ANDROID STATIC ANALYSIS REPORT

No icon

🤖 Prescription Scanner
(5.40.1400)

File Name: com.optimaxInvestments.GlassesUSA_1400.apk

Package Name: com.optimaxInvestments.GlassesUSA

Scan Date: Sept. 1, 2025, 6:42 a.m.

App Security Score: **51/100 (MEDIUM RISK)**

Grade:

B

Trackers Detection: 6/432

⬤ FINDINGS SEVERITY

🐛 HIGH	⚠ MEDIUM	ⓘ INFO	✔ SECURE	🔍 HOTSPOT
2	18	3	2	2

📦 FILE INFORMATION

File Name: com.optimaxInvestments.GlassesUSA_1400.apk
Size: 19.76MB
MD5: 3f629441a004a59e4b516aaa8c1236f5
SHA1: 82274caf90029139f070de3ef6f3573b2b48f258
SHA256: 1bf814693563cb779c486521d7850f7f13e95e5e7ce91a067fcc52f0ec358a42

ⓘ APP INFORMATION

App Name: Prescription Scanner
Package Name: com.optimaxInvestments.GlassesUSA
Main Activity:
Target SDK: 34
Min SDK: 28

Max SDK:
Android Version Name: 5.40.1400
Android Version Code: 1400

▪▪ APP COMPONENTS

Activities: 36
Services: 9
Receivers: 7
Providers: 5
Exported Activities: 3
Exported Services: 0
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: CN=gusa
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-11-29 08:48:33+00:00
Valid To: 2042-11-23 08:48:33+00:00
Issuer: CN=gusa
Serial Number: 0x4d478ca
Hash Algorithm: sha256
md5: 85f984fdabf04f1fc6cbc1b8011f534b
sha1: a3b1127a1b5b6eb6d7dbfb2aaf3699ede84094e1
sha256: 1c53590ffca5441ee366216914deece8d3e62df843b609c2daa9bbacf193c7e0
sha512: d1c1e117f79320cbc8d6cf5ba4fa1d054e94937385e758e55e1fb0c2123ba45dbc6109296e70e197f437dbb1e4185de1e37fcd146c1643e2eac9c9cd98303be7
PublicKey Algorithm: rsa
Bit Size: 2048

Fingerprint: fda06e77aaef687ebd2e0312b7f8510b0d0bc287537066905f6fa91ff8cfc4e9
Found 1 unique certificates

≣ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.optimaxInvestments.GlassesUSA.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

🦭 APKID ANALYSIS

FILE	DETAILS	
classes.dex	**FINDINGS**	**DETAILS**
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check
	Compiler	unknown (please file detection issue!)

FILE	DETAILS		
classes2.dex		**FINDINGS**	**DETAILS**
		yara_issue	yara issue - dex file recognized by apkid but not yara module
		Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check ro.hardware check ro.kernel.qemu check possible VM check
		Anti Debug Code	Debug.isDebuggerConnected() check
		Compiler	unknown (please file detection issue!)

FILE	DETAILS	
classes3.dex	**FINDINGS**	**DETAILS**
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.MODEL check Build.PRODUCT check Build.HARDWARE check Build.TAGS check network operator name check possible ro.secure check
	Compiler	unknown (please file detection issue!)
classes4.dex	**FINDINGS**	**DETAILS**
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.MODEL check Build.MANUFACTURER check network operator name check
	Compiler	unknown (please file detection issue!)

FILE	DETAILS	
classes5.dex	**FINDINGS**	**DETAILS**
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Compiler	unknown (please file detection issue!)

📑 BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.sixoversix.ui.activities.SplashActivity	Schemes: gusa://, prescriptionacanner://,

🔒 NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

📇 CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

🔍 MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
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.
3	Activity (com.sixoversix.ui.activities.SplashActivity) 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-Alias (com.sixoversix.glassesontemplateapp.Launcher) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Broadcast Receiver (com.appsflyer.SingleInstallBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Broadcast Receiver (com.sixoversix.notification.AlarmReceiver) 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.
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	Activity (androidx.compose.ui.tooling.PreviewActivity) 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.
9	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **7** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/airbnb/lottie/LottieAnimationView.java
				com/airbnb/lottie/PerformanceTracker.java
				com/airbnb/lottie/utils/LogcatLogger.java
				com/appsflyer/internal/AFb1tSDK.java
				com/appsflyer/internal/AFf1iSDK.java
				com/appsflyer/internal/AFf1jSDK.java
				com/appsflyer/internal/AFf1tSDK.java
				com/appsflyer/internal/AFg1dSDK.java
				com/appsflyer/internal/AFg1lSDK.java
				com/appsflyer/share/LinkGenerator.java
				com/bumptech/glide/Glide.java
				com/bumptech/glide/disklrucache/DiskLruCache.java
				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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/engine/bitmap_re cycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_re cycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/Disk LruCacheWrapper.java com/bumptech/glide/load/engine/cache/Me morySizeCalculator.java com/bumptech/glide/load/engine/executor/ GlideExecutor.java com/bumptech/glide/load/engine/executor/R untimeCompat.java com/bumptech/glide/load/engine/prefill/Bit mapPreFillRunner.java com/bumptech/glide/load/model/ByteBuffer Encoder.java com/bumptech/glide/load/model/ByteBuffer FileLoader.java com/bumptech/glide/load/model/FileLoader. java com/bumptech/glide/load/model/ResourceL oader.java com/bumptech/glide/load/model/StreamEnc oder.java com/bumptech/glide/load/resource/DefaultO nHeaderDecodedListener.java com/bumptech/glide/load/resource/bitmap/ BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/ BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/ DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/ Downsampler.java com/bumptech/glide/load/resource/bitmap/ DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/ HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/ TransformationUtils.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	com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SingletonConnectivityReceiver.java com/bumptech/glide/manager/SupportRequestManagerFragment.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/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/intercom/twig/Twig.java com/luna/commons/analytics/MixpanelApiWrapper.java com/luna/commons/logs/coralogix/CoralogixService.java com/luna/commons/logs/handlers/AndroidL

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ogHandler.java com/luna/commons/managers/TextToSpeechManager.java com/luna/commons/ui/colorCustomization/VectorFinder/AnimatedVectorDrawableCompat.java com/luna/commons/ui/colorCustomization/VectorFinder/PathParser.java com/luna/commons/ui/colorCustomization/VectorFinder/VectorDrawableCompat.java com/luna/commons/ui/fonts/FontsManager.java com/luna/commons/utils/RequestBodyUtils.java com/luna/corelib/actions/handlers/ChangeFocusToContinuesActionHandler.java com/luna/corelib/actions/handlers/ChangeFocusToFocusAreaActionHandler.java com/luna/corelib/actions/handlers/SetFocusDistanceActionHandler.java com/luna/corelib/camera/frames/ShowErrorTimer.java com/luna/corelib/camera/frames/process/SendFrameImageTask.java com/luna/corelib/pages/handlers/DeviceCalibrationV2MatrixPageHandler.java com/luna/corelib/pages/handlers/QRScanPageHandler.java com/luna/corelib/tilt/compress/impl/TimeLapseEncoder.java com/luna/sound_manager/managers/SoundItemHandler.java com/luna/sound_manager/managers/SoundManager.java com/luna/sound_manager/usecases/SoundPlayerUseCase.java com/mixpanel/android/mpmetrics/AnalyticsMessages.java com/mixpanel/android/mpmetrics/ConfigurationChecker.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mixpanel/android/mpmetrics/MPConfig.java
				com/mixpanel/android/mpmetrics/MPDbAdapter.java
				com/mixpanel/android/mpmetrics/MixpanelAPI.java
				com/mixpanel/android/mpmetrics/PersistentIdentity.java
				com/mixpanel/android/mpmetrics/ResourceReader.java
				com/mixpanel/android/mpmetrics/SessionMetadata.java
				com/mixpanel/android/mpmetrics/SystemInformation.java
				com/mixpanel/android/util/HttpService.java
				com/mixpanel/android/util/MPLog.java
				com/rits/cloning/Cloner.java
				com/sixoversix/managers/RateUsHelper.java
				com/sixoversix/managers/analytics/BIEventsManager.java
				com/sixoversix/managers/analytics/providers/AppsflyerManager.java
				com/sixoversix/ui/activities/BaseActivity.java
				com/sixoversix/ui/dialogs/BasePopupDialog.java
				com/sixoversix/ui/dialogs/RateUsThumbsPopupDialog.java
				de/tavendo/autobahn/AutobahnConnection.java
				de/tavendo/autobahn/AutobahnReader.java
				de/tavendo/autobahn/AutobahnWriter.java
				de/tavendo/autobahn/WebSocketConnection.java
				de/tavendo/autobahn/WebSocketReader.java
				de/tavendo/autobahn/WebSocketWriter.java
				io/branch/referral/BranchJsonConfig.java
				io/branch/referral/BranchLogger.java
				io/branch/referral/validators/IntegrationValidator.java
				io/github/aakira/napier/DebugAntilog.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/mozilla/classfile/TypeInfo.java org/mozilla/javascript/Interpreter.java org/mozilla/javascript/ScriptRuntime.java org/mozilla/javascript/tools/debugger/Dim.java org/mozilla/javascript/tools/jsc/Main.java org/mozilla/javascript/tools/shell/Main.java org/tensorflow/lite/NativeInterpreterWrapper.java org/tensorflow/lite/support/image/TensorBufferContainer.java org/tensorflow/lite/support/label/LabelUtil.java org/tensorflow/lite/support/metadata/MetadataExtractor.java org/tensorflow/lite/support/model/GpuDelegateProxy.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	org/mozilla/javascript/tools/debugger/Dim.java timber/log/Timber.java
3	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	com/luna/commons/utils/ViewUtils.java io/branch/referral/ShareLinkManager.java
4	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/mixpanel/android/mpmetrics/MPDbAdapter.java
5	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/appsflyer/internal/AFa1ySDK.java com/appsflyer/internal/AFb1aSDK.java com/appsflyer/internal/AFc1iSDK.java de/tavendo/autobahn/AutobahnConnection.java de/tavendo/autobahn/WebSocketWriter.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/luna/commons/logs/coralogix/client/CoralogixClient.java com/luna/corelib/server/RetrofitClient.java
7	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	coil/decode/GifDecoder.java coil/decode/VideoFrameDecoder.java coil/memory/MemoryCache.java coil/memory/MemoryCacheService.java coil/request/Parameters.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/luna/corelib/sdk/PageActionsHolder.java com/luna/corelib/sdk/config/ExternalConfigManager.java com/luna/corelib/sdk/preferences/PreferenceKeys.java com/luna/corelib/server/NetworkService.java com/luna/corelib/server/SdkHttpSslPinning.java com/luna/corelib/server/models/S3ObjectFields.java com/sixoversix/glassesontemplateapp/BuildConfig.java io/branch/referral/Branch.java io/branch/referral/BranchPreinstall.java io/branch/referral/PrefHelper.java io/branch/referral/ServerRequest.java io/branch/referral/ServerRequestQueue.java io/branch/referral/UniversalResourceAnalyse

NO	ISSUE	SEVERITY	STANDARDS	FILES
				r.java /branch/referral/validators/DeepLinkRoutingValidator.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java org/mozilla/javascript/ClassCache.java org/mozilla/javascript/ImporterTopLevel.java org/mozilla/javascript/NativeError.java org/mozilla/javascript/NativeJavaObject.java org/mozilla/javascript/ScriptRuntime.java org/mozilla/javascript/xmlimpl/XmlNode.java
8	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/luna/corelib/utils/RootUtil.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/luna/corelib/utils/RootUtil.java
10	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	coil/decode/SourceImageSource.java com/luna/commons/utils/FileUtils.java com/luna/commons/utils/IntentUtils.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	org/mozilla/javascript/tools/shell/Main.java
12	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFb1tSDK.java

🪪 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

🖧 BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	com/luna/corelib/camera/frames/data/RequestData.java com/mixpanel/android/mpmetrics/MPDbAdapter.java
00013	Read file and put it into a stream	file	coil/fetch/ContentUriFetcher.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1lSDK.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/resource/bitmap/ImageReader.java com/luna/commons/utils/FileUtils.java com/luna/corelib/pd/mtcnn/MtcnnUtils.java okio/Okio__JvmOkioKt.java org/codehaus/jackson/JsonFactory.java org/mozilla/javascript/tools/SourceReader.java org/mozilla/javascript/tools/debugger/Dim.java org/mozilla/javascript/tools/shell/Global.java org/tensorflow/lite/support/common/FileUtil.java pl/droidsonroids/relinker/elf/ElfParser.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	coil/disk/DiskCache.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/appsflyer/internal/AFg1lSDK.java com/luna/corelib/assets/AssetsDownloadManager.java com/luna/corelib/devicecalibration/DcFramesHolder.java com/luna/corelib/tilt/compress/impl/CodecImageUseCase$createVideosFromImages$1.java org/codehaus/jackson/map/ser/std/StdJdkSerializers.java org/mozilla/javascript/tools/jsc/Main.java org/tensorflow/lite/Interpreter.java org/tensorflow/lite/InterpreterImpl.java pl/droidsonroids/relinker/ReLinkerInstance.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/appsflyer/internal/AFd1oSDK.java com/appsflyer/internal/AFe1sSDK.java com/mixpanel/android/util/HttpService.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFd1oSDK.java com/appsflyer/internal/AFe1sSDK.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/mixpanel/android/util/HttpService.java org/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFd1oSDK.java com/appsflyer/internal/AFe1sSDK.java com/appsflyer/internal/AFf1mSDK.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/mixpanel/android/util/HttpService.java org/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1gSDK.java com/appsflyer/internal/AFi1lSDK.java com/appsflyer/internal/AFi1mSDK.java io/branch/coroutines/InstallReferrersKt.java
00036	Get resource file from res/raw directory	reflection	coil/map/ResourceIntMapper.java com/appsflyer/internal/AFb1tSDK.java com/appsflyer/internal/AFf1pSDK.java com/appsflyer/internal/AFi1lSDK.java com/appsflyer/internal/AFi1oSDK.java com/luna/commons/utils/IntentUtils.java io/branch/referral/Branch.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/luna/corelib/admin/AdminContentResolverWrapper.java
00009	Put data in cursor to JSON object	file	com/mixpanel/android/mpmetrics/MPDbAdapter.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFb1tSDK.java com/appsflyer/internal/AFc1uSDK.java com/luna/corelib/sdk/config/ExternalConfigIntentHandler.java io/branch/referral/Branch.java
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFg1lSDK.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFg1lSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/appsflyer/internal/AFb1tSDK.java com/appsflyer/internal/AFc1aSDK.java com/appsflyer/internal/AFc1uSDK.java com/appsflyer/internal/AFf1tSDK.java com/luna/commons/utils/IntentUtils.java com/sixoversix/managers/SupportManager.java com/sixoversix/ui/dialogs/RateUsPopupThanksDialog.java io/branch/referral/Branch.java io/branch/referral/validators/DeepLinkRoutingValidator.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java org/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFh1dSDK.java com/mixpanel/android/mpmetrics/SystemInformation.java io/branch/referral/SystemObserver.java
00094	Connect to a URL and read data from it	command network	com/mixpanel/android/util/HttpService.java org/mozilla/javascript/tools/shell/Global.java
00108	Read the input stream from given URL	network command	com/mixpanel/android/util/HttpService.java
00012	Read data and put it into a buffer stream	file	com/luna/commons/utils/FileUtils.java
00003	Put the compressed bitmap data into JSON object	camera	io/branch/referral/network/BranchRemoteInterfaceUrlConnection.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/luna/commons/utils/IntentUtils.java com/sixoversix/managers/SupportManager.java io/branch/referral/Branch.java
00189	Get the content of a SMS message	sms	com/luna/corelib/admin/AdminContentResolverWrapper.java
00126	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/luna/corelib/admin/AdminContentResolverWrapper.java
00188	Get the address of a SMS message	sms	com/luna/corelib/admin/AdminContentResolverWrapper.java
00200	Query data from the contact list	collection contact	com/luna/corelib/admin/AdminContentResolverWrapper.java
00187	Query a URI and check the result	collection sms calllog calendar	com/luna/corelib/admin/AdminContentResolverWrapper.java
00201	Query data from the call log	collection calllog	com/luna/corelib/admin/AdminContentResolverWrapper.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java
00023	Start another application from current application	reflection control	com/luna/commons/utils/IntentUtils.java
00056	Modify voice volume	control	com/luna/sound_manager/managers/SoundManagerInitializer.java

⬢ FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://glassesusa-6over6.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/84484401072/namespaces/firebase:fetch?key=AIzaSyBhoIG_NBQVaQ1g2Gz6Y2SIDQgpS-u0qeo is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'force_update_version': ''}, 'state': 'UPDATE', 'templateVersion': '1'}

⣿⣿ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.CAMERA, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE
Other Common Permissions	4/44	com.google.android.gms.permission.AD_ID, android.permission.FLASHLIGHT, 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
help.branch.io	ok	**IP:** 104.18.21.218 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** [Google Map](#)
api.coralogix.com	ok	**IP:** 52.214.88.252 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** [Google Map](#)
api.glasseson.com	ok	**IP:** 52.200.178.67 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** [Google Map](#)
sinapps.s	ok	No Geolocation information available.

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
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
6over6.com	ok	**IP:** 35.83.224.212 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
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
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
fdasub-api.myrx.luna.io	ok	**IP:** 34.194.56.200 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api.mixpanel.com	ok	**IP:** 107.178.240.159 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sars.s	ok	No Geolocation information available.
branch.app.link	ok	**IP:** 18.238.109.123 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sregister.s	ok	No Geolocation information available.
www.glassesusa.com	ok	**IP:** 23.62.226.44 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
scdn-ssettings.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
web.glasseson.com	ok	**IP:** 44.220.125.1 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** [Google Map](#)
api3-eu.branch.io	ok	**IP:** 18.155.173.33 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** [Google Map](#)
api.coralogix.us	ok	**IP:** 3.132.4.30 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **View:** [Google Map](#)
luna.io	ok	**IP:** 192.124.249.10 **Country:** United States of America **Region:** California **City:** Menifee **Latitude:** 33.679798 **Longitude:** -117.189484 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
127.0.0.1	ok	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
api.branch.io	ok	**IP:** 18.238.109.24 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
bnc.lt	ok	**IP:** 18.238.109.128 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
cdn.branch.io	ok	**IP:** 18.238.109.81 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
aps-webhandler.appsflyer.com	ok	**IP:** 18.238.109.53 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
dev.api.glasseson.com	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
api.eu.myrx.luna.io	ok	**IP:** 3.125.92.92 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
sapp.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
glassesusa-6over6.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
api2.branch.io	ok	**IP:** 18.238.96.12 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
www.6over6.com	ok	**IP:** 35.83.224.212 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

✉ EMAILS

EMAIL	FILE
scanner@glassesusa.com support@6over6.com	Android String Resource

🕵 TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"branch_io_key_live" : "key_live_leWwflvjEnWcm7TIaao0AnpeEvlpNk7B"

POSSIBLE SECRETS

"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"

"firebase_database_url" : "https://glassesusa-6over6.firebaseio.com"

"google_api_key" : "AIzaSyBhoIG_NBQVaQ1g2Gz6Y2SIDQgpS-u0qeo"

"google_crash_reporting_api_key" : "AIzaSyBhoIG_NBQVaQ1g2Gz6Y2SIDQgpS-u0qeo"

f9a6bac84287ef8a0940168bcb13f20e

f1a119c4-3d48-81cf-99b4-bc7617d03f71

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

470fa2b4ae81cd56ecbcda9735803434cec591fa

22ac6c1d7cc67be929fab3e61d3fbf7a

E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1

a004e9287589e9e96437a3ee994661b1

FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901

iWNR8lg8XrkQ8k4qTlljWDRZsOFmTvBydS7R8dmO

sha256/++MBgDH5WGvL9Bcn5Be30cRcL0f5O+NyoXuWtQdX1aI=

sha256/JSMzqOOrtyOT1kmau6zKhgT676hGgczD5VMdRMyJZFA=

POSSIBLE SECRETS

KQW4twqlX86RJBeBlpdFO5130psNVyvu8xhi9gTE

JlH2juyQdHaP4ArDrLc3d3G75tWxUHvS6zrydMkV

59d63370-6afd-da0a-7cac-04572a80ee08

FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212

85053bf24bba75239b16a601d9387e17

4c0eaf0d-e03c-44a5-a185-2601ffdc3985

dd39ac41fa2229582f5e29489e56fee5

8e4cac44-5736-4525-ab8b-abc3db119fda

lVwEizBRU63ne1nBKpuFA90UjtfmxAZHaSHnnbdH

0136024004378801593602050505

mO9c7Fcxn25Agc8FRXE3PfWFWLf3Go99vFzJJVJ0

3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F

NcAVrjDz76ast5BTjiNQkq1o4d3i6rwaFjdfoaB1

sha256/4a6cPehI7OG6cuDZka5NDZ7FR8a60d3auda+sKfg4Ng=

a32ea3c6c03a8550e7c28180ddfabd1f

▶ PLAYSTORE INFORMATION

Title: Prescription Scanner

Score: 3.9623826 **Installs:** 100,000+ **Price:** 0 **Android Version Support: Category:** Medical **Play Store URL:** com.optimaxInvestments.GlassesUSA

Developer Details: GlassesUSA.com, 8541133037155728674, None, https://www.glassesusa.com, service@glassesusa.com,

Release Date: Apr 16, 2018 **Privacy Policy:** Privacy link

Description:

Need your glasses prescription? Try our FREE app! Introducing Prescription Scanner: an easy, fast & FREE way of getting your prescription from your current eyeglasses without leaving the house. Just download the app, scan your glasses and shop a new pair online with your prescription at GlassesUSA.com. Key Benefits: * Convenient: Scan from the comfort of home * Easy & fast: Get your prescription in less than 5 minutes! * App is completely FREE * Accurate * FDA-Listed • All you need is a smartphone, computer and a standard-size magnetic card How it works: • Download the app & scan your current glasses using only a smartphone, computer screen and magnetic card. • Get accurate results through a quick, simple process with audio & video tutorials to guide you every step of the way. • Use the prescription to purchase new glasses online with an exclusive discount. About us: GlassesUSA.com is the #1 online retailer for prescription eyewear in the US, with a pair of glasses sold every minute! We're proud of changing the way people buy glasses and making them affordable for everyone. Discover 7000+ styles and a huge selection of brands including Ray-Ban, Oakley, Versace, Gucci and more. Find eyewear for every need including protective eyewear, blue light protection, prescription eyewear with anti-fog coatings, sports glasses, kids' glasses, contact lenses and more. Try on any frame online from home with our Virtual Mirror to see how they look on you. Enjoy free shipping on all orders right to your door, free returns and a 100% money-back guarantee. Who can use the Prescription Scanner? • Healthy individuals, 18 or older • People with see well their current prescription • Single vision prescription between -6.00 and +3.00 • Cylinder measurement lower than -2.50 Note: Please read our full Terms of Use. It includes, amongst other information, a detailed list of conditions and illnesses that are not eligible for accurate results. You should not use Prescription Scanner if you: • Have a progressive, multifocal, or bifocal prescription • Have a prescription that includes prism • Have a high single-vision (distance or reading) and/or astigmatism correction • Take medication that affects your vision • Have an illness or condition that affects eye health (refer to your doctor) Distributed by GlassesUSA.com. Manufactured by 6over6 Vision Ltd. For more details go to https://6over6.com/

☰ SCAN LOGS

Timestamp	Event	Error
2025-09-01 06:42:53	Generating Hashes	OK

2025-09-01 06:42:54	Extracting APK	OK
2025-09-01 06:42:54	Unzipping	OK
2025-09-01 06:43:01	Parsing APK with androguard	OK
2025-09-01 06:43:02	Extracting APK features using aapt/aapt2	OK
2025-09-01 06:43:02	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 06:43:05	Parsing AndroidManifest.xml	OK
2025-09-01 06:43:05	Extracting Manifest Data	OK
2025-09-01 06:43:05	Manifest Analysis Started	OK
2025-09-01 06:43:05	Performing Static Analysis on: Prescription Scanner (com.optimaxInvestments.GlassesUSA)	OK
2025-09-01 06:43:06	Fetching Details from Play Store: com.optimaxInvestments.GlassesUSA	OK

2025-09-01 06:43:08	Checking for Malware Permissions	OK
2025-09-01 06:43:08	Fetching icon path	OK
2025-09-01 06:43:08	Library Binary Analysis Started	OK
2025-09-01 06:43:08	Reading Code Signing Certificate	OK
2025-09-01 06:43:08	Running APKiD 2.1.5	OK
2025-09-01 06:43:11	Detecting Trackers	OK
2025-09-01 06:43:16	Decompiling APK to Java with JADX	OK
2025-09-01 06:44:06	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 06:44:06	Decompiling classes2.dex with JADX	OK
2025-09-01 06:44:16	Decompiling classes4.dex with JADX	OK
2025-09-01 06:44:26	Decompiling classes.dex with JADX	OK

2025-09-01 06:44:35	Decompiling classes3.dex with JADX	OK
2025-09-01 06:44:39	Decompiling classes5.dex with JADX	OK
2025-09-01 06:44:43	Decompiling classes2.dex with JADX	OK
2025-09-01 06:44:52	Decompiling classes4.dex with JADX	OK
2025-09-01 06:45:02	Decompiling classes.dex with JADX	OK
2025-09-01 06:45:11	Decompiling classes3.dex with JADX	OK
2025-09-01 06:45:15	Decompiling classes5.dex with JADX	OK
2025-09-01 06:45:20	Converting DEX to Smali	OK
2025-09-01 06:45:20	Code Analysis Started on - java_source	OK
2025-09-01 06:45:25	Android SBOM Analysis Completed	OK

2025-09-01 06:45:31	Android SAST Completed	OK
2025-09-01 06:45:31	Android API Analysis Started	OK
2025-09-01 06:45:37	Android API Analysis Completed	OK
2025-09-01 06:45:37	Android Permission Mapping Started	OK
2025-09-01 06:45:42	Android Permission Mapping Completed	OK
2025-09-01 06:45:43	Android Behaviour Analysis Started	OK
2025-09-01 06:45:50	Android Behaviour Analysis Completed	OK
2025-09-01 06:45:50	Extracting Emails and URLs from Source Code	OK
2025-09-01 06:45:54	Email and URL Extraction Completed	OK
2025-09-01 06:45:54	Extracting String data from APK	OK
2025-09-01 06:45:55	Extracting String data from Code	OK

2025-09-01 06:45:55	Extracting String values and entropies from Code	OK
2025-09-01 06:46:00	Performing Malware check on extracted domains	OK
2025-09-01 06:46:07	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.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.