ4i5kdohowUb1B-OnWxQP44. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.READ_PHONE_STATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	8/44	android.permission.BLUETOOTH, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.READ_CALENDAR, android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH_ADMIN, android.permission.BROADCAST_STICKY, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_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
sdk.iad-01.braze.com	ok	**IP:** 172.64.148.188 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.251.40.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.250.217.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
www.braze.com	ok	**IP:** 104.17.227.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sondheim.braze.com	ok	**IP:** 104.18.43.4 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.189.2 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
g.co	ok	**IP:** 142.250.72.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.example.com	ok	**IP:** 23.220.73.43 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map
youtrack.jetbrains.com	ok	**IP:** 63.33.88.220 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
accounts.google.com	ok	**IP:** 142.250.101.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
iamcache.braze	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developer.apple.com	ok	**IP:** 17.253.83.131 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
docs.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sapp.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
zoom.us	ok	**IP:** 170.114.52.2 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.333698 **Longitude:** -121.889297 **View:** Google Map
aomedia.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12

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

HARDCODED SECRETS

POSSIBLE SECRETS
"com_braze_api_key" : "5da9e158-3bff-4a09-9c25-51e2781c97cd"
"com_braze_firebase_cloud_messaging_sender_id" : "861261954957"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"google_api_key" : "AIzaSyDyiyGhF2qqJ4i5kdohowUb1B-OnWxQP44"
"google_crash_reporting_api_key" : "AIzaSyDyiyGhF2qqJ4i5kdohowUb1B-OnWxQP44"
5181942b9ebc31ce68dacb56c16fd79f
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212

POSSIBLE SECRETS
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
ae2044fb577e65ee8bb576ca48a2f06e
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkK
37a6259cc0c1dae299a7866489dff0bd
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1

PLAYSTORE INFORMATION

Title: LifeMD

Score: 4.827586 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.lifemd.care

Developer Details: LifeMD, LifeMD, None, https://lifemd.com/, stefan@lifemd.com,

Release Date: Jan 28, 2022 **Privacy Policy:** Privacy link

Description:

Nationwide access to the best online medical providers and prescriptions. No insurance needed. Access a new kind of healthcare with LifeMD. It's transparent healthcare that you can trust, without co-pays, surprise medical bills, or unnecessary specialist visits and diagnostics. LifeMD offers the best virtual healthcare, at the best price, from the best medical providers. Our medical providers aren't influenced by insurance companies or motivated by referrals. Their care and focus is only on providing their patients with the highest quality virtual care. Our providers can treat over 3,500 medical conditions online and are committed to providing exceptional care and a healthier you! LifeMD's medical providers are highly rated, well educated, and committed to your long term health. While many telehealth platforms assign you a random provider for each visit, LifeMD gives you a medical provider that gets to know you and your health, works with you over time to optimize your health, helps you to manage chronic conditions, and delivers personalized care for better outcomes and a healthier life. Your virtual visit with a LifeMD provider may be one of the most thorough medical visits you've ever had. Your provider will ask about your medical history, current symptoms, lifestyle, and the medications and supplements you currently take. Your provider will then provide a personalized treatment plan for you, and if appropriate, a prescription. What does LifeMD treat? Primary care for: • Acne • Allergies • Anxiety • Asthma • Back pain • Constipation • Depression • Diabetes • Erectile Dysfunction • Hair Loss • High Blood Pressure • High cholesterol/triglycerides • Insomnia/Sleep • Nail fungus • Osteoarthritis • Reflux [GERD] • Thyroid conditions • Weight-Loss Urgent Care for: • Allergies • Bronchitis • Colds • Dental infections • Diarrhea • Ear pain • Flu • Headache/migraines • Nausea • PrEP • Pink eye • Pneumonia • Rash • Sinus infection • Strep throat • Mild to moderate sunburn • Tonsillitis • UTIs • Vaginitis • Yeast Infections • And many more... Common prescriptions our medical providers write: • Anti-inflammatories • Antibiotics • Antiviral Medications • Antidepressants • Antipsychotics • Asthma control • Birth Control • Cholesterol medications • Diabetic medications • Diuretics • High blood pressure medication • PrEP • And many more... Access a new kind of healthcare with LifeMD. It's transparent healthcare that you can trust, without co-pays, surprise medical bills, or unnecessary specialist visits and diagnostics. LifeMD offers the best virtual healthcare, at the best price, from the best medical providers. Please also review our privacy policy. Notice of Collection: https://lifemd.com/ccpa

SCAN LOGS

Timestamp	Event	Error
2025-08-30 23:43:07	Generating Hashes	OK
2025-08-30 23:43:07	Extracting APK	OK
2025-08-30 23:43:07	Unzipping	OK
2025-08-30 23:43:07	Parsing APK with androguard	OK
2025-08-30 23:43:07	Extracting APK features using aapt/aapt2	OK

2025-08-30 23:43:07	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 23:43:09	Parsing AndroidManifest.xml	OK
2025-08-30 23:43:09	Extracting Manifest Data	OK
2025-08-30 23:43:09	Manifest Analysis Started	OK
2025-08-30 23:43:10	Performing Static Analysis on: LifeMD (com.lifemd.care)	OK
2025-08-30 23:43:11	Fetching Details from Play Store: com.lifemd.care	OK
2025-08-30 23:43:15	Checking for Malware Permissions	OK
2025-08-30 23:43:15	Fetching icon path	OK
2025-08-30 23:43:15	Library Binary Analysis Started	OK
2025-08-30 23:43:15	Reading Code Signing Certificate	OK

2025-08-30 23:43:16	Running APKiD 2.1.5	OK
2025-08-30 23:43:20	Detecting Trackers	OK
2025-08-30 23:43:22	Decompiling APK to Java with JADX	OK
2025-08-31 00:02:24	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/ccd369d4aa715a731a90ec2d797b9076/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/ccd369d4aa715a731a90ec2d797b9076/ccd369d4aa715a731a90ec2d797b9076.apk'], 999.9999851956964)
2025-08-31 00:02:24	Converting DEX to Smali	OK
2025-08-31 00:02:24	Code Analysis Started on - java_source	OK
2025-08-31 00:02:29	Android SBOM Analysis Completed	OK
2025-08-31 00:02:34	Android SAST Completed	OK
2025-08-31 00:02:34	Android API Analysis Started	OK
2025-08-31 00:02:42	Android API Analysis Completed	OK

2025-08-31 00:02:43	Android Permission Mapping Started	OK
2025-08-31 00:03:02	Android Permission Mapping Completed	OK
2025-08-31 00:03:03	Android Behaviour Analysis Started	OK
2025-08-31 00:03:14	Android Behaviour Analysis Completed	OK
2025-08-31 00:03:14	Extracting Emails and URLs from Source Code	OK
2025-08-31 00:03:18	Email and URL Extraction Completed	OK
2025-08-31 00:03:18	Extracting String data from APK	OK
2025-08-31 00:03:18	Extracting String data from Code	OK
2025-08-31 00:03:18	Extracting String values and entropies from Code	OK
2025-08-31 00:03:20	Performing Malware check on extracted domains	OK

2025-08-31 00:03:24	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.