ANDROID STATIC ANALYSIS REPORT

app_icon

CRICFy TV (5.0)

File Name:	cricfy-v5.5-cricfy.pro.apk
Package Name:	com.cricfy.tv
Scan Date:	Nov. 17, 2025, 2:10 p.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	23	2	2	1

FILE INFORMATION

File Name: cricfy-v5.5-cricfy.pro.apk
Size: 15.17MB
MD5: afb3d68c11410e19b8ab54634008dd47
SHA1: 4dd072af8582639f9cc1256ba5b70207678caefa
SHA256: 4e3e41e31451b7d750c0d29a2b0b2142d13071be4b0a562a40492fbead2e54a2

APP INFORMATION

App Name: CRICFy TV
Package Name: com.cricfy.tv
Main Activity: com.android.vending.tv.activities.Splash
Target SDK: 35
Min SDK: 21
Max SDK:
Android Version Name: 5.0
Android Version Code: 30

APP COMPONENTS

Activities: 13
Services: 14
Receivers: 14
Providers: 4
Exported Activities: 1
Exported Services: 1
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Vaishali Manpreet Basak, OU=Single, O=Individual, L=Bangalore, ST=Bangalore, C=91
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-10-22 09:29:55+00:00
Valid To: 2048-10-15 09:29:55+00:00
Issuer: CN=Vaishali Manpreet Basak, OU=Single, O=Individual, L=Bangalore, ST=Bangalore, C=91
Serial Number: 0x1
Hash Algorithm: sha256
md5: 5c163b1e7c0d318b7a1052158e7fd4de
sha1: f89a3c973f313ee413aca1e82980384c21987aa3
sha256: ad1b1fa1a1076416df7fc91c2ff6c9dbdf972d26b4b1eb5aada3b019673731b2
sha512: 7c2d1b5c89bd639aadda76c492eb2440095df5bad850764c11d62499b8bcd737395e5b5030e4a8fea2f63fae9c0371c9ea5f871fa69b5c0712257017ac27a35a
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: d6027d251dffb7f1c6b77df4371b4190ba1b3d8f8b612146c1430e22371100c9
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.Ad_ID	unknown	Unknown permission	Unknown permission from android reference
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.

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.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.cricfy.tv.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
Build.TAGS check
SIM operator check
network operator name check
ro.product.device check
ro.kernel.qemu check
possible ro.secure check
emulator file check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
lib/arm64-v8a/libtoolChecker.so	FINDINGS: anti_root — DETAILS: RootBeer
lib/armeabi-v7a/libtoolChecker.so	FINDINGS: anti_root — DETAILS: RootBeer
lib/x86/libtoolChecker.so	FINDINGS: anti_root — DETAILS: RootBeer
lib/x86_64/libtoolChecker.so	FINDINGS: anti_root — DETAILS: RootBeer

BROWSABLE ACTIVITIES

ACTIVITY	INTENT

ACTIVITY	INTENT
com.android.vending.tv.activities.PlayerActivity	Schemes: file://, content://, http://, https://, Hosts: *, Mime Types: video/*, Path Patterns: .*.3g2, .*..*.3g2, .*..*..*.3g2, .*..*..*..*.3g2, .*..*..*..*..*.3g2, .*..*..*..*..*..*.3g2, .*..*..*..*..*..*..*.3g2, .*.3gp, .*..*.3gp, .*..*..*.3gp, .*..*..*..*.3gp, .*..*..*..*..*.3gp, .*..*..*..*..*..*.3gp, .*..*..*..*..*..*..*.3gp, .*.3gp2, .*..*.3gp2, .*..*..*.3gp2, .*..*..*..*.3gp2, .*..*..*..*..*.3gp2, .*..*..*..*..*..*.3gp2, .*..*..*..*..*..*..*.3gp2, .*.3gpp, .*..*.3gpp, .*..*..*.3gpp, .*..*..*..*.3gpp, .*..*..*..*..*.3gpp, .*..*..*..*..*..*.3gpp, .*..*..*..*..*..*..*.3gpp, .*.mkv, .*..*.mkv, .*..*..*.mkv, .*..*..*..*.mkv, .*..*..*..*..*.mkv, .*..*..*..*..*..*.mkv, .*..*..*..*..*..*..*.mkv, .*.mp4, .*..*.mp4, .*..*..*.mp4, .*..*..*..*.mp4, .*..*..*..*..*.mp4, .*..*..*..*..*..*.mp4, .*..*..*..*..*..*..*.mp4, .*.webm, .*..*.webm, .*..*..*.webm, .*..*..*..*.webm, .*..*..*..*..*.webm, .*..*..*..*..*..*.webm, .*..*..*..*..*..*..*.webm, .*.3G2, .*..*.3G2, .*..*..*.3G2, .*..*..*..*.3G2, .*..*..*..*..*.3G2, .*..*..*..*..*..*.3G2, .*..*..*..*..*..*..*.3G2, .*.3GP, .*..*.3GP, .*..*..*.3GP, .*..*..*..*.3GP, .*..*..*..*..*.3GP, .*..*..*..*..*..*.3GP, .*..*..*..*..*..*..*.3GP, .*.3GP2, .*..*.3GP2, .*..*..*.3GP2, .*..*..*..*.3GP2, .*..*..*..*..*.3GP2, .*..*..*..*..*..*.3GP2, .*..*..*..*..*..*..*.3GP2, .*.3GPP, .*..*.3GPP, .*..*..*.3GPP, .*..*..*..*.3GPP, .*..*..*..*..*.3GPP, .*..*..*..*..*..*.3GPP, .*..*..*..*..*..*..*.3GPP, .*.MP4, .*..*.MP4, .*..*..*.MP4, .*..*..*..*.MP4, .*..*..*..*..*.MP4, .*..*..*..*..*..*.MP4, .*..*..*..*..*..*..*.MP4, .*.m3u8, .*..*.m3u8, .*..*..*.m3u8, .*..*..*..*.m3u8, .*..*..*..*..*.m3u8, .*..*..*..*..*..*.m3u8, .*..*..*..*..*..*..*.m3u8, .*.M3U8, .*..*.M3U8, .*..*..*.M3U8, .*..*..*..*.M3U8, .*..*..*..*..*.M3U8, .*..*..*..*..*..*.M3U8, .*..*..*..*..*..*..*.M3U8, .*.WEBM, .*..*.WEBM, .*..*..*.WEBM, .*..*..*..*.WEBM, .*..*..*..*..*.WEBM, .*..*..*..*..*..*.WEBM, .*..*..*..*..*..*..*.WEBM, .*.MKV, .*..*.MKV, .*..*..*.MKV, .*..*..*..*.MKV, .*..*..*..*..*.MKV, .*..*..*..*..*..*.MKV, .*..*..*..*..*..*..*.MKV,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

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: **2** | WARNING: **8** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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.
4	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
5	Activity (com.android.vending.tv.activities.PlayerActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	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.
7	Broadcast Receiver (com.startapp.sdk.adsbase.remoteconfig.BootCompleteListener) 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.
8	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
9	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

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

</> CODE ANALYSIS

HIGH: **2** | WARNING: **11** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/startapp/sdk/ads/interstitials/InterstitialAd.java com/startapp/sdk/internal/cl.java com/startapp/sdk/internal/g.java com/startapp/sdk/internal/nc.java com/startapp/sdk/internal/xh.java com/startapp/simple/bloomfilter/creation/TokenToBitSet.java com/unity3d/ads/UnityAdsBaseOptions.java com/unity3d/ads/adplayer/CommonGetWebViewCacheAssetLoader$invoke$1.java com/unity3d/ads/adplayer/CommonWebViewBridge.java com/unity3d/ads/core/data/datasource/AndroidDynamicDeviceInfoDataSource.java com/unity3d/ads/core/data/datasource/AndroidStaticDeviceInfoDataSource.java com/unity3d/ads/core/data/repository/AndroidDiagnosticEventRepository.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/unity3d/ads/core/domain/AndroidInitializeBoldSDK.java com/unity3d/ads/core/domain/CommonShouldAllowInitialization.java com/unity3d/ads/core/domain/LegacyLoadUseCase.java com/unity3d/ads/core/domain/LegacyShowUseCase$showError$1.java com/unity3d/ads/core/domain/LegacyShowUseCase.java com/unity3d/ads/gatewayclient/CommonGatewayClient.java com/unity3d/ads/metadata/InAppPurchaseMetaData.java com/unity3d/ads/metadata/MetaData.java com/unity3d/services/SDKErrorHandler.java com/unity3d/services/UnityServices.java com/unity3d/services/ads/UnityAdsImplementation.java com/unity3d/services/ads/adunit/AdUnitActivityController.java com/unity3d/services/ads/adunit/AdUnitViewHandlerFactory.java com/unity3d/services/ads/adunit/VideoPlayerHandler.java com/unity3d/services/ads/api/AdUnit.java com/unity3d/services/ads/api/VideoPlayer.java com/unity3d/services/ads/api/WebPlayer.java com/unity3d/services/ads/gmascar/adapters/ScarAdapterFactory.java com/unity3d/services/ads/gmascar/bridges/AdapterStatusBridge.java com/unity3d/services/ads/gmascar/bridges/InitializeListenerBridge.java com/unity3d/services/ads/gmascar/bridges/mobileads/MobileAdsBridge.java com/unity3d/services/ads/gmascar/bridges/mobileads/MobileAdsBridgeLegacy.java com/unity3d/services/ads/gmascar/finder/GMAInitializer.java com/unity3d/services/ads/gmascar/finder/ScarVersionFinder.java com/unity3d/services/ads/token/InMemoryAsyncTo

NO	ISSUE	SEVERITY	STANDARDS	FILES
				kenStorage.java com/unity3d/services/ads/token/NativeTokenGenerator.java com/unity3d/services/ads/topics/TopicsReceiver.java com/unity3d/services/ads/topics/TopicsService.java com/unity3d/services/ads/video/VideoPlayerView.java com/unity3d/services/ads/webplayer/WebPlayerView.java com/unity3d/services/banners/BannerView.java com/unity3d/services/banners/UnityBanners.java com/unity3d/services/core/api/Cache.java com/unity3d/services/core/api/DeviceInfo.java com/unity3d/services/core/api/Intent.java com/unity3d/services/core/api/Request.java com/unity3d/services/core/api/Sdk.java com/unity3d/services/core/broadcast/BroadcastEventReceiver.java com/unity3d/services/core/cache/CacheDirectory.java com/unity3d/services/core/cache/CacheThread.java com/unity3d/services/core/cache/CacheThreadHandler.java com/unity3d/services/core/configuration/ConfigurationReader.java com/unity3d/services/core/configuration/ConfigurationRequestFactory.java com/unity3d/services/core/configuration/EnvironmentCheck.java com/unity3d/services/core/configuration/ExperimentsReader.java com/unity3d/services/core/configuration/InitializationNotificationCenter.java com/unity3d/services/core/configuration/InitializeEventsMetricSender.java com/unity3d/services/core/configuration/InitializeThread.java com/unity3d/services/core/configuration/PrivacyConfigurationLoader.java com/unity3d/services/core/connectivity/ConnectivityMonitor.java com/unity3d/services/core/device/AdvertisingId.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a com/unity3d/services/core/device/Device.java com/unity3d/services/core/device/OpenAdvertisingId.java com/unity3d/services/core/device/Storage.java com/unity3d/services/core/device/reader/DeviceInfoReaderCompressor.java com/unity3d/services/core/device/reader/DeviceInfoReaderExtended.java com/unity3d/services/core/domain/task/InitializeSDK$doWork$2.java com/unity3d/services/core/domain/task/InitializeStateConfig$doWork$2.java com/unity3d/services/core/domain/task/InitializeStateCreate$doWork$2.java com/unity3d/services/core/domain/task/InitializeStateError$doWork$2.java com/unity3d/services/core/domain/task/InitializeStateLoadCache$doWork$2.java com/unity3d/services/core/domain/task/InitializeStateLoadCache.java com/unity3d/services/core/domain/task/InitializeStateLoadWeb$doWork$2.java com/unity3d/services/core/domain/task/InitializeStateNetworkError$doWork$2.java com/unity3d/services/core/domain/task/InitializeStateNetworkError.java com/unity3d/services/core/domain/task/InitializeStateReset$doWork$2.java com/unity3d/services/core/extensions/TaskExtensionsKt.java com/unity3d/services/core/log/DeviceLog.java com/unity3d/services/core/misc/JsonFlattener.java com/unity3d/services/core/misc/JsonStorage.java com/unity3d/services/core/misc/JsonStorageAggregator.java com/unity3d/services/core/misc/Utilities.java com/unity3d/services/core/misc/ViewUtilities.java com/unity3d/services/core/preferences/AndroidPreferences.java com/unity3d/services/core/properties/ClientProperties.java com/unity3d/services/core/properties/SdkPropertie

NO	ISSUE	SEVERITY	STANDARDS	FILES
				s.java com/unity3d/services/core/reflection/GenericBridge.java com/unity3d/services/core/request/WebRequest.java com/unity3d/services/core/request/WebRequestRunnable.java com/unity3d/services/core/request/WebRequestThread.java com/unity3d/services/core/request/metrics/MetricCommonTags.java com/unity3d/services/core/request/metrics/MetricSender$sendMetrics$$inlined$CoroutineExceptionHandler$1.java com/unity3d/services/core/request/metrics/MetricSender$sendMetrics$1.java com/unity3d/services/core/request/metrics/MetricSender.java com/unity3d/services/core/request/metrics/MetricSenderWithBatch.java com/unity3d/services/core/request/metrics/SDKMetrics.java com/unity3d/services/core/sensorinfo/SensorInfoListener.java com/unity3d/services/core/timer/BaseTimer.java com/unity3d/services/core/webview/WebView.java com/unity3d/services/core/webview/WebViewApp.java com/unity3d/services/core/webview/WebViewUrlBuilder.java com/unity3d/services/core/webview/bridge/Invocation.java com/unity3d/services/core/webview/bridge/NativeCallback.java com/unity3d/services/core/webview/bridge/WebViewBridge.java com/unity3d/services/core/webview/bridge/WebViewBridgeInterface.java com/unity3d/services/core/webview/bridge/WebViewCallback.java com/unity3d/services/store/core/StoreLifecycleListener.java com/unity3d/services/store/gpbl/bridges/CommonJ

NO	ISSUE	SEVERITY	STANDARDS	FILES
				sonResponseBridge.java com/unity3d/services/store/gpbl/bridges/PurchaseBridge.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	io/nn/lp/Loopop.java io/nn/lp/boot/BootReceiver.java io/nn/lp/service/LoopopService.java io/nn/lpop/AQ.java io/nn/lpop/AX.java io/nn/lpop/AbstractC0059Af.java io/nn/lpop/AbstractC1058dY.java io/nn/lpop/AbstractC1070df.java io/nn/lpop/AbstractC1367gm0.java io/nn/lpop/AbstractC1394h2.java io/nn/lpop/AbstractC1413hD.java io/nn/lpop/AbstractC1449hg0.java io/nn/lpop/AbstractC1635jg0.java io/nn/lpop/AbstractC1734kj.java io/nn/lpop/AbstractC2033nr0.java io/nn/lpop/AbstractC2044nz.java io/nn/lpop/AbstractC2129os0.java io/nn/lpop/AbstractC2206pk.java io/nn/lpop/AbstractC2294qh.java io/nn/lpop/AbstractC2309qo0.java io/nn/lpop/AbstractC2351rE.java io/nn/lpop/AbstractC2372rZ.java io/nn/lpop/AbstractC2506st0.java io/nn/lpop/AbstractC2511sx.java io/nn/lpop/AbstractC2726vD.java io/nn/lpop/AbstractC3032ya0.java io/nn/lpop/AbstractC3106zH.java io/nn/lpop/AbstractComponentCallbacksC0284Iw.java io/nn/lpop/AbstractServiceC1750kr.java io/nn/lpop/AnimationAnimationListenerC0248Hm.java io/nn/lpop/Au0.java io/nn/lpop/B4.java io/nn/lpop/B9.java io/nn/lpop/BO.java io/nn/lpop/BP.java io/nn/lpop/BQ.java io/nn/lpop/BinderC1236fO.java io/nn/lpop/BinderC1550ik0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/nn/lpop/BinderC1929nm0.java io/nn/lpop/BinderC2684uo0.java io/nn/lpop/BinderC3154zo0.java io/nn/lpop/Bn0.java io/nn/lpop/C0113Ch.java io/nn/lpop/C0191Fh.java io/nn/lpop/C0222Gm.java io/nn/lpop/C0274Im.java io/nn/lpop/C0316Kc.java io/nn/lpop/C0337Kx.java io/nn/lpop/C0346Lg.java io/nn/lpop/C0441Oy.java io/nn/lpop/C0486Qr.java io/nn/lpop/C0508Rn.java io/nn/lpop/C0512Rr.java io/nn/lpop/C0571Ty.java io/nn/lpop/C0579Ug.java io/nn/lpop/C0597Uy.java io/nn/lpop/C0605Vg.java io/nn/lpop/C0616Vr.java io/nn/lpop/C0655Xe.java io/nn/lpop/C0664Xn.java io/nn/lpop/C0675Xy.java io/nn/lpop/C0707Ze.java io/nn/lpop/C0708Zf.java io/nn/lpop/C0734a2.java io/nn/lpop/C0808aq.java io/nn/lpop/C0821ax.java io/nn/lpop/C0900bo0.java io/nn/lpop/C0921c1.java io/nn/lpop/C0945cG.java io/nn/lpop/C0990cm0.java io/nn/lpop/C0996cp0.java io/nn/lpop/C1040dG.java io/nn/lpop/C1102dv0.java io/nn/lpop/C1104dx.java io/nn/lpop/C1155ea0.java io/nn/lpop/C1203f00.java io/nn/lpop/C1292fx.java io/nn/lpop/C1377gr0.java io/nn/lpop/C1382gu.java io/nn/lpop/C1388gz.java io/nn/lpop/C1441hc0.java io/nn/lpop/C1482hz.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/nn/lpop/C1482hz.java io/nn/lpop/C1492i4.java io/nn/lpop/C1515iL.java io/nn/lpop/C1520iQ.java io/nn/lpop/C1523iT.java io/nn/lpop/C1568iu.java io/nn/lpop/C1572ix.java io/nn/lpop/C1594j9.java io/nn/lpop/C1688k9.java io/nn/lpop/C1729kg0.java io/nn/lpop/C1762kz.java io/nn/lpop/C1845lr0.java io/nn/lpop/C1850lu.java io/nn/lpop/C1871m60.java io/nn/lpop/C1893mP.java io/nn/lpop/C1903mZ.java io/nn/lpop/C1916mg.java io/nn/lpop/C1924mk.java io/nn/lpop/C1997nZ.java io/nn/lpop/C2038nu.java io/nn/lpop/C2057o50.java io/nn/lpop/C2103of0.java io/nn/lpop/C2104og.java io/nn/lpop/C2115ol0.java io/nn/lpop/C2121oo0.java io/nn/lpop/C2138oz.java io/nn/lpop/C2171pL.java io/nn/lpop/C2198pg.java io/nn/lpop/C2209pl0.java io/nn/lpop/C2230px.java io/nn/lpop/C2244q5.java io/nn/lpop/C2312qq.java io/nn/lpop/C2333r3.java io/nn/lpop/C2356rJ.java io/nn/lpop/C2527t6.java io/nn/lpop/C2575th.java io/nn/lpop/C2599tt.java io/nn/lpop/C2674uj0.java io/nn/lpop/C2746vX.java io/nn/lpop/C2789vu.java io/nn/lpop/C2798w00.java io/nn/lpop/C2824wH.java io/nn/lpop/C2828wL.java io/nn/lpop/C2844wa0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/nn/lpop/C2860wi0.java io/nn/lpop/C2917xG.java io/nn/lpop/C2920xJ.java io/nn/lpop/C2948xf0.java io/nn/lpop/C2953xi.java io/nn/lpop/C2955xj.java io/nn/lpop/C2990y20.java io/nn/lpop/C3012yH.java io/nn/lpop/C3045yh.java io/nn/lpop/C3108zJ.java io/nn/lpop/C3160zr0.java io/nn/lpop/C5.java io/nn/lpop/CV.java io/nn/lpop/CallableC0294Jg.java io/nn/lpop/DD.java io/nn/lpop/DL.java io/nn/lpop/DQ.java io/nn/lpop/Db0.java io/nn/lpop/DialogInterfaceOnCancelListenerC0560Tn.java io/nn/lpop/DialogInterfaceOnClickListenerC1494i5.java io/nn/lpop/DialogInterfaceOnClickListenerC2023nm0.java io/nn/lpop/Dk0.java io/nn/lpop/EQ.java io/nn/lpop/Eb0.java io/nn/lpop/FM.java io/nn/lpop/Fb0.java io/nn/lpop/Fq0.java io/nn/lpop/Fs0.java io/nn/lpop/G5.java io/nn/lpop/GQ.java io/nn/lpop/H60.java io/nn/lpop/HandlerC2211pm0.java io/nn/lpop/HandlerC3058yn0.java io/nn/lpop/IL.java io/nn/lpop/Ib0.java io/nn/lpop/Ic0.java io/nn/lpop/J4.java io/nn/lpop/Jb0.java io/nn/lpop/Jh0.java io/nn/lpop/K4.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/nn/lpop/K80.java io/nn/lpop/Kb0.java io/nn/lpop/Kj0.java io/nn/lpop/L9.java io/nn/lpop/LL.java io/nn/lpop/LZ.java io/nn/lpop/LayoutInflaterFactory2C0465Pw.java io/nn/lpop/Le0.java io/nn/lpop/Lj0.java io/nn/lpop/Ll0.java io/nn/lpop/M3.java io/nn/lpop/ML.java io/nn/lpop/MQ.java io/nn/lpop/Mi0.java io/nn/lpop/Mr0.java io/nn/lpop/Mu0.java io/nn/lpop/N0.java io/nn/lpop/N1.java io/nn/lpop/NX.java io/nn/lpop/Nb0.java io/nn/lpop/Nd0.java io/nn/lpop/Nr0.java io/nn/lpop/O4.java io/nn/lpop/OZ.java io/nn/lpop/Od0.java io/nn/lpop/Pd0.java io/nn/lpop/Pj0.java io/nn/lpop/Pm0.java io/nn/lpop/QR.java io/nn/lpop/Qd0.java io/nn/lpop/Qk0.java io/nn/lpop/R30.java io/nn/lpop/R4.java io/nn/lpop/RB.java io/nn/lpop/RQ.java io/nn/lpop/RunnableC0242Hg.java io/nn/lpop/RunnableC0969cc.java io/nn/lpop/RunnableC1074dh.java io/nn/lpop/RunnableC1689k90.java io/nn/lpop/RunnableC2531t8.java io/nn/lpop/RunnableC2972xr0.java io/nn/lpop/RunnableC3076yy.java io/nn/lpop/S2.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/nn/lpop/S4.java io/nn/lpop/SD.java io/nn/lpop/SF.java io/nn/lpop/Sd0.java io/nn/lpop/ServiceConnectionC1737kk0.java io/nn/lpop/Sq0.java io/nn/lpop/St0.java io/nn/lpop/TO.java io/nn/lpop/To0.java io/nn/lpop/U1.java io/nn/lpop/U4.java io/nn/lpop/U80.java io/nn/lpop/UN.java io/nn/lpop/V1.java io/nn/lpop/V80.java io/nn/lpop/VZ.java io/nn/lpop/ViewOnKeyListenerC0134Dc.java io/nn/lpop/Vo0.java io/nn/lpop/X70.java io/nn/lpop/X90.java io/nn/lpop/XM.java io/nn/lpop/XX.java io/nn/lpop/Xl0.java io/nn/lpop/Yf0.java io/nn/lpop/Z40.java io/nn/lpop/ZB.java io/nn/lpop/ZU.java io/nn/lpop/ZV.java io/nn/lpop/Ze0.java io/nn/lpop/Zq0.java io/nn/lpop/rv0.java io/nn/lpop/wv0.java
2	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/unity3d/ads/core/data/datasource/AndroidStaticDeviceInfoDataSource.java com/unity3d/services/core/device/Device.java io/nn/lpop/FQ.java io/nn/lpop/R4.java io/nn/lpop/RB.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/startapp/sdk/adsbase/cache/a.java com/startapp/sdk/internal/el.java com/startapp/sdk/internal/gj.java com/startapp/sdk/internal/p.java com/unity3d/services/core/configuration/Configuration.java io/nn/lpop/AbstractC2421s0.java io/nn/lpop/C0150Ds.java io/nn/lpop/C0501Rg.java io/nn/lpop/C0605Vg.java io/nn/lpop/C0805ao0.java io/nn/lpop/C0909bt.java io/nn/lpop/C0930c50.java io/nn/lpop/C1003ct.java io/nn/lpop/C1075dh0.java io/nn/lpop/C1102dv0.java io/nn/lpop/C1535ic0.java io/nn/lpop/C2385rg.java io/nn/lpop/C2867wm.java io/nn/lpop/C2879ws.java io/nn/lpop/C3024yT.java io/nn/lpop/Eb0.java io/nn/lpop/KY.java io/nn/lpop/LY.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/startapp/sdk/internal/ge.java com/startapp/sdk/internal/s9.java io/nn/lpop/Au0.java io/nn/lpop/Bq0.java io/nn/lpop/Bv0.java io/nn/lpop/C0259Hx.java io/nn/lpop/C0423Og.java io/nn/lpop/C1649jn0.java io/nn/lpop/C2212pn.java io/nn/lpop/H20.java io/nn/lpop/Le0.java io/nn/lpop/Nq0.java io/nn/lpop/OT.java io/nn/lpop/RunnableC0082Bc.java io/nn/lpop/SD.java io/nn/lpop/U00.java io/nn/lpop/Xl0.java io/nn/lpop/ZL.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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/unity3d/ads/core/configuration/GameServerIdReader.java com/unity3d/ads/core/data/datasource/AndroidMediationDataSource.java com/unity3d/ads/core/data/datasource/AndroidTcfDataSource.java com/unity3d/ads/metadata/InAppPurchaseMetaData.java com/unity3d/services/ads/gmascar/utils/ScarConstants.java com/unity3d/services/core/configuration/ExperimentObject.java com/unity3d/services/core/device/reader/DeviceInfoReaderFilterProvider.java com/unity3d/services/core/device/reader/JsonStorageKeyNames.java com/unity3d/services/core/properties/SdkProperties.java io/nn/lpop/AM.java io/nn/lpop/FJ.java
6	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/startapp/sdk/ads/banner/bannerstandard/BannerStandard.java com/startapp/sdk/internal/hb.java com/unity3d/services/ads/webplayer/WebPlayerView.java com/unity3d/services/core/webview/WebView.java io/nn/lpop/N6.java
7	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/startapp/sdk/internal/sj.java io/nn/lpop/C1075dh0.java io/nn/lpop/C1102dv0.java io/nn/lpop/Fe0.java io/nn/lpop/MQ.java io/nn/lpop/wv0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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/startapp/sdk/internal/i7.java com/unity3d/ads/core/data/datasource/AndroidDynamicDeviceInfoDataSource.java com/unity3d/services/core/cache/CacheDirectory.java io/nn/lpop/C0771aV.java
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/startapp/sdk/internal/i7.java com/startapp/sdk/internal/il.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/startapp/sdk/internal/of.java io/nn/lpop/C2690ur0.java
11	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	io/nn/lpop/T2.java
12	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/startapp/sdk/internal/q.java
13	Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	io/nn/lpop/Ll0.java
14	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/startapp/sdk/internal/jd.java io/nn/lpop/C2904x60.java io/nn/lpop/Fs0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
15	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/unity3d/services/core/webview/WebView.java
16	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/startapp/sdk/internal/nf.java com/startapp/sdk/internal/of.java io/nn/lpop/Ze0.java
17	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	io/nn/lpop/C1398h4.java

SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	x86/libgav1JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	x86/libffmpegJNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	x86/libnativesdk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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', '__memset_chk', '__vsnprintf_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	armeabi-v7a/libgav1JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	armeabi-v7a/libffmpegJNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi-v7a/libnativesdk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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', '__memset_chk', '__vsnprintf_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	armeabi-v7a/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86_64/libgav1JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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', '__memset_chk', '__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86_64/libffmpegJNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	x86_64/libnativesdk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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', '__memset_chk', '__vsnprintf_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__strchr_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	x86_64/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	arm64-v8a/libgav1JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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', '__strlen_chk', '__memcpy_chk', '__memmove_chk', '__memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	arm64-v8a/libffmpegJNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	arm64-v8a/libnativesdk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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', '__memset_chk', '__vsnprintf_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__strchr_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	arm64-v8a/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	x86/libgav1JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	x86/libffmpegJNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	x86/libnativesdk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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', '__memset_chk', '__vsnprintf_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	x86/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	armeabi-v7a/libgav1JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	armeabi-v7a/libffmpegJNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	armeabi-v7a/libnativesdk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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', '__memset_chk', '__vsnprintf_chk', '__strchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	armeabi-v7a/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	x86_64/libgav1JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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', '__memset_chk', '__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	x86_64/libffmpegJNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	x86_64/libnativesdk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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', '__memset_chk', '__vsnprintf_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__strchr_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	x86_64/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	arm64-v8a/libgav1JNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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', '__strlen_chk', '__memcpy_chk', '__memmove_chk', '__memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	arm64-v8a/libffmpegJNI.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	arm64-v8a/libnativesdk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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', '__memset_chk', '__vsnprintf_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__strchr_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	arm64-v8a/libtoolChecker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	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.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/startapp/sdk/internal/gj.java com/startapp/sdk/internal/j0.java com/startapp/sdk/internal/t6.java com/startapp/sdk/internal/xh.java com/unity3d/ads/core/domain/AndroidHandleOpenUrl.java com/unity3d/services/core/api/Intent.java io/nn/lpop/AbstractC1070df.java io/nn/lpop/Au0.java io/nn/lpop/C0675Xy.java io/nn/lpop/C1482hz.java io/nn/lpop/C1792lI.java io/nn/lpop/C2599tt.java io/nn/lpop/Fe0.java io/nn/lpop/RunnableC3087z4.java io/nn/lpop/S1.java io/nn/lpop/U1.java io/nn/lpop/ZU.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/startapp/sdk/internal/gj.java com/startapp/sdk/internal/j0.java com/startapp/sdk/internal/t6.java com/unity3d/ads/core/domain/AndroidHandleOpenUrl.java com/unity3d/services/core/api/Intent.java io/nn/lpop/C1482hz.java io/nn/lpop/C1792lI.java io/nn/lpop/Fe0.java io/nn/lpop/S1.java io/nn/lpop/U1.java io/nn/lpop/ZU.java

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	com/unity3d/services/core/api/Cache.java com/unity3d/services/core/api/DeviceInfo.java com/unity3d/services/core/configuration/Configuration.java com/unity3d/services/core/device/Device.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/startapp/sdk/internal/d7.java com/startapp/sdk/internal/hf.java com/startapp/sdk/internal/i7.java com/startapp/sdk/internal/jd.java com/startapp/sdk/internal/k2.java com/startapp/sdk/internal/p7.java com/unity3d/ads/core/domain/GetCachedAsset.java com/unity3d/services/core/cache/CacheDirectory.java com/unity3d/services/core/device/Device.java com/unity3d/services/core/misc/Utilities.java io/nn/lpop/AQ.java io/nn/lpop/AbstractC0696Yt.java io/nn/lpop/AbstractC1070df.java io/nn/lpop/AbstractC2309qo0.java io/nn/lpop/Bn0.java io/nn/lpop/C0476Qh.java io/nn/lpop/C0616Vr.java io/nn/lpop/C0868bX.java io/nn/lpop/C2201ph0.java io/nn/lpop/C2953xi.java io/nn/lpop/C3113zO.java io/nn/lpop/CallableC0268lg.java io/nn/lpop/DQ.java io/nn/lpop/E7.java io/nn/lpop/Fs0.java io/nn/lpop/H50.java io/nn/lpop/IQ.java io/nn/lpop/KV.java io/nn/lpop/LH.java io/nn/lpop/M50.java io/nn/lpop/N1.java io/nn/lpop/Od0.java io/nn/lpop/Pd0.java io/nn/lpop/RQ.java io/nn/lpop/Sq0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/startapp/sdk/internal/gj.java com/startapp/sdk/internal/j0.java com/startapp/sdk/internal/xh.java io/nn/lpop/AbstractC1070df.java io/nn/lpop/AbstractC2033nr0.java io/nn/lpop/C0107Cb.java io/nn/lpop/C0663Xm.java io/nn/lpop/C0868bX.java io/nn/lpop/C1482hz.java io/nn/lpop/K80.java io/nn/lpop/S1.java io/nn/lpop/ZU.java
00096	Connect to a URL and set request method	command network	com/startapp/sdk/internal/y8.java com/unity3d/services/core/request/WebRequest.java io/nn/lpop/C0316Kc.java io/nn/lpop/C0895bm.java io/nn/lpop/C1128eA.java io/nn/lpop/Ll0.java
00089	Connect to a URL and receive input stream from the server	command network	com/startapp/sdk/internal/jd.java com/startapp/sdk/internal/q2.java com/startapp/sdk/internal/y8.java com/unity3d/services/core/request/WebRequest.java io/nn/lpop/C0316Kc.java io/nn/lpop/C0895bm.java io/nn/lpop/C0980ch0.java io/nn/lpop/C1850lu.java io/nn/lpop/Ll0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/startapp/sdk/internal/y8.java com/unity3d/services/core/request/WebRequest.java io/nn/lpop/C0316Kc.java io/nn/lpop/C0688Yl.java io/nn/lpop/C0895bm.java io/nn/lpop/C1850lu.java io/nn/lpop/C2057o50.java io/nn/lpop/Ll0.java io/nn/lpop/Tq0.java
00094	Connect to a URL and read data from it	command network	com/startapp/sdk/internal/hf.java com/startapp/sdk/internal/jd.java com/startapp/sdk/internal/y8.java com/unity3d/services/core/request/WebRequest.java io/nn/lpop/C0895bm.java io/nn/lpop/Ll0.java
00108	Read the input stream from given URL	network command	com/startapp/sdk/internal/jd.java com/startapp/sdk/internal/y8.java com/unity3d/services/core/request/WebRequest.java io/nn/lpop/C0895bm.java io/nn/lpop/Ll0.java io/nn/lpop/Ns0.java io/nn/lpop/Rq0.java
00030	Connect to the remote server through the given URL	network	com/startapp/sdk/internal/q2.java io/nn/lpop/C0688Yl.java io/nn/lpop/C0895bm.java io/nn/lpop/C1128eA.java io/nn/lpop/Ll0.java io/nn/lpop/Tq0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	com/unity3d/services/core/device/Device.java com/unity3d/services/core/misc/Utilities.java io/nn/lpop/C2953xi.java io/nn/lpop/Fs0.java
00085	Get the ISO country code and put it into JSON	collection telephony	com/unity3d/services/core/device/Device.java
00022	Open a file from given absolute path of the file	file	com/unity3d/ads/core/data/repository/AndroidCacheRepository.java com/unity3d/ads/core/domain/AndroidHttpClientProvider.java com/unity3d/ads/core/domain/GetCachedAsset.java com/unity3d/services/core/api/Cache.java com/unity3d/services/core/cache/CacheDirectory.java com/unity3d/services/core/misc/Utilities.java com/unity3d/services/core/properties/SdkProperties.java io/nn/lpop/C0083Bd.java io/nn/lpop/C1838lo.java io/nn/lpop/C1894mQ.java io/nn/lpop/Fe0.java io/nn/lpop/LH.java io/nn/lpop/M50.java io/nn/lpop/OH.java io/nn/lpop/RQ.java
00079	Hide the current app's icon	evasion	io/nn/lpop/LS.java
00078	Get the network operator name	collection telephony	com/startapp/sdk/internal/ci.java com/unity3d/ads/core/data/datasource/AndroidDynamicDeviceInfoDataSource.java
00034	Query the current data network type	collection network	com/startapp/sdk/internal/ie.java com/unity3d/ads/core/data/datasource/AndroidDynamicDeviceInfoDataSource.java

RULE ID	BEHAVIOUR	LABEL	FILES
00132	Query The ISO country code	telephony collection	com/unity3d/ads/core/data/datasource/AndroidDynamicDeviceInfoDataSource.java
00125	Check if the given file path exist	file	com/unity3d/services/core/cache/CacheThreadHandler.java io/nn/lpop/MQ.java
00024	Write file after Base64 decoding	reflection file	com/unity3d/services/core/api/Cache.java io/nn/lpop/AbstractC1070df.java io/nn/lpop/BQ.java io/nn/lpop/C0504Rj.java io/nn/lpop/OH.java
00091	Retrieve data from broadcast	collection	io/nn/lp/service/LoopopService.java io/nn/lpop/C2599tt.java io/nn/lpop/C2853wf.java io/nn/lpop/DQ.java
00005	Get absolute path of file and put it to JSON object	file	com/unity3d/services/core/api/Cache.java com/unity3d/services/core/misc/Utilities.java
00012	Read data and put it into a buffer stream	file	io/nn/lpop/C0616Vr.java
00072	Write HTTP input stream into a file	command network file	com/startapp/sdk/internal/jd.java
00121	Create a directory	file command	io/nn/lpop/MQ.java
00191	Get messages in the SMS inbox	sms	io/nn/lpop/AbstractC3033yb.java io/nn/lpop/K80.java
00104	Check if the given path is directory	file	io/nn/lpop/AbstractC3033yb.java
00056	Modify voice volume	control	io/nn/lpop/UT.java

RULE ID	BEHAVIOUR	LABEL	FILES
00026	Method reflection	reflection	io/nn/lpop/BQ.java
00147	Get the time of current location	collection location	io/nn/lpop/J4.java
00075	Get location of the device	collection location	io/nn/lpop/J4.java
00115	Get last known location of the device	collection location	io/nn/lpop/J4.java
00187	Query a URI and check the result	collection sms calllog calendar	io/nn/lpop/C1373gp0.java
00023	Start another application from current application	reflection control	com/startapp/sdk/internal/gj.java
00028	Read file from assets directory	file	io/nn/lpop/P6.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/963020218535/namespaces/firebase:fetch?key=AIzaSyAh9jkEU0E_UYxH0m_BKAt-uUSTiTPqhb8 is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'cric_api1': 'https://indsp1.site/', 'cric_api2': 'https://cfymarkscanjiostar80.top'}, 'state': 'UPDATE', 'templateVersion': '110'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK
Other Common Permissions	5/44	android.permission.BLUETOOTH, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.c2dm.permission.RECEIVE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.googleadservices.com	ok	**IP:** 142.250.67.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mozilla.org	ok	**IP:** 35.190.14.201 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
support.start.io	ok	**IP:** 216.198.53.11 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
github.com	ok	**IP:** 20.207.73.82 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.cricbuzz.com	ok	**IP:** 23.221.86.37 **Country:** Thailand **Region:** Chachoengsao **City:** Chachoengsao **Latitude:** 13.688200 **Longitude:** 101.071564 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
req.startappservice.com	ok	**IP:** 138.2.84.229 **Country:** United States of America **Region:** California **City:** Belmont **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map
app-measurement.com	ok	**IP:** 172.217.27.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
d2to8y50b3n6dq.cloudfront.net	ok	**IP:** 49.44.79.236 **Country:** India **Region:** Kerala **City:** Kochi **Latitude:** 9.939880 **Longitude:** 76.260223 **View:** Google Map
www.example.com	ok	**IP:** 184.84.232.10 **Country:** India **Region:** Karnataka **City:** Bengaluru **Latitude:** 12.976230 **Longitude:** 77.603287 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 142.250.76.68 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
google.com	ok	**IP:** 142.251.222.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.250.193.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
aomedia.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
adsmetadata.startappservice.com	ok	**IP:** 138.2.84.229 **Country:** United States of America **Region:** California **City:** Belmont **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map
cnn.com	ok	**IP:** 151.101.195.5 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebaseremoteconfigrealtime.googleapis.com	ok	**IP:** 142.250.182.42 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.66.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
default.url	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
d26xw8rp6mlgfg.cloudfront.net	ok	**IP:** 49.44.79.236 **Country:** India **Region:** Kerala **City:** Kochi **Latitude:** 9.939880 **Longitude:** 76.260223 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.183.162 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.18.196 **Country:** Brazil **Region:** Sao Paulo **City:** Sao Paulo **Latitude:** -23.547501 **Longitude:** -46.636108 **View:** Google Map
info.startappservice.com	ok	**IP:** 151.101.39.52 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
schemas.microsoft.com	ok	**IP:** 13.107.246.58 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
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
rtstv.xyz	ok	**IP:** 49.44.79.236 **Country:** India **Region:** Kerala **City:** Kochi **Latitude:** 9.939880 **Longitude:** 76.260223 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
adsmetadata.mobileadexchange.net	ok	**IP:** 138.2.84.229 **Country:** United States of America **Region:** California **City:** Belmont **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.startapp.com	ok	**IP:** 3.81.242.98 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
geoip.api.p3insight.de	ok	**IP:** 49.44.79.236 **Country:** India **Region:** Kerala **City:** Kochi **Latitude:** 9.939880 **Longitude:** 76.260223 **View:** Google Map
scar.unityads.unity3d.com	ok	**IP:** 34.128.182.103 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
drive.google.com	ok	**IP:** 142.250.206.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
amazon.com	ok	**IP:** 98.87.170.71 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
goo.gl	ok	**IP:** 142.251.220.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebaseinstallations.googleapis.com	ok	**IP:** 142.251.221.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
gateway.unityads.unity3d.com	ok	**IP:** 34.149.76.49 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	ok	**IP:** 142.251.221.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
infoevent.startappservice.com	ok	**IP:** 138.2.84.229 **Country:** United States of America **Region:** California **City:** Belmont **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map
dashif.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
plus.google.com	ok	**IP:** 142.250.66.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
funnel-assets.startappservice.com	ok	**IP:** 151.101.39.52 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
0.0.0.0	ok	**IP:** 0.0.0.0 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.77.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
vk.com	ok	**IP:** 87.240.132.67 **Country:** Russian Federation **Region:** Sankt-Peterburg **City:** Saint Petersburg **Latitude:** 59.894440 **Longitude:** 30.264170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
imp.startappservice.com	ok	**IP:** 138.2.84.229 **Country:** United States of America **Region:** California **City:** Belmont **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	io/nn/lpop/BinderC0902bp0.java

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Startapp	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/195
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121

HARDCODED SECRETS

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyAh9jkEU0E_UYxH0m_BKAt-uUSTiTPqhb8"
"google_api_key" : "AIzaSyAh9jkEU0E_UYxH0m_BKAt-uUSTiTPqhb8"
14fd050ed80e4eee66bf5018ad4f44e2
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
2F73797374656D2F6C69622F6C69627265666572656E63652D72696C2E736F
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
49f946663a8deb7054212b8adda248c6
90b2221a199608088559e06f03cd5978
9a04f079-9840-4286-ab92-e65be0885f95
3A757365722F72656C656173652D6B657973
84098ee7ef8622a9defc2ef043cd8930b617b10e-
e2719d58-a985-b3c9-781a-b030af78d30e
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
c103703e120ae8cc73c9248622f3cd1e

SCAN LOGS

Timestamp	Event	Error
2025-11-17 14:10:51	Generating Hashes	OK
2025-11-17 14:10:51	Extracting APK	OK
2025-11-17 14:10:51	Unzipping	OK
2025-11-17 14:10:51	Parsing APK with androguard	OK
2025-11-17 14:10:52	Extracting APK features using aapt/aapt2	OK
2025-11-17 14:10:52	Getting Hardcoded Certificates/Keystores	OK
2025-11-17 14:10:55	Parsing AndroidManifest.xml	OK
2025-11-17 14:10:55	Extracting Manifest Data	OK
2025-11-17 14:10:55	Manifest Analysis Started	OK
2025-11-17 14:10:55	Reading Network Security config from network_security_config.xml	OK

2025-11-17 14:10:55	Parsing Network Security config	OK
2025-11-17 14:10:55	Performing Static Analysis on: CRICFy TV (com.cricfy.tv)	OK
2025-11-17 14:10:56	Fetching Details from Play Store: com.cricfy.tv	OK
2025-11-17 14:10:57	Checking for Malware Permissions	OK
2025-11-17 14:10:57	Fetching icon path	OK
2025-11-17 14:10:57	Library Binary Analysis Started	OK
2025-11-17 14:10:57	Analyzing lib/x86/libgav1JNI.so	OK
2025-11-17 14:10:57	Analyzing lib/x86/libffmpegJNI.so	OK
2025-11-17 14:10:57	Analyzing lib/x86/libnativesdk.so	OK
2025-11-17 14:10:57	Analyzing lib/x86/libtoolChecker.so	OK
2025-11-17 14:10:57	Analyzing lib/armeabi-v7a/libgav1JNI.so	OK

2025-11-17 14:10:57	Analyzing lib/armeabi-v7a/libffmpegJNI.so	OK
2025-11-17 14:10:57	Analyzing lib/armeabi-v7a/libnativesdk.so	OK
2025-11-17 14:10:57	Analyzing lib/armeabi-v7a/libtoolChecker.so	OK
2025-11-17 14:10:57	Analyzing lib/x86_64/libgav1JNI.so	OK
2025-11-17 14:10:57	Analyzing lib/x86_64/libffmpegJNI.so	OK
2025-11-17 14:10:57	Analyzing lib/x86_64/libnativesdk.so	OK
2025-11-17 14:10:57	Analyzing lib/x86_64/libtoolChecker.so	OK
2025-11-17 14:10:57	Analyzing lib/arm64-v8a/libgav1JNI.so	OK
2025-11-17 14:10:57	Analyzing lib/arm64-v8a/libffmpegJNI.so	OK
2025-11-17 14:10:57	Analyzing lib/arm64-v8a/libnativesdk.so	OK
2025-11-17 14:10:57	Analyzing lib/arm64-v8a/libtoolChecker.so	OK

2025-11-17 14:10:57	Analyzing apktool_out/lib/x86/libgav1JNI.so	OK
2025-11-17 14:10:57	Analyzing apktool_out/lib/x86/libffmpegJNI.so	OK
2025-11-17 14:10:57	Analyzing apktool_out/lib/x86/libnativesdk.so	OK
2025-11-17 14:10:57	Analyzing apktool_out/lib/x86/libtoolChecker.so	OK
2025-11-17 14:10:57	Analyzing apktool_out/lib/armeabi-v7a/libgav1JNI.so	OK
2025-11-17 14:10:57	Analyzing apktool_out/lib/armeabi-v7a/libffmpegJNI.so	OK
2025-11-17 14:10:57	Analyzing apktool_out/lib/armeabi-v7a/libnativesdk.so	OK
2025-11-17 14:10:57	Analyzing apktool_out/lib/armeabi-v7a/libtoolChecker.so	OK
2025-11-17 14:10:57	Analyzing apktool_out/lib/x86_64/libgav1JNI.so	OK
2025-11-17 14:10:57	Analyzing apktool_out/lib/x86_64/libffmpegJNI.so	OK
2025-11-17 14:10:57	Analyzing apktool_out/lib/x86_64/libnativesdk.so	OK

2025-11-17 14:10:57	Analyzing apktool_out/lib/x86_64/libtoolChecker.so	OK
2025-11-17 14:10:57	Analyzing apktool_out/lib/arm64-v8a/libgav1JNI.so	OK
2025-11-17 14:10:57	Analyzing apktool_out/lib/arm64-v8a/libffmpegJNI.so	OK
2025-11-17 14:10:58	Analyzing apktool_out/lib/arm64-v8a/libnativesdk.so	OK
2025-11-17 14:10:58	Analyzing apktool_out/lib/arm64-v8a/libtoolChecker.so	OK
2025-11-17 14:10:58	Reading Code Signing Certificate	OK
2025-11-17 14:10:59	Running APKiD 3.0.0	OK
2025-11-17 14:11:04	Detecting Trackers	OK
2025-11-17 14:11:05	Decompiling APK to Java with JADX	OK
2025-11-17 14:11:33	Converting DEX to Smali	OK
2025-11-17 14:11:33	Code Analysis Started on - java_source	OK

2025-11-17 14:11:41	Android SBOM Analysis Completed	OK
2025-11-17 14:11:47	Android SAST Completed	OK
2025-11-17 14:11:47	Android API Analysis Started	OK
2025-11-17 14:11:52	Android API Analysis Completed	OK
2025-11-17 14:11:53	Android Permission Mapping Started	OK
2025-11-17 14:11:59	Android Permission Mapping Completed	OK
2025-11-17 14:11:59	Android Behaviour Analysis Started	OK
2025-11-17 14:12:09	Android Behaviour Analysis Completed	OK
2025-11-17 14:12:09	Extracting Emails and URLs from Source Code	OK
2025-11-17 14:12:13	Email and URL Extraction Completed	OK
2025-11-17 14:12:13	Extracting String data from APK	OK

2025-11-17 14:12:13	Extracting String data from SO	OK
2025-11-17 14:12:13	Extracting String data from Code	OK
2025-11-17 14:12:13	Extracting String values and entropies from Code	OK
2025-11-17 14:12:15	Performing Malware check on extracted domains	OK
2025-11-17 14:12:23	Saving to Database	OK

Report Generated by - MobSF v4.4.3

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.