ANDROID STATIC ANALYSIS REPORT

app_icon

🤖 EVA AI (ex-Journey) (3.49.0)

File Name:	EVA AI Chat Bot & Soulmate_3.49.0_Apkpure.apk
Package Name:	com.ifriend.app
Scan Date:	Dec. 4, 2023, 3:07 a.m.
App Security Score:	**37/100 (HIGH RISK)**
Grade:	C
Trackers Detection:	7/428

FINDINGS SEVERITY

🐞 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
10	16	1	2	2

FILE INFORMATION

File Name: EVA AI Chat Bot & Soulmate_3.49.0_Apkpure.apk
Size: 49.53MB
MD5: fb5607a5d62140fa98448f052eb086e7
SHA1: b9c1f552acaa6ab35abe019906b7feed984247ef
SHA256: f6fe0c74de77d0c778d25cbc624970bcae66e4afd4fe2e2993fc917db25fe022

APP INFORMATION

App Name: EVA AI (ex-Journey)
Package Name: com.ifriend.app
Main Activity:
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 3.49.0

Android Version Code: 36961

◫ APP COMPONENTS

Activities: 11
Services: 9
Receivers: 6
Providers: 5
Exported Activities: 7
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

✳ CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-02-08 10:13:25+00:00
Valid To: 2051-02-08 10:13:25+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x7fa952d1c8844c0697f968e120cb97a3efc84be6
Hash Algorithm: sha256
md5: 8d6154a33e039554e079ad7d11b1b792
sha1: ca5acd5b5bd0a38aef1a548f579921194102673c
sha256: 903fbfbdb4c14e72d862476cbd6bcfe0dff730543fc935731804e33c859cc6c7
sha512: e8db12cc0c8cb7256194032787bfecebcd930ae113674cfedf5d7863598116a2b2046f3d593d7e9588fe183cd1877c30a99c8e4952558e1ba9800a425eac3f41
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 650d0dcaad59f572ba4d9fde90635619175be9e44bacf1c352b9a043e1fa5af9
Found 1 unique certificates

≡ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.POST_NOTIFICATIONS	dangerous		Allows an app to post notifications
android.permission.READ_MEDIA_IMAGES	dangerous		Allows an application to read image files from external storage.
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
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.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.ifriend.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

ⵙ APKID ANALYSIS

FILE	DETAILS	
classes.dex	**FINDINGS**	**DETAILS**
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes2.dex	**FINDINGS**	**DETAILS**
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check ro.kernel.qemu check possible VM check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes3.dex	**FINDINGS**	**DETAILS**
	Anti-VM Code	Build.MANUFACTURER check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS
classes4.dex	

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check
Anti Debug Code	Debug.isDebuggerConnected() check
Compiler	r8 without marker (suspicious)

classes5.dex

FINDINGS	DETAILS
Compiler	r8 without marker (suspicious)

FILE	DETAILS
classes6.dex	**FINDINGS / DETAILS** **Anti-VM Code** — Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check **Compiler** — r8 without marker (suspicious)
classes7.dex	**FINDINGS / DETAILS** **Anti Debug Code** — Debug.isDebuggerConnected() check **Anti-VM Code** — Build.MODEL check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check **Compiler** — r8 without marker (suspicious)

classes6.dex

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check
Compiler	r8 without marker (suspicious)

classes7.dex

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.MODEL check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check
Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes8.dex	**FINDINGS**	**DETAILS**
	Compiler	unknown (please file detection issue!)

🗔 BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.ifriend.app.ui.splash.SplashActivity	Schemes: https://, Hosts: evaai.onelink.me, journeyapp.onelink.me, www.ifriend.ai, ifriend.ai, www.evaapp.ai, evaapp.ai, journeyapp.ai, www.journeyapp.ai, Path Prefixes: /2Npy, /9rvJ, /email-confirmation, /avatars, /chat,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.ifriend.app,

🔒 NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is configured to trust user installed certificates.
2	*	warning	Base config is configured to trust system certificates.

📇 CERTIFICATE ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

🔍 MANIFEST ANALYSIS

HIGH: **7** | WARNING: **5** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=23]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	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
4	Activity (com.ifriend.app.ui.splash.SplashActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity-Alias (com.ifriend.app.ui.splash.PremiumSplashActivity) is not Protected. [android:exported=true]	high	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.
6	Activity-Alias (com.ifriend.app.ui.splash.NotPremiumSplashActivity) is not Protected. [android:exported=true]	high	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.
7	Activity (com.ifriend.chat.presentation.ui.AppActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.ifriend.registration.presentation.ui.RegistrationActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
11	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
12	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.
13	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **8** | INFO: **1** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				by/kirich1409/viewbindingdelegate/LifecycleViewBindingProperty.java cc/cloudist/acplibrary/ACProgressCustom.java cc/cloudist/acplibrary/views/CustomView.java cc/cloudist/acplibrary/views/PieView.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/appsflyer/AFLogger.java com/bumptech/glide/Glide.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 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.ja

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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/DefaultOnHeaderDecodedListener.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
				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
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/manager/DefaultConnectivityMonitorFactory.java
				com/bumptech/glide/manager/RequestManagerFragment.java
				com/bumptech/glide/manager/RequestManagerRetriever.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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/ifriend/analytics/AppsFlyerAnalyticsSender.java
				com/ifriend/analytics/FirebaseAnalyticsSender.java
				com/ifriend/animatedBackground/droplet/DropletBackgroundView$touchEvent$1.java
				com/ifriend/animatedBackground/droplet/DropletBackgroundView.java
				com/ifriend/chat/new_chat/list/presentationSystems/audio/decode/DecodingAudioEventsHandlingSystem.java
				com/ifriend/chat/presentation/utils/ScreenshotDetectionDelegate.java
				com/ifriend/core/MessagesSourceLifecycleController$subscribeOnConnectionAvailability$1.java
				com/ifriend/data/networking/api/FirebaseApiRepositoryImpl$unsubscribe$2$1.java
				com/ifriend/data/socket/MessagesSocketUrlProvider.java
				com/ifriend/data/storages/tags/TagsStorageImpl.java
				com/ifriend/icon_switcher/AppComponentPostponedSwitcher.java
				com/ifriend/infrastructure/ProdLogger.java
				com/ifriend/infrastructure/audio/player/MediaPlayerPlaybackController.java
				com/ifriend/infrastructure/connectivity/InternetConnectionImpl$isInternetAvailable$2.java
				com/ifriend/infrastructure/connectivity/InternetConnectionImpl.java
				com/ifriend/keychain/KeychainAdapter.java
				com/ifriend/keychain/KeychainModule.java
				com/ifriend/keychain/cipherStorage/CipherStorageBase.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/ifriend/keychain/cipherStorage/CipherStorageFacebook Conceal.java com/ifriend/keychain/cipherStorage/CipherStorageKeystore AesCbc.java com/ifriend/keychain/cipherStorage/CipherStorageKeystore RsaEcb.java com/ifriend/registration/presentation/bridges/facebook/Fac ebookAuthorizationBridgeImpl.java com/ifriend/ui/base/FragmentLifecycleLogger.java com/ifriend/ui/base/mvvm/FragmentBaseView.java com/ifriend/ui/utils/insets/InsetsExtensionsKt.java com/redmadrobot/extensions/viewbinding/ViewBindingKt.j ava com/tbuonomo/viewpagerdotsindicator/DotsIndicator.java eightbitlab/com/blurview/BlurView.java io/github/aakira/napier/DebugAntilog.java io/grpc/netty/shaded/io/netty/util/Version.java io/grpc/okhttp/internal/Platform.java io/sentry/SystemOutLogger.java io/sentry/android/core/AndroidLogger.java io/sentry/transport/StdoutTransport.java org/conscrypt/ct/CTVerifier.java timber/log/Timber.java
				coil/memory/MemoryCache.java coil/memory/MemoryCacheService.java coil/request/Parameters.java com/airbnb/lottie/compose/RememberLottieCompositionKt. 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.ja va com/ifiend/billing/impl/manager/BillingManagerImpl.java com/ifriend/app/appsflyer/AppsFlyerInitDelegateImpl.java com/ifriend/chat/new_chat/list/player/AudioPlayer.java com/ifriend/core/local/impl/common/LocalDataConst.java com/ifriend/core/remote/interceptors/DataDogAuthIntercep

NO	ISSUE	SEVERITY	STANDARDS	FILES
				tor.java com/ifriend/data/memorycached/chats/ChatConfigsMemoryCachedSourceImpl.java
2	[Files may contain hardcoded sensitive information like usernames, passwords, keys etc.](#)	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/ifriend/data/memorycached/onboarding/OnboardingChatConfigsMemoryCachedSourceImpl.java com/ifriend/data/networking/OkHttpClientProviderKt.java com/ifriend/data/networking/responses/EmailRegistrationRequest.java com/ifriend/data/networking/responses/EmailRegistrationResponse.java com/ifriend/data/repository/onboarding/OnboardingAnswersRepositoryImpl.java com/ifriend/data/socket/common/SocketMessageKeys.java com/ifriend/data/storages/diary/ShownDiaryNotesDaoImpl.java com/ifriend/domain/config/ConfigEntity.java com/ifriend/domain/data/install/PreferencesAppInstallStorage.java com/ifriend/domain/rateUs/RateUsStateStorageImpl.java com/ifriend/keychain/KeychainAdapterKt.java com/ifriend/keychain/KeychainModule.java com/ifriend/logger/impl/logic/AppLoggerInteractorImpl.java com/ifriend/long_term_notifications/impl/LongTermNotificationManagerImpl.java com/ifriend/popup/api/PopupResultModelKt.java com/ifriend/popup/impl/CommonPopupDialog.java com/ifriend/popup/impl/UpgradePopupDialog.java com/ifriend/presentation/features/chatsettings/ui/ChatSettingsFragment.java com/ifriend/presentation/features/chatstore/ui/ChatsStoreFragment.java com/ifriend/presentation/features/purchases/billing/delegate/BillingPurchaseDelegateImpl.java com/ifriend/presentation/features/purchases/chatsubscription/common/mappers/SubscriptionBenefitsMapper.java com/ifriend/presentation/features/purchases/premium/viewmodel/BuyPremiumViewModel.java com/ifriend/presentation/navigation/navflow/NavHostFlowFragment.java com/ifriend/push_notification/PushConstant.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/ifriend/registration/presentation/ui/email/resetPasswo rd/ResetPasswordFragmentKt.java com/ifriend/ui/base/ChangeNetworkStateBugPermission.jav a com/ifriend/ui/base/modalMessage/ChooseVoicePopupDele gate.java com/ifriend/ui/base/modalMessage/GeneratingAnimatedAv atarPopupDelegate.java com/ifriend/ui/base/modalMessage/RateAppPopupDelegate .java com/ifriend/ui/base/modalMessage/RequestSextingPopupD elegate.java com/ifriend/ui/base/modalMessage/UpgradeAppPopupDele gate.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/TransportFrameUtil.java io/grpc/netty/shaded/io/netty/handler/codec/http/HttpHead ers.java io/grpc/netty/shaded/io/netty/handler/proxy/Socks4ProxyH andler.java io/grpc/netty/shaded/io/netty/handler/proxy/Socks5ProxyH andler.java io/grpc/netty/shaded/io/netty/handler/ssl/PemPrivateKey.ja va io/grpc/netty/shaded/io/netty/handler/ssl/SslMasterKeyHan dler.java io/opencensus/metrics/AutoValue_LabelKey.java io/opencensus/tags/AutoValue_Tag.java io/opencensus/trace/AutoValue_Tracestate_Entry.java org/conscrypt/OpenSSLECKeyFactory.java org/conscrypt/OpenSSLRSAKeyFactory.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/ifriend/app/di/modules/data/ApiModule.java com/ifriend/app/di/modules/data/datadog/DataDogModule.java io/grpc/netty/shaded/io/netty/handler/ssl/JdkSslClientContext.java io/grpc/netty/shaded/io/netty/handler/ssl/JdkSslServerContext.java io/grpc/netty/shaded/io/netty/handler/ssl/ReferenceCountedOpenSslClientContext.java io/grpc/netty/shaded/io/netty/handler/ssl/ReferenceCountedOpenSslServerContext.java io/grpc/netty/shaded/io/netty/handler/ssl/SslContext.java io/grpc/netty/shaded/io/netty/handler/ssl/util/FingerprintTrustManagerFactory.java io/grpc/okhttp/OkHttpChannelBuilder.java org/conscrypt/Conscrypt.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/Platform.java org/conscrypt/SSLParametersImpl.java
4	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	org/conscrypt/Conscrypt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/ifriend/domain/newChat/chat/models/MessageTag.java io/grpc/internal/DnsNameResolver.java io/grpc/internal/ExponentialBackoffPolicy.java io/grpc/internal/RetriableStream.java io/grpc/netty/shaded/io/netty/handler/ssl/util/ThreadLocalInsecureRandom.java io/grpc/netty/shaded/io/netty/util/internal/PlatformDependent.java io/grpc/netty/shaded/io/netty/util/internal/ThreadLocalRandom.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
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	io/grpc/netty/shaded/io/netty/channel/epoll/LinuxSocket.java io/grpc/netty/shaded/io/netty/handler/codec/http2/HttpConversionUtil.java io/grpc/netty/shaded/io/netty/handler/codec/socksx/v4/Socks4ServerDecoder.java io/grpc/netty/shaded/io/netty/handler/codec/socksx/v5/Socks5CommandRequestDecoder.java io/grpc/netty/shaded/io/netty/handler/ssl/util/OpenJdkSelfSignedCertGenerator.java org/conscrypt/CertificatePriorityComparator.java org/conscrypt/ChainStrengthAnalyzer.java org/conscrypt/EvpMdRef.java org/conscrypt/OAEPParameters.java org/conscrypt/OidData.java org/conscrypt/OpenSSLCipherRSA.java org/conscrypt/OpenSSLECGroupContext.java org/conscrypt/OpenSSLProvider.java org/conscrypt/OpenSSLSignature.java org/conscrypt/TrustManagerImpl.java org/conscrypt/ct/CTConstants.java
7	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	coil/decode/SourceImageSource.java io/grpc/netty/shaded/io/netty/handler/codec/http/multipart/AbstractDiskHttpData.java io/grpc/netty/shaded/io/netty/handler/ssl/util/SelfSignedCertificate.java io/grpc/netty/shaded/io/netty/util/internal/NativeLibraryLoader.java org/conscrypt/NativeLibraryLoader.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/airbnb/lottie/network/NetworkCache.java com/appsflyer/internal/ag.java io/grpc/netty/shaded/io/netty/handler/codec/http/websocketx/WebSocketUtil.java io/grpc/okhttp/internal/Util.java
9	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/ifriend/chat/presentation/utils/ScreenshotDetectionDelegate.java io/sentry/android/core/DefaultAndroidEventProcessor.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/DefaultAndroidEventProcessor.java io/sentry/android/core/internal/util/RootChecker.java
11	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/RootChecker.java
12	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	io/grpc/netty/shaded/io/netty/handler/codec/http/websocketx/WebSocketUtil.java io/grpc/netty/shaded/io/netty/handler/ssl/util/FingerprintTrustManagerFactory.java

🏴 SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/x86/libconceal.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/x86/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/x86/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/x86/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/armeabi/libconceal.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/x86_64/libconceal.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/x86_64/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	lib/x86_64/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	lib/x86_64/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	lib/armeabi-v7a/libconceal.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	lib/armeabi-v7a/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	lib/armeabi-v7a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	lib/armeabi-v7a/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	lib/arm64-v8a/libconceal.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	lib/arm64-v8a/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	lib/arm64-v8a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	lib/arm64-v8a/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memmove_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	lib/x86/libconceal.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	lib/x86/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	lib/x86/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	lib/x86/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	lib/armeabi/libconceal.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	lib/x86_64/libconceal.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	lib/x86_64/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	lib/x86_64/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	lib/x86_64/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__read_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	lib/armeabi-v7a/libconceal.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	lib/armeabi-v7a/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	lib/armeabi-v7a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	lib/armeabi-v7a/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	lib/arm64-v8a/libconceal.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning 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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	lib/arm64-v8a/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
33	lib/arm64-v8a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	lib/arm64-v8a/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memmove_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	True info Symbols are stripped.

🪪 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

❗ OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

⚲ DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
smonitorsdk.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
www.evaapp.ai	ok	No Geolocation information available.
www.eclipse.org	ok	No Geolocation information available.
sdlsdk.s	ok	No Geolocation information available.
github.com	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
wiki.eclipse.org	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
drive.google.com	ok	No Geolocation information available.
api.ifriend.ai	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
www.openssl.org	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
svalidate.s	ok	No Geolocation information available.
resources.lovinga.com	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
play.google.com	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
tools.ietf.org	ok	No Geolocation information available.
cdn-settings.appsflyersdk.com	ok	No Geolocation information available.
cdn-testsettings.appsflyersdk.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
netty.io	ok	No Geolocation information available.
sstats.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
http-intake.logs.datadoghq.com	ok	No Geolocation information available.

🕵 TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OpenTelemetry (OpenCensus, OpenTracing)	Analytics	https://reports.exodus-privacy.eu.org/trackers/412

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyBvbDvA3CgaFc7E-RDl5BhDGkFdI4uu4IQ"
"com_facebook_device_auth_instructions" : "facebook.com/device􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀"
"facebook_client_token" : "7717d9e2e59a84bb14f178fe1a6a50d4"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"com_facebook_device_auth_instructions" : "􀀀􀀀facebook.com/device􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀􀀀"
"google_crash_reporting_api_key" : "AIzaSyBvbDvA3CgaFc7E-RDl5BhDGkFdI4uu4IQ"
"password" : "Password"
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
470fa2b4ae81cd56ecbcda9735803434cec591fa
cc2751449a350f668590264ed76692694a80308a
b4050a850c04b3abf54132565044b0b7d7bfd8ba270b39432355ffb4
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123

POSSIBLE SECRETS

eyJhbGciOiJSUzI1NiIsIng1YyI6WyJNSUlDNlRDQ0FkRUNBU293RFFZSktvWklodmNOQVFFTEJRQXdEeekVOTUFzR0ExVUVBd3dFVW05dmREQWVGdzB4TkRFeE1UZ3hOalUw TUROYUZ3MHpOREV4TVRNeE5qVTBNRE5hTUdZeEN6QUpCZ05WQkFZVEVFsVlRNUk13RVFZRFZRUUlEQXBEWVd4cFptOXlibWxoWxoTVJZd0ZBWURWUVFIREExTmIzVnVkR0Z wYmlCV2FXVjNNNUlF3RWdZRFZRUUtEQXRIYjI5bmJHVWdTVzVqTGpFVU1CSUdBMVVFQXd3T3TFptOXZMbUpoY2k1amIyMHdnZ0VpTUEwR0NTcUdTSWIzRFFFQkFRVUFBNEl CRHdBd2dnRUtBb0lCQVFEekZWS0pPa3FUUbXl5ak1IV0JPckxkcFltYzBFY3ZHM01vaGFWK1VKclZyST JTRHlrWThZV1NrVEt6OUJLbUY4SFAvR2pppQUERzMzE4NENlajliMVdleXZ WQjhSajNndUgzb0wrc0pUM3U5VjJ5NHp5bzV4TzZGV01CWUVRNlg4RGtHbFl0VHA1dGhlWWJSclhORUx1bDRsRitMdEhUQ2FBQU5STWtPbDBORW9MYTZCUmhPRzY4Z0 ZmSUF4eDVsVDhSRUU5dXR2UHV5K3JDYUJIbmZIT1BmOHBuMExTdmNlQmlqU0lGb1MzWTVjcmpQVmp5aVBBWlVlVlV25IVEZBaWxmSG5wTEJsR3hwQ3lsZVBRaE1LclBjZ 3ZEb0Q5bmQwTEE2eFlMRjdEUFhYU2E4RkxPK2ZQVjhDTkpDQXNGdXE5UmxmMlR0M1NqTHRXUll1aD2VMdWN0UDdBZ01CQUFFd0RRWUpLb1pJaHZjTkFRRUxCUUFFZ2 dFQkFFc01BQlpsKzhSbGGGswaHFCa3RzRHVycmk0bkYvMDdDDblNCZS96VWJUaVloTXByN1ZSSURsSExvZTVsc2xMaWxmWHp2YXltY01GZUgxdUJ4TndoZjdJTzdXdkl3UWVVS FNWK3JIeU55Z1RUaWVPMEpuOEh3KzRTQ29oSEFkTXZENVXRXduM0x2K1c0eTdPaGFTYnpsaFZDVkNuRkxxWS2ljQmF5VVhIdGRKWEpJQ29rUjQraC9XTk03ZzBpS1RoYW taT3lmYjhoMXBoeTdUTVRWbFBGS3JjVkRvNW05K0dodFFBDNFBOakdMb2s2ci9qeDQeDlDSU9DYXBJcWk4ZlhlKRU94S3ZpbFllQVlxZmpXdmh4MDBqdUVVQkhycENNROHdUNF RBK0xsSTAyY1J6NXJ4VzRGUUF6MU5kb0c5SFpEWlldhK05ORlRaZEFtdFdQSk1MZCs4TDHzbDQ9IiwiTUlJQzhUQ0NBZG1nQXdJQkFnSUpBBTU5JMTVIckd5bGdtNQTBHQ1NxR 1NJYjNJNEUUVCQ3dVQU1BOHhEVEFMQmdOVkJBTU1CRkp2YjNRd0hoY05VFF4TVRFNE1UWTFOREFF6V2hjTk16UXhNVEV6TVRZMU5EQXpXakFQTVEwd0N3WURWUVFER EFSU2IyT0BNSUlCSWpBTkJna3Foa2lHOXcwQkFRRUZBUU9EQVE4QU1JSUJDZ0tDQVFFQXplVU5jNGJTV0hoT1RVKzVNUS9sT21talFXcGZCaStGSnV4dm9lT21Rd2k2ZnJQS 0tzYUtLWUdmQ1RQbEtFMGRtckVQOTVibmxvvcUw1eEFwUDE3b3JqVWU2S1J0SkF3Rk5JNUVaYWRJZmpiaC9xKzg1QzFDcDJCUzJZbXVbXpYYWkhQNjN5eUJwMDVZY2JNS3 dDQkhYYUFnWWJtVFRrKzQrMXBqTnBIUDZZaUYyZ0NQdlNmem9rR3loYnZZCcW5QYm5UZEk5dzZmak5CWUFici91Qk9UVTB2SzRrdHpsV2s1bHZzbTUxZTh2c0xTcVdob0 hBRHEwQXJpQWVsVTRTHNTQUNrUlVRU3hXVjBLNWh6VHY0ZWN2Q2JHOWRza2lEQ3dXZyt1VFJTb0FGZVppaE9OTDAwMHE3VmV5M0RaVGNMbDgvTzROUVZhWll1aU FnVldsV2Nzd0lEQVFBQm8xQXdUakFkQmdOVkhRNEVGZ1FVc2ltbElsSRGNKUjBvZll3b004S3dIRk9IK3NJd0h3WURWUjBqQkQ0ZvQVVzaW1sSVJEY0pSMG9mUjdvTThLd0 hGT0grc0l3REFZRFZSMFRCQVV3QXdFQFi96QU5CZ2txaGtpRzl3MEJBUXNGQUFPQ0FRRUFXUWw4U21iUW9CVjN0ak9KOHpNbGGNOMHhPUHBTU05ieDBnN0VML2RRZ0p wZXQwTWNXNjJSSGxnUUFPS2JTM1BSZW8ybnNSQi9aUnlZRHU0aTEzWkhaOGJNc0dPRVM0QlFwejEzbXRtWGc5UmhzWHFMMGVEWWZCY2pqdGxydVVieEghuQUxwNFZ OMXpWZHlXQVBDDajBldTNNeHBnTVdjeW41MFFtaUpTai9FcXUvbExodmUvd0t2akc1V2huVjh1UktSdUZiRmN0MERIQUhNblpxRkhjjR1M1U28wY1luU2ZLNWZiQlJOZWxH ZmxocGJiUHAwVjBhWGxaW5xRDBZZTNPYVpkRnErMnJQMW9DL2E1L091NExzcFkzYjVvRDlyRU5keTdicTBLZXdQRnRnUHZVa0pySjNUemJpd3ZwZ2haN3pHMjZibko1ST d1YzR5MVZ1anFhT0E9PSJdfQ

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

9b8f518b086098de3d77736f9458a3d2f6f95a37

51953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

POSSIBLE SECRETS

FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212

115792089210356248762697446949407573530086143415290314195533631308867097853951

W1zcp5YuPDw8mIQDVCH2uQY7qs2ejdZj5LIgIz4CbQ0wg53rlwE7DDQM6MNUgZLnzNmMSMfFrpE7

8a3c4b262d721acd49a4bf97d5213199c86fa2b9

3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F

16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

7b58a99c6712905b57726b9d4b987e4d

edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901

051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

01360240043788015936020505

E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1

2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3

686479766013060971498190079908139321726943530014330540939446345918554318339765539424507746333217197532963996371363321113864768612440380340372808892707005449

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

POSSIBLE SECRETS

39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

bd376388b5f723fb4c22dfe6cd4375a05a07476444d5819985007e34

df6b721c8b4d3b6eb44c861d4415007e5a35fc95

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

yHTAZeApn5rh6Uzfx06Gv6eHdM34YL

115792089210356248762697446949407573529996955224135760342422259061068512044369

tgLRb4bjuZVA8xvQ9uHNs8UtpBIOiUcagzvtKyyfCofk5U5sNb54GgVVYxa6p4A1ObdJv1jjlUOnzR8keX5LsAM4Ia7xeqiFh0GER4l0ulVChy

6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

b70e0cbd6bb4bf7f321390b94a03c1d356c21122343280d6115c1d21

eWzIsJF4PExQap9HK6Vlz8DGlgGwoiLCtyOEK0Bfu

b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

9a04f079-9840-4286-ab92-e65be0885f95

e2719d58-a985-b3c9-781a-b030af78d30e

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

c56fb7d591ba6704df047fd98f535372fea00211

Report Generated by - MobSF v3.7.9 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.