



ANDROID STATIC ANALYSIS REPORT

CT

 Therapy (7.0.0.7)

File Name:

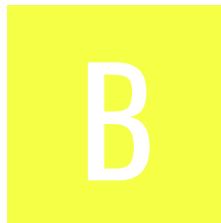
base.apk

Package Name: com.constanttherapy.android.main

Scan Date: Nov. 28, 2024, 1:57 a.m.






App Security Score: 49/100 (MEDIUM RISK)

Grade:



Trackers Detection: 4/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
3	21	2	2	2

FILE INFORMATION

File Name: base.apk

Size: 22.32MB

MD5: d66f70f0a21a7993a997c61f6058ab7c

SHA1: 208f6884b4a9d10814d43094d122d3d7184b3fd8

SHA256: 36731a7129bbfb49ef94f6fa01f0a8dc52f0d76efb7631021e3f7a01d375099c

APP INFORMATION

App Name: Therapy

Package Name: com.constanttherapy.android.main

Main Activity: com.constanttherapy.android.main.SplashScreenActivity

Target SDK: 35

Min SDK: 23

Max SDK:

Android Version Name: 7.0.0.7

Android Version Code: 700007

APP COMPONENTS

Activities: 65

Services: 12

Receivers: 6
Providers: 4
Exported Activities: 4
Exported Services: 0
Exported Receivers: 3
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=MA, L=Lexington, CN=Veera Anantha
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-11-05 01:27:34+00:00
Valid To: 2039-10-30 01:27:34+00:00
Issuer: C=US, ST=MA, L=Lexington, CN=Veera Anantha
Serial Number: 0x54597d06
Hash Algorithm: sha1
md5: 16a562013716ac4982b3201f4e1e97be
sha1: 672a8e38301737339d4c3494d3395218a6cd169f
sha256: 678ab86a86fca878676386b5a5e24bc10b10a0484f5cc44a2faec48430750eb9
sha512: 39276e329e4ba6fef76c901e7e7ea8452710550c4eb68032498586de612797598f818c5aa1d63a742194a120c7e1c86c84fc4c2cca981f706069b35db1950079
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: a814d1a9bb1d70258f43a016b7a79a2d21b42d9e160e3588768d51e2cd5457db
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
------------	--------	------	-------------

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.constanttherapy.android.main.permission.RECEIVE_ADM_MESSAGE	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.amazon.device.messaging.permission.RECEIVE	unknown	Unknown permission	Unknown permission from android reference
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.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_AD SERVICES_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_AD SERVICES_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.
com.constanttherapy.android.main.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check SIM operator check network operator name check ro.kernel.qemu check
	Obfuscator	Kiwi encrypter
	Compiler	r8 without marker (suspicious)
classes2.dex	FINDINGS	DETAILS
	Compiler	unknown (please file detection issue!)
classes3.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.TAGS check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes4.dex	FINDINGS	DETAILS
	Anti Debug Code	Debug.isDebuggerConnected() check
	Anti-VM Code	Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check network operator name check possible VM check
	Compiler	r8 without marker (suspicious)
classes5.dex	FINDINGS	DETAILS
	Compiler	r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.constanttherapy.android.main.SplashScreenActivity	Schemes: ctapp://, https://, Hosts: login, app.constanttherapy.com, appstaging.constanttherapy.com, appdev.constanttherapy.com, Path Prefixes: /login, Path Patterns: /login,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | 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.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 9 | 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	Activity (com.constanttherapy.android.main.flow.activity.PatientSignUpActivity) 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	Activity (com.constanttherapy.android.advancedmode.AdvancedModeActivity) 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.
5	Activity (com.constanttherapy.android.main.features.subscribe.SubscriptionActivity) 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.
6	Activity (com.constanttherapy.android.homescreen.PatientHomeActivity) 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.
7	Content Provider (com.constanttherapy.android.provider.CacheFileProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	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.

NO	ISSUE	SEVERITY	DESCRIPTION
9	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.
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: 2 | WARNING: 8 | INFO: 1 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptechnology/load/Option.java com/bumptechnology/load/engine/DataCacheKey.java com/bumptechnology/load/engine/EngineResource.java com/bumptechnology/load/engine/ResourceCacheKey.java com/bumptechnology/manager/RequestManagerRetriever.java com/constanttherapy/android/advancedmode/clinician/patientList/PatientListActivity.java com/constanttherapy/android/advancedmode/clinician/patientList/email/PatientEmailActivity.java com/constanttherapy/android/advancedmode/clinician/patientList/instructions/PatientInstructionsActivity.java com/constanttherapy/android/bridge/BridgeActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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: MSTS STORAGE 1.1	com/constanttherapy/android/bridge/BridgeActivity.java com/constanttherapy/android/fragments/AudioFragment.java com/constanttherapy/android/fragments/DropFragment.java com/constanttherapy/android/fragments/WordFragment.java com/constanttherapy/android/fragments/image/FunctionalMathData.java com/constanttherapy/android/fragments/image/FunctionalMathWebViewFragment.java com/constanttherapy/android/fragments/image/ImageAudioFragment.java com/constanttherapy/android/fragments/image/ImageFragment.java com/constanttherapy/android/fragments/image/ImageFragmentBase.java com/constanttherapy/android/fragments/image/LabeledImageFragment.java com/constanttherapy/android/fragments/image/RotatableImageFragment.java com/constanttherapy/android/homescreen/password/ChangePasswordObject.java com/constanttherapy/android/homescreen/patientsettings/dialog/AddATherapistObject.java com/constanttherapy/android/homescreen/patientsettings/model/AddClinicianBody.java com/constanttherapy/android/homescreen/patientsettings/model/TherapistData.java com/constanttherapy/android/main/HomeworkInstructionsActivity.java com/constanttherapy/android/main/data/network/api/AuthInterceptor.java com/constanttherapy/android/main/data/network/values/ChangePasswordObject.java com/constanttherapy/android/main/data/network/values/SelectionListItem.java com/constanttherapy/android/main/data/network/values/ServiceResetPassword.java com/constanttherapy/android/main/data/network/values/UserTypeResponse.java com/constanttherapy/android/main/features/forgot/ForgotPopup.java com/constanttherapy/android/main/features/landing/LandingScreen.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
			OWASP MASVS: MSTG-STORAGE-T4	andingscreen.java com/constanttherapy/android/main/features/landing/clinician/ClinicianLandingScreen.java com/constanttherapy/android/main/features/login/CommonRequestData.java com/constanttherapy/android/main/features/login/LoginRequestData.java com/constanttherapy/android/main/features/login/TypeOfUserData.java com/constanttherapy/android/main/features/login/mfa/MfaActivity.java com/constanttherapy/android/main/features/login/screen/LoginPresenter.java com/constanttherapy/android/main/features/signup/clinician/ClinicianAccount.java com/constanttherapy/android/main/features/signup/patientByClinician/PatientByClinicianSignupData.java com/constanttherapy/android/main/features/user/AddPatientByClinicianRequestBody.java com/constanttherapy/android/main/features/user/AutoValue_User.java com/constanttherapy/android/main/features/user/PatientUser.java com/constanttherapy/android/main/features/user/Users.java com/constanttherapy/android/main/flow/activity/PatientSignUpActivity.java com/constanttherapy/android/parade/NewParade.java com/constanttherapy/android/provider/TherapyContract.java com/constanttherapy/android/scoring/SessionSummaryActivity.java com/constanttherapy/android/service/SyncService.java com/constanttherapy/android/share/util/ImageMapData.java com/constanttherapy/android/signup/v3/api/AutoValue_Account.java com/constanttherapy/android/signup/v3/api/AutoValue_SignupFields.java com/constanttherapy/android/signup/v3/api/SignupStrings.java com/constanttherapy/android/util/AppsFlyerSdkHelper.java com/constanttherapy/android/util/BundleKeys.java com/constanttherapy/android/util/SharedPrefHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				va flow/internal/LifecycleIntegration.java flow/State.java
				io/grpc/internal/DnsNameResolver.java io/grpc/internal/ServiceConfigUtil.java io/grpc/internal/TransportFrameUtil.java io/opencensus/metrics/AutoValue_LabelKey.java io/opencensus/tags/AutoValue_Tag.java io/opencensus/trace/AutoValue_Tracestate_Entry.java org/jboss/logging/LoggerProviders.java rx/internal/schedulers/NewThreadWorker.java
				butterknife/ButterKnife.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 va com/amazon/device/simplesignin/SimpleSignInService.java ava 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/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1uSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1cSDK.java com/appsflyer/internal/AFf1dSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1kSDK.java com/appsflyer/internal/AFf1ISDK.java com/appsflyer/internal/AFf1tSDK.java com/appsflyer/internal/AFg1hSDK.java com/appsflyer/internal/AFg1jSDK.java com/appsflyer/internal/AFg1nSDK.java com/appsflyer/share/CrossPromotionHelper.java com/appsflyer/share/LinkGenerator.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableT

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information OWASP MASVS: MSTG-STORAGE-3	oBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareC onfigState.java com/bumptech/glide/load/resource/bitmap/Transform ationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDeco der.java com/bumptech/glide/load/resource/gif/ByteBufferGifD ecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEnc oder.java com/bumptech/glide/load/resource/gif/StreamGifDeco der.java com/bumptech/glide/manager/DefaultConnectivityMon itor.java com/bumptech/glide/manager/DefaultConnectivityMon itorFactory.java com/bumptech/glide/manager/RequestManagerFragme nt.java com/bumptech/glide/manager/RequestManagerRetriev er.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManage rFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget .java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSign ature.java com/bumptech/glide/util/ContentLengthInputStream.ja va com/bumptech/glide/util/pool/FactoryPools.java com/constanttherapy/android/main/data/network/api/ ApiUtils.java com/constanttherapy/android/main/features/app_versi on/AppVersionCallback.java com/constanttherapy/android/main/features/signup/ac count/AccountScreen\$onFinishInflate\$2.java com/constanttherapy/android/service/SyncService.java com/constanttherapy/android/widget/CustomTextureVi ew.java com/github/mikephil/charting/charts/BarChart.java

NO	ISSUE	SEVERITY	STANDARDS	com/github/mikephil/charting/charts/BarLineChartBase FILES com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/components/AxisBase.java com/github/mikephil/charting/data/ChartData.java com/github/mikephil/charting/listener/BarLineChartTouchListener.java com/github/mikephil/charting/utils/FileUtils.java com/github/mikephil/charting/utils/Utils.java com/h6ah4i/android/widget/advrecyclerview/animators/GeneralItemAnimator.java com/h6ah4i/android/widget/advrecyclerview/animators/impl/ItemAddAnimationManager.java com/h6ah4i/android/widget/advrecyclerview/animators/impl/ItemChangeAnimationManager.java com/h6ah4i/android/widget/advrecyclerview/animators/impl/ItemMoveAnimationManager.java com/h6ah4i/android/widget/advrecyclerview/animators/impl/ItemRemoveAnimationManager.java com/h6ah4i/android/widget/advrecyclerview/draggable/DraggableItemWrapperAdapter.java com/h6ah4i/android/widget/advrecyclerview/draggable/RecyclerViewDragDropManager.java com/nuance/nmdp/speechkit/cg.java com/nuance/nmdp/speechkit/j.java com/nuance/nmsp/client/sdk/oem/d.java fr/tvbarthel/lib/blurdialogfragment/BlurDialogEngine.java fr/tvbarthel/lib/blurdialogfragment/RenderScriptBlurHelper.java io/grpc/okhttp/internal/Platform.java org/slf4j/helpers/Util.java org/slf4j/impl/AndroidLoggerAdapter.java rx/internal/util/IndexedRingBuffer.java rx/internal/util/RxRingBuffer.java rx/plugins/RxJavaHooks.java timber/log/Timber.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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 com/constanttherapy/android/main/BuildConfig.java com/nuance/nmdp/speechkit/ax.java
4	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	com/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFb1gSDK.java com/appsflyer/internal/AFc1fSDK.java com/constanttherapy/android/adapters/SequenceDragAdapter.java com/constanttherapy/android/fragments/ActiveSentenceCompletionDragFragment.java com/constanttherapy/android/fragments/AuditoryCommandDragFragment.java com/constanttherapy/android/fragments/OrderWordByConceptDragFragment.java com/constanttherapy/android/fragments/SequenceDragFragment.java com/constanttherapy/android/fragments/SpokenWordGridDragFragment.java com/constanttherapy/android/fragments/WrittenDragFragment.java com/constanttherapy/android/fragments/matching/DragMatchingFragment.java com/constanttherapy/android/fragments/oddoneout/OddOneOutDragFragment.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/ExponentialBackoffPolicy.java io/grpc/internal/RetriableStream.java io/grpc/okhttp/OkHttpClientTransport.java io/grpc/util/RoundRobinLoadBalancer.java io/opencensus/trace/SpanId.java io/opencensus/trace/TraceId.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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/constanttherapy/android/provider/TherapyDatabase.java
6	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/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java
7	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/nuance/nmsp/client/sdk/oem/f.java io/grpc/okhttp/OkHttpChannelBuilder.java io/grpc/okhttp/internal/Util.java
8	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/constanttherapy/android/main/features/login/sso/DialogSSOLoginFragment.java com/constanttherapy/android/main/features/subscribe/win11/DialogWindowsSubscriptionActivity.java
9	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 com/constanttherapy/android/main/app/PicassoHelper.java com/constanttherapy/android/main/data/network/NetworkRepo.java com/nuance/nmdp/speechkit/eh.java io/grpc/okhttp/OkHttpChannelBuilder.java
10	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/constanttherapy/android/main/app/App.java
11	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	io/grpc/okhttp/internal/Util.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/bumptechnology/glide/BuildConfig.java com/bumptechnology/glide/gifdecoder/BuildConfig.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	-----	-----------------	-------	-------	---------	---------	---------------------

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libnmsp_sk_speex.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi/libnmsp_sk_speex.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>No RELRO high</p> <p>This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	x86/libnmsp_sk_speex.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	arm64-v8a/libnmsp_sk_speex.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86_64/libnmsp_sk_speex.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	armeabi-v7a/libnmsp_sk_speex.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi/libnmsp_sk_speex.so	<p>False high</p> <p>The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>No RELRO high</p> <p>This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86/libnmsp_sk_speex.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	arm64-v8a/libnmsp_sk_speex.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86_64/libnmsp_sk_speex.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p>	<p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>False warning</p> <p>Symbols are available.</p>

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/amazon/a/a/i/a.java com/amazon/a/a/i/g.java com/amazon/device/iap/internal/a/a.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1vSDK.java com/constanttherapy/android/advancedmode/clinician/patientList/qr/PatientQRActivity.java com/constanttherapy/android/advancedmode/clinician/transferToDirect/CanDoHomeworkActivity.java com/constanttherapy/android/advancedmode/tasks/TaskDetailsDialog.java com/constanttherapy/android/homescreen/screen/ReportSender.java com/constanttherapy/android/main/HomeworkInstructionsActivity.java com/constanttherapy/android/main/features/app_version/AppVersionCallback.java com/constanttherapy/android/main/features/help/HelpScreen.java com/constanttherapy/android/main/features/landing/clinician/ClinicianLandingScreen.java com/constanttherapy/android/main/features/login/mismatchAccount/PatientAndClinicianMismatchScreen.java com/constanttherapy/android/main/features/subscribe/SubscribeDialogFactory.java com/constanttherapy/android/scoring/SessionSummaryActivity.java com/constanttherapy/android/util/Prompt.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/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1vSDK.java com/constanttherapy/android/advancedmode/AdvancedModeActivity.java com/constanttherapy/android/advancedmode/clinician/patientList/email/PatientEmailActivity.java com/constanttherapy/android/advancedmode/clinician/patientList/instructions/PatientInstructionsActivity.java com/constanttherapy/android/advancedmode/clinician/patientList/qr/PatientQRActivity.java com/constanttherapy/android/advancedmode/clinician/removePatient/RemovePatientActivity.java com/constanttherapy/android/advancedmode/clinician/transferToDirect/CanDoHomeworkActivity.java com/constanttherapy/android/assessment/ClinicianTaskSummaryActivity.java com/constanttherapy/android/assessment/TaskSummaryActivity.java com/constanttherapy/android/firebase/CtNotificationManager.java com/constanttherapy/android/main/features/login/mfa/MfaActivity.java com/constanttherapy/android/main/features/subscribe/win11/DialogWindowsSubscriptionActivity.java com/constanttherapy/android/main/flow/activity/PatientSignUpActivity.java com/constanttherapy/android/parade/BaseParade.java com/constanttherapy/android/service/SyncService.java
00022	Open a file from given absolute path of the file	file	com/amazon/a/a/b/b.java com/appsflyer/internal/AFg1jSDK.java com/constanttherapy/android/fragments/DrawingFragment.java com/constanttherapy/android/fragments/ResizableWebViewFragment.java com/constanttherapy/android/main/data/audio/LifecycleAwareSimpleMediaPlayer.java com/constanttherapy/android/main/data/recog/CTRecognitionClient.java com/constanttherapy/android/util/ScreenshotCapturer.java com/fasterxml/jackson/databind/ser/std/FileSerializer.java com/github/mikephil/charting/charts/Chart.java com/jakewharton/picasso/OkHttp3Downloader.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1bSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1jSDK.java
00162	Create InetAddress object and connecting to it	socket	io/grpc/okhttp/internal/Platform.java
00163	Create new Socket and connecting to it	socket	io/grpc/okhttp/internal/Platform.java
00013	Read file and put it into a stream	file	com/amazon/c/a/a/c.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1jSDK.java com/bumptechnology/glide/disklru/DiskLruCache.java com/bumptechnology/glide/load/model/FileLoader.java com/constanttherapy/android/main/data/recog/AudioFileTransformer.java com/constanttherapy/android/main/data/recog/CTRecognitionClient.java com/fasterxml/jackson/core/JsonFactory.java com/fasterxml/jackson/core/TokenStreamFactory.java com/fasterxml/jackson/databind/ObjectReader.java okio/Okio__JvmOkioKt.java org.threeten/bp/chrono/HijrahDate.java
00023	Start another application from current application	reflection control	com/constanttherapy/android/main/features/landing/clinician/ClinicianLandingScreen.java com/constanttherapy/android/main/features/login/mismatchAccount/PatientAndClinicianMismatchScreen.java
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/bumptechnology/glide/load/data/HttpUrlFetcher.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/appsflyer/internal/AFf1jSDK.java com/bumptechnology/load/data/HttpUrlFetcher.java
00202	Make a phone call	control	com/constanttherapy/android/main/features/help/HelpScreen.java
00203	Put a phone number into an intent	control	com/constanttherapy/android/main/features/help/HelpScreen.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/constanttherapy/android/main/features/app_version/AppVersionCallback.java com/constanttherapy/android/main/features/help/HelpScreen.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFi1xSDK.java com/constanttherapy/android/advancedmode/clinician/settings/CheckInternetConnectionDialog.java com/constanttherapy/android/main/features/check_network/CheckNetworkScreen.java com/nuance/nmdp/speechkit/j.java
00036	Get resource file from res/raw directory	reflection	com/amazon/a/a/i/g.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFf1qSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1nSDK.java
00012	Read data and put it into a buffer stream	file	com/amazon/c/a/a/c.java
00056	Modify voice volume	control	com/constanttherapy/android/parade/NewParade.java com/constanttherapy/android/parade/Parade.java
00034	Query the current data network type	collection network	com/constanttherapy/android/advancedmode/clinician/settings/CheckInternetConnectionDialog.java com/constanttherapy/android/main/features/check_network/CheckNetworkScreen.java

RULE ID	BEHAVIOUR	LABEL	FILES
00130	Get the current WIFI information	wifi collection	com/constanttherapy/android/advancedmode/clinician/settings/CheckInternetConnectionDialog.java com/constanttherapy/android/main/features/check_network/CheckNetworkScreen.java
00175	Get notification manager and cancel notifications	notification	com/constanttherapy/android/firebase/CtNotificationManager.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1bSDK.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1bSDK.java com/bumptechnology/load/data/mediastore/ThumbFetcher.java
00025	Monitor the general action to be performed	reflection	com/appsflyer/internal/AFb1vSDK.java
00030	Connect to the remote server through the given URL	network	com/bumptechnology/load/data/HttpUrlFetcher.java
00112	Get the date of the calendar event	collection calendar	com/fasterxml/jackson/databind/ser/std/StdKeySerializers.java com/fasterxml/jackson/databind/util/StdDateFormat.java
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFg1jSDK.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFg1jSDK.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFi1bSDK.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFi1bSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFi1bSDK.java
00201	Query data from the call log	collection callog	com/appsflyer/internal/AFi1bSDK.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://constant-therapy-b5470.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebase-remoteconfig.firebaseio.com/v1/projects/923544178940/namespaces/firebase:fetch?key=AlzaSyAeC95c_U7MexvGrg639gGFthurkSP9dg. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.RECORD_AUDIO, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.WAKE_LOCK
Other Common Permissions	5/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, 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
www.constanttherapy.com	ok	IP: 141.193.213.11 Country: United States of America Region: Texas City: Austin Latitude: 30.271158 Longitude: -97.741699 View: Google Map
dev2.constanttherapy.com	ok	IP: 54.198.125.250 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	IP: 159.100.250.151 Country: Switzerland Region: Vaud City: Lausanne Latitude: 46.515999 Longitude: 6.632820 View: Google Map
constanttherapyhealth.com	ok	IP: 141.193.213.11 Country: United States of America Region: Texas City: Austin Latitude: 30.271158 Longitude: -97.741699 View: Google Map
ssdk-services.s	ok	No Geolocation information available.
svalidate-and-log.s	ok	No Geolocation information available.
hindi.constanttherapy.com	ok	No Geolocation information available.
simpresion.s	ok	No Geolocation information available.
code.google.com	ok	IP: 216.58.211.238 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
dev.constanttherapy.com	ok	IP: 18.206.175.6 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
play.google.com	ok	IP: 216.58.211.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.amazon.com	ok	IP: 18.165.130.223 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
github.com	ok	IP: 140.82.121.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
appqa1.constanttherapy.com	ok	IP: 52.85.49.99 Country: Finland Region: Uusimaa City: Helsinki Latitude: 60.169521 Longitude: 24.935450 View: Google Map
sonelink.s	ok	No Geolocation information available.
appstaging.constanttherapy.com	ok	IP: 3.164.206.85 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
app.constanttherapy.com	ok	IP: 3.164.206.119 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
ct-res.s3.amazonaws.com	ok	IP: 3.5.9.14 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
sars.s	ok	No Geolocation information available.
tempapp.constanttherapy.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
--------	--------	-------------

aps-webhandler.appsflyer.com	ok	IP: 18.165.122.69 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
constant-therapy-b5470.firebaseio.com	ok	IP: 34.120.206.254 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
api3.constanttherapy.com	ok	IP: 3.218.192.237 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
scdn-ssettings.s	ok	No Geolocation information available.
scdn-stestsettings.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api4.constanttherapy.com	ok	IP: 35.170.142.58 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
s3.amazonaws.com	ok	IP: 52.216.208.0 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
thelearningcorp.com	ok	IP: 141.193.213.11 Country: United States of America Region: Texas City: Austin Latitude: 30.271158 Longitude: -97.741699 View: Google Map
www.bbc.com	ok	IP: 151.101.244.81 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.googleapis.com	ok	IP: 216.58.210.138 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
sinapps.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
javax.xml.xmlconstants	ok	No Geolocation information available.
appdev.constanttherapy.com	ok	IP: 52.85.49.15 Country: Finland Region: Uusimaa City: Helsinki Latitude: 60.169521 Longitude: 24.935450 View: Google Map
www.google.com	ok	IP: 216.58.210.164 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
staging.constanttherapy.com	ok	IP: 34.192.235.215 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
sdlsdk.s	ok	No Geolocation information available.
svalidate.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
support@constanttherapy.com	com/constanttherapy/android/util/Constants.java

EMAIL	FILE
c1@mailinator.com	com/constanttherapy/android/main/features/landing/clinician/ClinicianLandingScreen.java
support@constant-therapy.com support@constanttherapy.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OpenTelemetry (OpenCensus, OpenTracing)	Analytics	https://reports.exodus-privacy.eu.org/trackers/412

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AlzaSyAeC95c-U7MexvGrg639gGFthurkSP9dg"
"remote_user" : "user"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"firebase_database_url" : "https://constant-therapy-b5470.firebaseio.com"

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AlzaSyAeC95c-_U7MexvGrg639gGFthurkSP9dg"
"branch_sdk_key" : "key_live_pnKFpmqFFP4hdDdtlCOUbligxDmU9wO3"
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
470fa2b4ae81cd56ecbcda9735803434cec591fa
258EAF5-E914-47DA-95CA-C5AB0DC85B11
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
23456789abcdefghijklmnopqrstuvwxyz

PLAYSTORE INFORMATION

Title: Constant Therapy: Brain Rehab

Score: 4.38 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** [com.constanttherapy.android.main](https://play.google.com/store/apps/details?id=com.constanttherapy.android.main)

Developer Details: Constant Therapy Health, Inc., 6415468762837389968, 405 Waltham St., Suite 222 Lexington, MA 02421, <https://thelearningcorp.com/constant-therapy/>, support@constanttherapy.com,

Release Date: Nov 17, 2014 **Privacy Policy:** [Privacy link](#)

Description:

Constant Therapy is an award-winning, science-based cognitive, language, and speech therapy app designed to help people recovering from stroke, traumatic brain injury (TBI), or people living with aphasia, apraxia, dementia, and other neurological conditions. Join a community of 600,000+ users who have embraced progress, completing 250 million+ evidence-based therapy activities through Constant Therapy. Get unlimited therapy, guided by AI, that allows you to engage in therapy exercises when and where you want. Constant Therapy is designed

to address concerns such as: – I know what I want to say but can’t find the words – My family can’t understand me when I talk – Before my TBI, I was a math whiz. Now, I have trouble with everyday math – I am forgetful, and I need help improving my memory – Staying on task has been difficult for me since my stroke. I need to fine-tune my attention & executive functioning – My loved one is getting speech therapy once a month, but it’s not enough. They need daily therapy - I want to go beyond basic brain training and need science based therapy

FEATURES & BENEFITS

- Whether you’re recovering from a stroke, TBI, aphasia, apraxia, dementia, or other neurological conditions, you choose your speech and cognitive therapy rehabilitation goals, and the app delivers customized & ever-adjusting exercises based on your unique needs
- Tackle memory challenges, enhance communication skills, and regain everyday abilities through your individualized program
- Engage in speaking, memory, attention, reading, writing, language, math, comprehension, problem solving, visual processing, auditory memory, and many other essential skill-building exercises
- Work independently at home, pair the app with in-clinic therapy, or add your clinician so they can monitor your progress
- Enjoy our friendly, live, Customer Support – trained to work with people with cognitive, communication, and speech challenges
- Monitor your progress with real-time, easy-to-understand performance reports
- Improve your chances for positive results: research has shown that patients using Constant Therapy get 5x more therapy practice, show faster improvement, and better outcomes***
- Access the world’s most comprehensive library of evidence-based exercises: over 500,000 exercises across 90 therapy areas developed by neuroscientists and clinicians
- Try before you subscribe with a free 14-day trial

*****THE SCIENCE BEHIND CONSTANT THERAPY**

Constant Therapy sets the gold standard with over 70 studies validating the clinical evidence behind our speech, language, and cognitive therapy exercises. We are also backed by 17 peer-reviewed research studies which substantiate the efficacy of Constant Therapy. For a complete list of clinical studies and research visit: constanttherapyhealth.com/science/

Constant Therapy is so much more than a brain-training app or brain games. It was designed by clinicians and scientists at Boston University specifically to target the challenges of recovery after stroke, brain injury, TBI, aphasia, dementia, apraxia, and other neurological disorders. It systematically tracks patient progress across a variety of functional domains including: language, cognition, memory, speech, language, attention, comprehension, visual processing and much more. A multiple-award winner from Hearst Health, UCSF Health Hub, Fierce Innovation Awards, the American Stroke Association, and AARP, Constant Therapy is recommended by thousands of speech-language pathologists, neurologists, occupational therapists, and clinicians at hospitals, clinics, and rehabilitation facilities everywhere.

SIGN UP FOR A FREE 14-DAY TRIAL

CONTACT US support@constanttherapy.com constanttherapy.com **TERMS** constanttherapy.com/privacy/ constanttherapy.com/eula/

Constant Therapy does not provide rehabilitation services or guarantee improvements in brain function. It provides tools for self-help and tools for patients to work with their clinicians.

☰ SCAN LOGS

Timestamp	Event	Error
2024-11-28 01:57:32	Generating Hashes	OK
2024-11-28 01:57:32	Extracting APK	OK
2024-11-28 01:57:32	Unzipping	OK
2024-11-28 01:57:32	Getting Hardcoded Certificates/Keystores	OK

2024-11-28 01:57:33	Parsing APK with androguard	OK
2024-11-28 01:57:38	Parsing AndroidManifest.xml	OK
2024-11-28 01:57:38	Extracting Manifest Data	OK
2024-11-28 01:57:38	Manifest Analysis Started	OK
2024-11-28 01:57:38	Performing Static Analysis on: Therapy (com.constanttherapy.android.main)	OK
2024-11-28 01:57:38	Fetching Details from Play Store: com.constanttherapy.android.main	OK
2024-11-28 01:57:38	Checking for Malware Permissions	OK
2024-11-28 01:57:38	Fetching icon path	OK
2024-11-28 01:57:38	Library Binary Analysis Started	OK
2024-11-28 01:57:38	Analyzing apktool_out/lib/armeabi-v7a/libnmsp_sk_speex.so	OK
2024-11-28 01:57:38	Analyzing apktool_out/lib/armeabi/libnmsp_sk_speex.so	OK
2024-11-28 01:57:38	Analyzing apktool_out/lib/x86/libnmsp_sk_speex.so	OK

2024-11-28 01:57:38	Analyzing apktool_out/lib/arm64-v8a/libnmsp_sk_speex.so	OK
2024-11-28 01:57:38	Analyzing apktool_out/lib/x86_64/libnmsp_sk_speex.so	OK
2024-11-28 01:57:38	Analyzing lib/armeabi-v7a/libnmsp_sk_speex.so	OK
2024-11-28 01:57:38	Analyzing lib/armeabi/libnmsp_sk_speex.so	OK
2024-11-28 01:57:39	Analyzing lib/x86/libnmsp_sk_speex.so	OK
2024-11-28 01:57:39	Analyzing lib/arm64-v8a/libnmsp_sk_speex.so	OK
2024-11-28 01:57:39	Analyzing lib/x86_64/libnmsp_sk_speex.so	OK
2024-11-28 01:57:39	Reading Code Signing Certificate	OK
2024-11-28 01:57:40	Running APKiD 2.1.5	OK
2024-11-28 01:57:48	Detecting Trackers	OK
2024-11-28 01:57:56	Decompiling APK to Java with JADX	OK
2024-11-28 01:59:21	Converting DEX to Smali	OK

2024-11-28 01:59:21	Code Analysis Started on - java_source	OK
2024-11-28 01:59:29	Android SBOM Analysis Completed	OK
2024-11-28 01:59:47	Android SAST Completed	OK
2024-11-28 01:59:47	Android API Analysis Started	OK
2024-11-28 01:59:53	Android API Analysis Completed	OK
2024-11-28 01:59:53	Android Permission Mapping Started	OK
2024-11-28 02:00:06	Android Permission Mapping Completed	OK
2024-11-28 02:00:08	Android Behaviour Analysis Started	OK
2024-11-28 02:00:13	Android Behaviour Analysis Completed	OK
2024-11-28 02:00:14	Extracting Emails and URLs from Source Code	OK
2024-11-28 02:00:23	Email and URL Extraction Completed	OK
2024-11-28 02:00:23	Extracting String data from APK	OK

2024-11-28 02:00:23	Extracting String data from SO	OK
2024-11-28 02:00:23	Extracting String data from Code	OK
2024-11-28 02:00:23	Extracting String values and entropies from Code	OK
2024-11-28 02:00:30	Performing Malware check on extracted domains	OK
2024-11-28 02:00:33	Saving to Database	OK

Report Generated by - MobSF v4.2.7

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.

© 2024 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).