ANDROID STATIC ANALYSIS REPORT

Wheel With Me (5.9.7.2)

File Name:	Wheel With Me Adapt Fit_5.9.7.2_APKPure.apk
Package Name:	breakthroughapps.com.wheelwithme
Scan Date:	Nov. 29, 2024, 10:15 p.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	7/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
6	28	3	3	2

FILE INFORMATION

File Name: Wheel With Me Adapt Fit_5.9.7.2_APKPure.apk
Size: 70.83MB
MD5: 1584eb41f302ee8aad52b35fa5ae54e4
SHA1: adb7ecc08f20865b3b5474f3e713a15d2233a16e
SHA256: ddf2ea3b8c1be3aff22d21188f91848de0f40cf675a4968bf9bccbfdbbe2c16f

APP INFORMATION

App Name: Wheel With Me
Package Name: breakthroughapps.com.wheelwithme
Main Activity: breakthroughapps.com.partner_platform.MainActivity
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 5.9.7.2
Android Version Code: 18

APP COMPONENTS

Activities: 27
Services: 18
Receivers: 24
Providers: 9
Exported Activities: 5
Exported Services: 3
Exported Receivers: 7
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-03-16 12:33:08+00:00
Valid To: 2052-03-16 12:33:08+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xf01f262e25a6f617eaa43585b1af9ad0225c85cd
Hash Algorithm: sha256
md5: 81adf99ed798d294f1882a8a2e14511f
sha1: d3ab2bb33ca8f5fef085043e6b52b3a4e0ebc8f2
sha256: b7bbe7c1ef2e2210483ee7092452ad35eb0f1cc437374b179bcb7b3818428310
sha512: 1b991dd7ea0d1e5bf54e583b20d4c7d714f5d797194cbf0916107936d004d123a37ad4c7b6937fa811962e5a3c58970b57cc1d4d34b53f06014a70329a063c49
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: acf668d37577d9b165895affd264c37b554a7fc0026a2e229a17e80f7455225f
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.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.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
breakthroughapps.com.wheelwithme.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.

APKID ANALYSIS

FILE	DETAILS

<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.BOARD check
Build.TAGS check
SIM operator check
network operator name check
ro.kernel.qemu check</td></tr>
<tr><td>Obfuscator</td><td>Kiwi encrypter</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.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
possible Build.SERIAL check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.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.TAGS check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
breakthroughapps.com.partner_platform.MainActivity	Schemes: https://, @string/purchasely_prefix://, Hosts: @string/deep_link_prefix, @string/one_link_prefix, ply,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.breakthroughapps.com.wheelwithme,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

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: **16** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 5.1-5.1.1, [minSdk=22]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
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	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.
4	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Service (com.ryanheise.audioservice.AudioService) is not Protected. [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.
6	Broadcast Receiver (com.ryanheise.audioservice.MediaButtonReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	Activity (io.purchasely.purchasely_flutter.PLYProductActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Activity (io.purchasely.purchasely_flutter.PLYSubscriptionsActivity) 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.
10	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.
11	Broadcast Receiver (com.clevertap.android.sdk.pushnotification.fcm.CTFirebaseMessagingReceiver) 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.
12	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.
14	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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.
15	Broadcast Receiver (com.amazon.device.iap.ResponseReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.inapp.purchasing.Permission.NOTIFY [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
16	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.
17	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
18	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

HIGH: **3** | WARNING: **10** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A2/a.java A4/a.java B1/b.java C/c.java C0/a.java C0/c.java C4/h.java C7/d.java E5/e.java F/c.java G6/e.java G6/g.java H6/a.java J7/b.java J9/c.java K2/k.java M1/c.java M4/a.java N2/a.java O/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				O3/C0668u.java P3/h.java P4/d.java Q3/g.java Q4/b.java S/a.java S1/e.java S1/h.java S4/g.java V/c.java V1/A.java V1/C0808f.java V1/O.java V5/w.java W/a.java W0/a.java W0/n.java W0/o.java W0/p.java W1/C0853c.java W1/C0856f.java W1/G.java W1/m.java W4/i.java X/a.java X0/a.java Y0/d.java Y0/e.java Z/A.java Z/C0887e.java Z/m.java Z/v.java Z/w.java Z1/l.java Z3/e.java a1/C0896c.java a1/e.java a2/e.java a2/f.java b6/b.java c1/j.java c1/k.java c2/C1145a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c6/C1169c.java com/amazon/a/a/g/d.java com/amazon/a/a/o/c.java com/amazon/c/a/a/d.java com/amazon/device/drm/LicensingService.java com/amazon/device/drm/a/d/c.java com/amazon/device/iap/PurchasingService.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/BroadcastHandler.java com/amazon/device/simplesignin/SimpleSignInService.java com/amazon/device/simplesignin/a/c/b.java com/appsflyer/appsflyersdk/AppsflyerSdkPlugin.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1qSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1jSDK.java com/appsflyer/internal/AFf1kSDK.java com/appsflyer/internal/AFg1jSDK.java com/bumptech/glide/b.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/h.java com/bumptech/glide/load/engine/i.java com/bumptech/glide/load/engine/j.java com/bumptech/glide/load/engine/v.java com/bumptech/glide/load/resource/bitmap/A.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/c.java com/bumptech/glide/load/resource/bitmap/d.java com/bumptech/glide/load/resource/bitmap/l.java com/bumptech/glide/load/resource/bitmap/m.java com/bumptech/glide/load/resource/bitmap/q.java com/bumptech/glide/load/resource/bitmap/y.java com/clevertap/android/sdk/s.java com/journeyapps/barcodescanner/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/journeyapps/barcodescanner/e.java com/pichillilorenzo/flutter_inappwebview/MyCookieManager.java com/pichillilorenzo/flutter_inappwebview/Util.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview/in_app_browser/InAppBrowserActivity.java com/pichillilorenzo/flutter_inappwebview/in_app_browser/InAppBrowserManager.java com/pichillilorenzo/flutter_inappwebview/webview/JavaScriptBridgeInterface.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/DisplayListenerProxy.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/FlutterWebView.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/InAppWebView.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/InAppWebViewChromeClient.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/InAppWebViewClient.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/InAppWebViewClientCompat.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/InAppWebViewRenderProcessClient.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/InputAwareWebView.java com/revenuecat/purchases/common/DefaultLogHandler.java com/revenuecat/purchases/hybridcommon/CommonKt.java com/revenuecat/purchases/hybridcommon/mappers/PurchasesPeriod.java com/revenuecat/purchases_flutter/PurchasesFlutterPlugin.java com/ryanheise/audioservice/AudioService.java com/ryanheise/audioservice/a.java com/shockwave/pdfium/PdfiumCore.java com/yalantis/ucrop/UCropActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/yalantis/ucrop/view/b.java d1/e.java d1/i.java defpackage/b.java e1/C1798b.java e1/ExecutorServiceC1797a.java e2/f.java e2/i.java e2/l.java e4/C1805b.java e8/C1821b.java f1/C1845c.java f1/C1846d.java f1/C1848f.java f1/s.java f1/t.java g0/InterfaceC1873c.java g4/AbstractC1888a.java g4/C1889b.java g4/e.java g4/h.java g8/C1896a.java h1/AbstractC1934a.java h2/C1937a.java h8/C1949a.java i6/C1988h.java i6/C1992l.java i6/C1995o.java i7/i.java io/flutter/plugins/firebase/crashlytics/n.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundService.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java io/flutter/plugins/firebase/messaging/b.java io/flutter/plugins/firebase/messaging/i.java io/flutter/plugins/googlesignin/b.java io/flutter/plugins/imagepicker/o.java io/flutter/plugins/pathprovider/b.java io/flutter/plugins/sharedpreferences/b.java io/flutter/plugins/urllauncher/d.java io/purchasely/ext/PLYLogger.java io/purchasely/google/Security.java io/purchasely/managers/PLYEventManager$startP

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/purchasely/managers/PLYEventManager$startPeriodicTasks$1.java io/purchasely/managers/PLYEventManager.java io/purchasely/purchasely_flutter/NativeView.java io/purchasely/purchasely_flutter/PurchaselyFlutterPlugin.java io/sentry/C2.java io/sentry/android/core/C2098u.java io/sentry/flutter/SentryFlutterPlugin.java j4/C2216a.java j6/C2218a.java j7/C2220a.java j7/c.java j7/g.java j7/h.java j7/l.java j7/n.java j7/q.java k0/C2229a.java k4/C2251a.java k6/C2256c.java l0/l.java l0/y.java l1/C2313a.java l1/d.java l1/j.java l4/g.java l4/q.java l4/r.java l5/C2344u.java l5/C2345v.java l5/C2349z.java l5/E.java l5/F.java l5/I.java l5/J.java l5/M.java l5/U.java l5/X.java l5/c0.java l6/C2350a.java l6/C2351b.java l6/c.java l6/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				l6/f.java m2/C2369D.java m2/K.java m2/L.java m2/v.java m5/C2406g.java m5/o.java m6/AbstractC2414e.java n1/C2431e.java n1/C2432f.java n1/o.java n1/p.java n1/r.java n1/s.java n7/C2460c.java o0/q.java o1/C2499d.java p/C2523d.java p4/C2552b.java p5/C2560f.java p7/C.java p7/E.java p7/i.java q0/k.java q1/C2585h.java q2/C2588c.java q8/C2604c.java q8/H0.java r1/i.java s/f.java s5/r.java t1/b.java u8/C2984a.java v1/C2998a.java v2/C3003c.java vn/hunghd/flutterdownloader/DownloadWorker.java vn/hunghd/flutterdownloader/a.java w2/C3090q.java w2/C3096w.java w7/AsyncTaskC3133a.java w7/AsyncTaskC3134b.java x4/C3153a.java x7/C3158a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				x7/C3158a.java x7/C3160c.java x7/C3163f.java z2/C3238e.java z2/HandlerC3241h.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	G7/a.java b6/b.java com/amazon/a/a/o/b/a.java com/revenuecat/purchases/common/UtilsKt.java io/sentry/util/s.java v2/C3001a.java
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	B8/e.java B8/h.java V5/H.java W2/u0.java X8/a.java com/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java com/appsflyer/internal/AFb1hSDK.java com/appsflyer/internal/AFc1fSDK.java e4/C1804a.java io/grpc/internal/A0.java io/grpc/internal/C.java io/grpc/internal/E.java io/sentry/metrics/h.java l6/c.java m2/K.java o7/d.java v8/i.java w3/C3101b.java
				N0/m.java P5/a.java R5/b.java R5/s.java S5/f.java Y1/g.java Z0/f.java coil/memory/MemoryCache.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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/appsflyer/appsflyersdk/AppsFlyerConstants.java com/bumptech/glide/load/engine/d.java com/bumptech/glide/load/engine/o.java com/bumptech/glide/load/engine/t.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/models/NotificationDetails.java com/pichillilorenzo/flutter_inappwebview/credential_database/URLCredentialContract.java com/pichillilorenzo/flutter_inappwebview/types/ClientCertResponse.java com/pichillilorenzo/flutter_inappwebview/types/HttpAuthResponse.java com/pichillilorenzo/flutter_inappwebview/types/URLCredential.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/BackgroundAwareCallbackCacheKey.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsSynchronizer.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/common/verification/SigningManager.java com/revenuecat/purchases/strings/ConfigureStrings.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/revenuecat/purchases/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java io/grpc/internal/N0.java io/purchasely/managers/PLYUserAttributeManager.java io/purchasely/models/PLYImage.java r9/C2728g0.java u5/C2942e.java
5	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	A7/b.java C0/a.java ba/a.java io/flutter/plugins/pathprovider/a.java io/flutter/plugins/pathprovider/b.java io/sentry/android/core/S.java m2/K.java vn/hunghd/flutterdownloader/DownloadWorker.java y7/C3216e.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/amazon/device/drm/LicensingService.java com/amazon/device/iap/PurchasingService.java com/clevertap/android/sdk/h.java z3/C3244c.java
7	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	io/purchasely/views/PLYWebViewActivity.java
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	V1/C.java V1/C0803a.java V1/C0810h.java V1/F.java V1/O.java c2/j.java i2/C1967b.java w2/C3096w.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	F0/v.java b6/c.java com/journeyapps/barcodescanner/e.java da/h.java io/flutter/plugins/imagepicker/l.java
10	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	Q5/A1.java Q5/C0699b1.java R2/M.java R2/U.java ca/h.java com/pichillilorenzo/flutter_inappwebview/credential_database/CredentialDatabaseHelper.java h0/C1932a.java p7/i.java vn/hunghd/flutterdownloader/b.java
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	I1/g.java I9/c.java I9/d.java I9/g.java I9/h.java com/amazon/a/a/o/b/a.java vn/hunghd/flutterdownloader/DownloadWorker.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	W4/v.java io/sentry/android/core/internal/util/n.java s5/C2800i.java
13	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFb1vSDK.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	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	W1/C0854d.java e2/l.java y1/C3197a.java
15	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/clevertap/android/sdk/inapp/c.java
16	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/n.java
17	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/clevertap/android/sdk/inbox/f.java io/flutter/plugin/editing/b.java io/flutter/plugin/platform/c.java
18	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	y1/C3197a.java

SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libsentry-android.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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libflutter.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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info 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	armeabi-v7a/libmodpng.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
4	armeabi-v7a/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__strlen_chk', '__vsnprintf_chk', '__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	armeabi-v7a/libmodpdfium.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/libc++_shared.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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi-v7a/libapp.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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info 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
8	armeabi-v7a/libmodft2.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	armeabi-v7a/libjniPdfium.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
10	x86/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	x86/libmodpng.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
12	x86/libsentry.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: ['__strlen_chk', '__vsnprintf_chk', '__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	x86/libmodpdfium.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
14	x86/libc++_shared.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', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	x86/libmodft2.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
16	x86/libjniPdfium.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	arm64-v8a/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	arm64-v8a/libflutter.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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	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', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	arm64-v8a/libmodpng.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: ['__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	arm64-v8a/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__strlen_chk', '__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	arm64-v8a/libmodpdfium.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: ['__strlen_chk', '__snprintf_chk', '__strchr_chk', '__vsnprintf_chk', '__read_chk', '__sprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	arm64-v8a/libc++_shared.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', '__read_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	arm64-v8a/libapp.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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info 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
24	arm64-v8a/libmodft2.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: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	arm64-v8a/libjniPdfium.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
26	x86_64/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	x86_64/libflutter.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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	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', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	x86_64/libmodpng.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: ['__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	x86_64/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__strlen_chk', '__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	x86_64/libmodpdfium.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: ['__strlen_chk', '__snprintf_chk', '__strchr_chk', '__vsnprintf_chk', '__read_chk', '__sprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	x86_64/libc++_shared.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', '__read_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	x86_64/libapp.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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info 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
33	x86_64/libmodft2.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: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	x86_64/libjniPdfium.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
35	armeabi-v7a/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
36	armeabi-v7a/libflutter.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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info 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
37	armeabi-v7a/libmodpng.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
38	armeabi-v7a/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__strlen_chk', '__vsnprintf_chk', '__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
39	armeabi-v7a/libmodpdfium.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
40	armeabi-v7a/libc++_shared.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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
41	armeabi-v7a/libapp.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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info 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
42	armeabi-v7a/libmodft2.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
43	armeabi-v7a/libjniPdfium.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
44	x86/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
45	x86/libmodpng.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
46	x86/libsentry.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: ['__strlen_chk', '__vsnprintf_chk', '__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
47	x86/libmodpdfium.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
48	x86/libc++_shared.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', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
49	x86/libmodft2.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
50	x86/libjniPdfium.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
51	arm64-v8a/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
52	arm64-v8a/libflutter.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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	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', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
53	arm64-v8a/libmodpng.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: ['__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
54	arm64-v8a/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__strlen_chk', '__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
55	arm64-v8a/libmodpdfium.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: ['__strlen_chk', '__snprintf_chk', '__strchr_chk', '__vsnprintf_chk', '__read_chk', '__sprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
56	arm64-v8a/libc++_shared.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', '__read_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
57	arm64-v8a/libapp.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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info 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
58	arm64-v8a/libmodft2.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: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
59	arm64-v8a/libjniPdfium.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
60	x86_64/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
61	x86_64/libflutter.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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	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', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
62	x86_64/libmodpng.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: ['__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
63	x86_64/libsentry.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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: ['__strlen_chk', '__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
64	x86_64/libmodpdfium.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: ['__strlen_chk', '__snprintf_chk', '__strchr_chk', '__vsnprintf_chk', '__read_chk', '__sprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
65	x86_64/libc++_shared.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', '__read_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
66	x86_64/libapp.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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info 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
67	x86_64/libmodft2.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: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
68	x86_64/libjniPdfium.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
00091	Retrieve data from broadcast	collection	com/amazon/device/drm/a/d/c.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/a/c/b.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1jSDK.java com/clevertap/android/sdk/h.java com/clevertap/android/sdk/pushnotification/CTNotificationIntentService.java com/clevertap/android/sdk/pushnotification/fcm/CTFirebaseMessagingReceiver.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/ActionBroadcastReceiver.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview/in_app_browser/InAppBrowserActivity.java io/purchasely/purchasely_flutter/PLYProductActivity.java io/purchasely/views/PLYActivity.java io/purchasely/views/PLYTVLinkActivity.java io/purchasely/views/PLYWebViewActivity.java m2/C2369D.java
			C0/a.java H/l.java M9/w.java O1/b.java S8/g.java S8/i.java T9/k.java W1/C0856f.java X0/a.java b6/c.java ca/f.java com/amazon/c/a/a/c.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1nSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/bumptech/glide/load/a.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview/Util.java com/revenuecat/purchases/common/FileHelper.java e0/c.java e2/l.java f1/C1848f.java f2/j.java i2/C1966a.java io/purchasely/managers/PLYContentIdManager$retrieve$2.java io/purchasely/managers/PLYContentIdManager.java io/purchasely/managers/PLYUserAttributeManager$retrieveAttributes$2.java io/purchasely/managers/PLYUserAttributeManager.java io/purchasely/storage/PLYActiveSubscriptionsStorage$load$2.java io/purchasely/storage/PLYActiveSubscriptionsStorage.java io/purchasely/storage/PLYPurchasesStorage$load$2.java io/purchasely/storage/PLYPurchasesStorage.java io/sentry/C2184w.java io/sentry/Q0.java io/sentry/S0.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/util/e.java o2/k.java p0/C2534i.java s5/C2775A.java t5/C2850d.java x5/e.java x7/C3162e.java z5/C3251a.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/k.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/k.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	b6/c.java com/appsflyer/internal/AFg1nSDK.java f2/j.java i2/C1966a.java o2/k.java t5/C2850d.java z5/C3251a.java
00022	Open a file from given absolute path of the file	file	C0/a.java G0/a.java H/l.java com/amazon/a/a/b/b.java com/appsflyer/internal/AFg1nSDK.java com/journeyapps/barcodescanner/e.java com/zt/shareextend/ShareExtendProvider.java da/h.java e0/C1796a.java h0/C1933b.java io/flutter/plugins/imagepicker/l.java io/flutter/plugins/pathprovider/b.java io/sentry/AbstractC2157p.java io/sentry/C2123f2.java io/sentry/C2184w.java io/sentry/Q0.java io/sentry/S0.java io/sentry/android/core/C2103z.java io/sentry/android/core/S.java io/sentry/android/core/cache/b.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java t5/C2850d.java vn/hunghd/flutterdownloader/a.java y7/C3216e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFg1nSDK.java t5/C2850d.java
00096	Connect to a URL and set request method	command network	N3/s.java Y1/g.java c6/C1169c.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/pichillilorenzo/flutter_inappwebview/Util.java com/revenuecat/purchases/common/HTTPClient.java io/sentry/transport/o.java
00089	Connect to a URL and receive input stream from the server	command network	N3/s.java Y1/g.java c6/C1169c.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/bumptech/glide/load/data/j.java com/revenuecat/purchases/common/HTTPClient.java io/sentry/transport/o.java v2/C3003c.java vn/hunghd/flutterdownloader/DownloadWorker.java x1/C3149e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	N3/s.java Y1/g.java Z3/d.java c6/C1169c.java com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/appsflyer/internal/AFf1oSDK.java com/bumptech/glide/load/data/j.java com/revenuecat/purchases/common/HTTPClient.java io/sentry/transport/o.java vn/hunghd/flutterdownloader/DownloadWorker.java x1/C3149e.java
00036	Get resource file from res/raw directory	reflection	C7/d.java L0/e.java W0/a.java W0/n.java com/amazon/a/a/i/g.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1sSDK.java com/clevertap/android/sdk/h.java com/clevertap/android/sdk/pushnotification/CTNotificationIntentService.java com/clevertap/android/sdk/pushnotification/CTPushNotificationReceiver.java com/clevertap/android/sdk/pushnotification/d.java com/clevertap/android/sdk/pushnotification/e.java com/clevertap/android/sdk/pushnotification/g.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/CustomTabsHelper.java com/ryanheise/audioservice/AudioService.java io/purchasely/common/ContextExtensionsKt.java m2/C2372a.java m2/K.java m2/L.java m2/P.java w1/C3043H.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	A2/a.java C7/d.java E5/e.java I7/b.java T0/a.java W0/a.java W0/n.java W0/p.java Z/g.java com/amazon/a/a/i/a.java com/amazon/a/a/i/g.java com/amazon/device/iap/internal/a/a.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1cSDK.java com/appsflyer/internal/AFc1jSDK.java com/appsflyer/internal/AFf1sSDK.java com/clevertap/android/sdk/InAppNotificationActivity.java com/clevertap/android/sdk/h.java com/clevertap/android/sdk/inapp/a.java com/clevertap/android/sdk/inbox/g.java com/clevertap/android/sdk/pushnotification/CTNotificationIntentService.java com/clevertap/android/sdk/pushnotification/CTPushNotificationReceiver.java com/clevertap/android/sdk/pushnotification/e.java com/clevertap/android/sdk/pushnotification/g.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/ChromeCustomTabsChannelDelegate.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/TrustedWebActivity.java com/pichillilorenzo/flutter_inappwebview/in_app_browser/InAppBrowserManager.java com/ryanheise/audioservice/AudioService.java d8/h.java e7/C1819a.java io/flutter/plugins/imagepicker/l.java io/flutter/plugins/urllauncher/c.java io/purchasely/common/ContextExtensionsKt.java io/purchasely/ext/PLYDeeplinkManager.java io/purchasely/google/GoogleStore.java io/purchasely/purchasely_flutter/PurchaselyFlutterPlugin.java io/purchasely/views/presentation/PLYPresentationView.java

RULE ID	BEHAVIOUR	LABEL	FILES
			l5/P.java m2/C2369D.java m2/C2372a.java m2/K.java m2/L.java m2/P.java w1/C3043H.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1qSDK.java m2/C2369D.java m2/C2372a.java m2/K.java
00003	Put the compressed bitmap data into JSON object	camera	Z1/l.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/InAppWebView.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	I7/b.java T0/a.java W0/a.java W0/n.java W0/p.java com/pichillilorenzo/flutter_inappwebview/in_app_browser/InAppBrowserManager.java io/flutter/plugins/urllauncher/c.java m2/K.java m2/L.java w1/C3043H.java
00012	Read data and put it into a buffer stream	file	C0/a.java W1/C0856f.java com/amazon/c/a/a/c.java e2/l.java io/sentry/C2184w.java io/sentry/Q0.java io/sentry/cache/b.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/util/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	C0/a.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/InAppWebViewChromeClient.java
00015	Put buffer stream (data) to JSON object	file	m2/K.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFh1cSDK.java com/clevertap/android/sdk/o.java m2/K.java
00009	Put data in cursor to JSON object	file	A1/b.java m2/K.java vn/hunghd/flutterdownloader/DownloadWorker.java
00065	Get the country code of the SIM card provider	collection	com/clevertap/android/sdk/o.java
00162	Create InetSocketAddress object and connecting to it	socket	I9/b.java I9/h.java
00163	Create new Socket and connecting to it	socket	I9/b.java I9/h.java
00004	Get filename and put it to JSON object	file collection	f2/C1855f.java o2/C2502c.java s2/C2772a.java
00125	Check if the given file path exist	file	f2/C1855f.java
00202	Make a phone call	control	W0/p.java
00203	Put a phone number into an intent	control	W0/p.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java m2/C2369D.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java m2/C2369D.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java m2/C2369D.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFi1oSDK.java m2/C2369D.java
00187	Query a URI and check the result	collection sms calllog calendar	m2/C2369D.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFi1oSDK.java m2/C2369D.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	a1/C0896c.java com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java m2/C2369D.java vn/hunghd/flutterdownloader/a.java
00030	Connect to the remote server through the given URL	network	N3/s.java com/appsflyer/internal/AFb1uSDK.java com/bumptech/glide/load/data/j.java com/pichillilorenzo/flutter_inappwebview/Util.java io/sentry/transport/o.java vn/hunghd/flutterdownloader/DownloadWorker.java x1/C3149e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/c.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java
00123	Save the response to JSON after connecting to the remote server	network command	com/pichillilorenzo/flutter_inappwebview/Util.java vn/hunghd/flutterdownloader/DownloadWorker.java
00094	Connect to a URL and read data from it	command network	N3/s.java com/pichillilorenzo/flutter_inappwebview/Util.java vn/hunghd/flutterdownloader/DownloadWorker.java w1/C3043H.java w5/C3129a.java
00056	Modify voice volume	control	Z/F.java m7/b.java
00025	Monitor the general action to be performed	reflection	com/appsflyer/internal/AFc1jSDK.java
00072	Write HTTP input stream into a file	command network file	vn/hunghd/flutterdownloader/DownloadWorker.java
00108	Read the input stream from given URL	network command	N3/s.java vn/hunghd/flutterdownloader/DownloadWorker.java
00183	Get current camera parameters and change the setting.	camera	j7/h.java
00126	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	vn/hunghd/flutterdownloader/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00192	Get messages in the SMS inbox	sms	ba/a.java com/appsflyer/internal/AFb1jSDK.java
00034	Query the current data network type	collection network	w1/C3043H.java
00102	Set the phone speaker on	command	m7/b.java
00016	Get location info of the device and put it to JSON object	location collection	O1/a.java
00132	Query The ISO country code	telephony collection	O3/S.java
00114	Create a secure socket connection to the proxy address	network command	D9/f.java
00054	Install other APKs from file	reflection	ca/f.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/683804635522/namespaces/firebase:fetch?key=AIzaSyDE57iPO-KSoiyCyV8tBLowo9199fZq7cE. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.CAMERA
Other Common Permissions	5/44	android.permission.FOREGROUND_SERVICE, android.permission.READ_CALENDAR, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
api-paywalls.revenuecat.com	ok	**IP:** 34.198.224.250 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.css	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
www.interpretation	ok	No Geolocation information available.
www.manifestations	ok	No Geolocation information available.
www.c	ok	No Geolocation information available.
www.a	ok	No Geolocation information available.
www.googleorganizationautocompleterequirementsconservative	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
facebook.com	ok	**IP:** 157.240.205.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase-settings.crashlytics.com	ok	**IP:** 216.58.211.227 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
docs.google.com	ok	**IP:** 216.58.211.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
accounts.google.com	ok	**IP:** 64.233.162.84 **Country:** Brazil **Region:** Sao Paulo **City:** Sao Paulo **Latitude:** -23.547501 **Longitude:** -46.636108 **View:** Google Map
api.revenuecat.com	ok	**IP:** 34.198.224.250 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sars.s	ok	No Geolocation information available.
flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
journeyapps.com	ok	**IP:** 108.156.22.7 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
api-staging.purchasely.io	ok	**IP:** 104.18.20.12 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
errors.rev.cat	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
sconversions.s	ok	No Geolocation information available.
api.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
svalidate.s	ok	No Geolocation information available.
api-diagnostics.revenuecat.com	ok	**IP:** 3.211.205.154 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
paywall.purchasely.io	ok	**IP:** 104.18.20.12 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
docs.revenuecat.com	ok	**IP:** 3.164.206.60 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
graph.s	ok	No Geolocation information available.
tracking-staging.purchasely.io	ok	**IP:** 104.18.21.12 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.vimeo.com	ok	**IP:** 162.159.138.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebasestorage.googleapis.com	ok	**IP:** 216.58.209.170 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
.css	ok	No Geolocation information available.
scdn-stestsettings.s	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
.jpg	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
developer.android.com	ok	**IP:** 216.58.210.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
www.years	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developers.facebook.com	ok	**IP:** 157.240.205.1 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
firebase.google.com	ok	**IP:** 216.58.211.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.world	ok	**IP:** 75.2.38.108 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
sinapps.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 216.58.211.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dashif.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
www.recent	ok	No Geolocation information available.
o1107917.ingest.sentry.io	ok	**IP:** 34.120.195.249 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.example.com	ok	**IP:** 93.184.215.14 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.hortcut	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
static.wizrocket.com	ok	**IP:** 18.165.140.92 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.maryochsner.com	ok	**IP:** 198.185.159.145 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.734699 **Longitude:** -74.005898 **View:** Google Map
www.language	ok	No Geolocation information available.
www.in	ok	No Geolocation information available.
graph-video.s	ok	No Geolocation information available.
.facebook.com	ok	No Geolocation information available.
www.style	ok	**IP:** 75.2.38.108 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
www.wencodeuricomponent	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.risktabsprev10pxrise25pxblueding300ballfordearnwildbox.fairlackverspairjunetechifpickevil	ok	No Geolocation information available.
tracking.purchasely.io	ok	**IP:** 104.18.21.12 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.purchasely.io	ok	**IP:** 104.18.20.12 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
issuetracker.google.com	ok	**IP:** 216.58.211.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
simpression.s	ok	No Geolocation information available.
www.breakthroughapps.io	ok	**IP:** 198.49.23.145 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.734699 **Longitude:** -74.005898 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sapp.s	ok	No Geolocation information available.
www.purchasely.com	ok	**IP:** 199.60.103.29 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.370129 **Longitude:** -71.086304 **View:** Google Map
sviap.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
www.text-decoration	ok	No Geolocation information available.
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
sattr.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
paywall-staging.purchasely.io	ok	**IP:** 104.18.20.12 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.icon	ok	No Geolocation information available.
www.amazon.com	ok	**IP:** 18.165.130.223 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

EMAILS

EMAIL	FILE
help@purchasely.com	io/purchasely/managers/PLYUserManager$startUserTransfer$1.java
entitlementinfoimpl@1698195990.fromjson	

EMAIL	FILE
entitlementinfoimpl@1698193996.fromjson 418c854c985437a11640@o1107917.ingest 26055323eb4749895ee0@o1107917.ingest 4a66a7f74c8e84d15ab0@o1107917.ingest 41f8a78b18d2f6b89a79@o1107917.ingest _nativesocket@14069316.normal 47ce8f59c94bcd0280c1@o1107917.ingest 4e6f8a42f23d14ba516a@o1107917.ingest entitlementinfosimpl@1957312893.fromjson 4fa892bb0fb3ae742b66@o1107917.ingest _growablelist@0150898._ofefficie _hashcollisionnode@255137193.fromcollis _growablelist@0150898._ofgrowabl 4c13a4bad14c02ab32bd@o1107917.ingest 414c8a25408911929482@o1107917.ingest pricingphaseimpl@1969464389.fromjson 409c972eb50202be85ec@o1107917.ingest _typeerror@0150898._create dofferingcontextimpl@1966456690.fromjson 479e95e39d6cd3dfa59b@o1107917.ingest _bytebuffer@7027147._new _planguidecategory@1224064120.fromjson _assetmanifestbin@37287047.fromstanda 996a351dfb1f0e288bc9@o1107917.ingest support@breakthroughapps.zendesk _timer@1026248._internal periodimpl@1965419416.fromjson 4ccf95aba327e23b91cb@o1107917.ingest _growablelist@0150898._literal 4fb58210bb8a1c41df93@o1107917.ingest _filestream@14069316.forstdin _growablelist@0150898.of 469cb24fb8811bcecfca@o1107917.ingest storetransactionimpl@1958339892.fromjson 48dfbaeb72921bc0992c@o1107917.ingest offeringsimpl@1648143891.fromjson _posemediamodel@1198159854.fromjson _uri@0150898.notsimple _questionoption@1236361616.fromjson _compressednode@255137193.single 4156a2aa3985efa08eae@o1107917.ingest 4b51a1b08ea01bd838e9@o1107917.ingest 4267b34ac65e4706aa5e@o1107917.ingest 42118afb00705ab402e7@o1107917.ingest	

EMAIL	FILE
[illegible]@o1107917.ingest 45579b93c46db1feebe4@o1107917.ingest 4ce08569c3f6992e60c8@o1107917.ingest 4a5283fe4a1efc4c1b5f@o1107917.ingest _imagefilter@15065589.composed 4d1aac86ca61c15ac343@o1107917.ingest _pointerpanzoomdata@585213599.fromupdate _list@0150898.of _dailycontent@1209229446.fromjson _nativesocket@14069316.pipe _quotemodel@1134017879.fromjson _list@0150898.generate _socket@14069316._readpipe 9a1277c785cf90b732d1@o1107917.ingest 4b638a5f44f8437596eb@o1107917.ingest 4fde83f4d892a0f1b357@o1107917.ingest 45949dfc96b8107d8750@o1107917.ingest 4d9f9e25ff10a6afbbb3@o1107917.ingest 489cae9377a1b6e63ba1@o1107917.ingest _colorfilter@15065589.srgbtoline _growablelist@0150898._literal2 4ced90466ee8b483c1d2@o1107917.ingest _uri@0150898.file _growablelist@0150898._literal7 1bc3d6ca6f57544935e9@o1107917.ingest _timer@1026248.periodic 4360b7c6e05d7cd2a22a@o1107917.ingest 4c6598a3558dfceed35d@o1107917.ingest 4edca50d692b3dd2f788@o1107917.ingest customerinfoimpl@1822493635.fromjson 442e9fd90a4363a3611c@o1107917.ingest 4e0ea841381139d75122@o1107917.ingest 45e6814c4aa61370c463@o1107917.ingest _growablelist@0150898._literal1 4d0ea7767210356d4c7e@o1107917.ingest 44a382684148eefbee5c@o1107917.ingest _rawsocket@14069316._readpipe _imagefilter@15065589.fromcolorf 4d5db1d7d787d843e9f8@o1107917.ingest _uri@0150898.directory _receiveportimpl@1026248.fromrawrec _growablelist@0150898.generate 4dd19d8f6796c9cf092e@o1107917.ingest _internetaddress@14069316.fixed	apktool_out/lib/armeabi-v7a/libapp.so

EMAIL	FILE
_cookie@13463476.fromsetcoo 402ba9d58a86d0325849@o1107917.ingest 47d28e424ff743803b51@o1107917.ingest authenticationscheme@13463476.fromstring _httpparser@13463476.requestpar 407b911b5b802c38f616@o1107917.ingest 432abfbe3437a0577f2f@o1107917.ingest d2e4178ad8de8a7f1fa0@o1107917.ingest sessionfeedbackmodel@1214291106.fromjson 4b74a941a5ca8ffa6b81@o1107917.ingest _list@0150898._ofgrowabl _colorfilter@15065589.lineartosr packageimpl@1649483590.fromjson ntroductorypriceimpl@1962433645.fromjson _future@4048458.immediate 4cc7aa5bcaa4bf87d33b@o1107917.ingest _resourcelistmodel@1228243210.fromjson 4def9fd3c1bf000763e6@o1107917.ingest 413aaf5c7aff0ec0310b@o1107917.ingest _file@14069316.fromrawpat targetingcontextimpl@1967465736.fromjson 4449ae9318cb6da29b11@o1107917.ingest support@breakthroughapps.io _growablelist@0150898._literal6 4a94896b69e5b160b4e9@o1107917.ingest ngstreamsubscription@4048458.zoned 4e30a5608694381e2140@o1107917.ingest _growablelist@0150898._literal3 _colorfilter@15065589.mode _list@0150898._ofarray _growablelist@0150898._literal5 4f29abd47a40bfd0983b@o1107917.ingest 4dac8b38d0d9f272b967@o1107917.ingest _double@0150898.fromintege f5bf2ed77e3423abd5db@o1107917.ingest _invocationmirror@0150898._withtype 4ec1be07746efb6a205b@o1107917.ingest offeringimpl@1964197943.fromjson _future@4048458.zonevalue _growablelist@0150898.withcapaci _recipecontentmodel@1226008229.fromjson _growablelist@0150898._ofarray imagefilter@15065589.blur	

EMAIL	FILE
4a7e8c1fe83b6ff1a123@o1107917.ingest _list@0150898.empty 47a4bc21f1b3de2921ff@o1107917.ingest 7cb2a798b556c77805a1@o1107917.ingest 493281f15a31e4bfe49a@o1107917.ingest 45b8835a11064bad0b0e@o1107917.ingest 3b235c9d068ebbf8e260@o1107917.ingest 431785eee658a72051aa@o1107917.ingest _link@14069316.fromrawpat 484ab3ee6002779d883d@o1107917.ingest 49128c1438d6247a2ee7@o1107917.ingest _growablelist@0150898._ofother _uri@0150898.https _future@4048458.immediatee _list@0150898._ofefficie _httpparser@13463476.responsepa 17a3810769a36f1687e7@o1107917.ingest priceimpl@1968459876.fromjson _growablelist@0150898._literal8 49d0b9a7605cb4103d1f@o1107917.ingest storeproductimpl@1650169359.fromjson _recipecategory@1196063334.fromjson eproductdiscountimpl@1972036751.fromjson 452b97d809fd1ddf9b3d@o1107917.ingest _assertionerror@0150898._create _list@0150898._ofother _nativesocket@14069316.listen _growablelist@0150898._literal4 _appuser@1202499523.fromjson	
appro@openssl.org	apktool_out/lib/arm64-v8a/libflutter.so
4b74a941a5ca8ffa6b81@o1107917.ingest	apktool_out/lib/arm64-v8a/libapp.so
appro@openssl.org	apktool_out/lib/x86_64/libflutter.so
4b74a941a5ca8ffa6b81@o1107917.ingest	apktool_out/lib/x86_64/libapp.so
entitlementinfoimpl@1698195990.fromjson 418c854c985437a11640@o1107917.ingest 26055323eb4749895ee0@o1107917.ingest	

EMAIL	FILE
4a66a7f74c8e84d15ab0@o1107917.ingest	
4118a78b18d2f6b89a79@o1107917.ingest	
_nativesocket@14069316.normal	
47ce8f59c94bcd0280c1@o1107917.ingest	
4e6f8a42f23d14ba516a@o1107917.ingest	
entitlementinfosimpl@1957312893.fromjson	
4fa892bb0fb3ae742b66@o1107917.ingest	
_growablelist@0150898._ofefficie	
_hashcollisionnode@255137193.fromcollis	
_growablelist@0150898._ofgrowabl	
4c13a4bad14c02ab32bd@o1107917.ingest	
414c8a25408911929482@o1107917.ingest	
pricingphaseimpl@1969464389.fromjson	
409c972eb50202be85ec@o1107917.ingest	
_typeerror@0150898._create	
dofferingcontextimpl@1966456690.fromjson	
479e95e39d6cd3dfa59b@o1107917.ingest	
_bytebuffer@7027147._new	
_planguidecategory@1224064120.fromjson	
_assetmanifestbin@37287047.fromstanda	
996a351dfb1f0e288bc9@o1107917.ingest	
support@breakthroughapps.zendesk	
_timer@1026248._internal	
periodimpl@1965419416.fromjson	
4ccf95aba327e23b91cb@o1107917.ingest	
_growablelist@0150898._literal	
4fb58210bb8a1c41df93@o1107917.ingest	
_filestream@14069316.forstdin	
_growablelist@0150898.of	
469cb24fb8811bcecfca@o1107917.ingest	
storetransactionimpl@1958339892.fromjson	
48dfbaeb72921bc0992c@o1107917.ingest	
offeringsimpl@1648143891.fromjson	
_posemediamodel@1198159854.fromjson	
_uri@0150898.notsimple	
_questionoption@1236361616.fromjson	
_compressednode@255137193.single	
4156a2aa3985efa08eae@o1107917.ingest	
4b51a1b08ea01bd838e9@o1107917.ingest	
4267b34ac65e4706aa5e@o1107917.ingest	
42118afb00705ab402e7@o1107917.ingest	
45579b93c46db1feebe4@o1107917.ingest	
4ce08569c3f6992e60c8@o1107917.ingest	

EMAIL	FILE
4a5283fe4a1efc4c1b5f@o1107917.ingest _imagefilter@15065589.composed 4d1aac86ca61c15ac343@o1107917.ingest _pointerpanzoomdata@585213599.fromupdate _list@0150898.of _dailycontent@1209229446.fromjson _nativesocket@14069316.pipe _quotemodel@1134017879.fromjson _list@0150898.generate _socket@14069316._readpipe 9a1277c785cf90b732d1@o1107917.ingest 4b638a5f44f8437596eb@o1107917.ingest 4fde83f4d892a0f1b357@o1107917.ingest 45949dfc96b8107d8750@o1107917.ingest 4d9f9e25ff10a6afbbb3@o1107917.ingest 489cae9377a1b6e63ba1@o1107917.ingest _colorfilter@15065589.srgbtoline _growablelist@0150898._literal2 4ced90466ee8b483c1d2@o1107917.ingest _uri@0150898.file _growablelist@0150898._literal7 1bc3d6ca6f57544935e9@o1107917.ingest _timer@1026248.periodic 4360b7c6e05d7cd2a22a@o1107917.ingest 4c6598a3558dfceed35d@o1107917.ingest 4edca50d692b3dd2f788@o1107917.ingest customerinfoimpl@1822493635.fromjson 442e9fd90a4363a3611c@o1107917.ingest 4e0ea841381139d75122@o1107917.ingest 45e6814c4aa61370c463@o1107917.ingest _growablelist@0150898._literal1 4d0ea7767210356d4c7e@o1107917.ingest 44a382684148eefbee5c@o1107917.ingest _rawsocket@14069316._readpipe _imagefilter@15065589.fromcolorf 4d5db1d7d787d843e9f8@o1107917.ingest _uri@0150898.directory _receiveportimpl@1026248.fromrawrec _growablelist@0150898.generate 4dd19d8f6796c9cf092e@o1107917.ingest _internetaddress@14069316.fixed _cookie@13463476.fromsetcoo 402ba9d58a86d0325849@o1107917.ingest	lib/armeabi-v7a/libapp.so

EMAIL	FILE
47d28e424ff743803b51@o1107917.ingest	
authenticationscheme@13463476.fromstring	
_httpparser@13463476.requestpar	
407b911b5b802c38f616@o1107917.ingest	
432abfbe3437a0577f2f@o1107917.ingest	
d2e4178ad8de8a7f1fa0@o1107917.ingest	
sessionfeedbackmodel@1214291106.fromjson	
4b74a941a5ca8ffa6b81@o1107917.ingest	
_list@0150898._ofgrowabl	
_colorfilter@15065589.lineartosr	
packageimpl@1649483590.fromjson	
ntroductorypriceimpl@1962433645.fromjson	
_future@4048458.immediate	
4cc7aa5bcaa4bf87d33b@o1107917.ingest	
_resourcelistmodel@1228243210.fromjson	
4def9fd3c1bf000763e6@o1107917.ingest	
413aaf5c7aff0ec0310b@o1107917.ingest	
_file@14069316.fromrawpat	
targetingcontextimpl@1967465736.fromjson	
4449ae9318cb6da29b11@o1107917.ingest	
support@breakthroughapps.io	
_growablelist@0150898._literal6	
4a94896b69e5b160b4e9@o1107917.ingest	
ngstreamsubscription@4048458.zoned	
4e30a5608694381e2140@o1107917.ingest	
_growablelist@0150898._literal3	
_colorfilter@15065589.mode	
_list@0150898._ofarray	
_growablelist@0150898._literal5	
4f29abd47a40bfd0983b@o1107917.ingest	
4dac8b38d0d9f272b967@o1107917.ingest	
_double@0150898.fromintege	
f5bf2ed77e3423abd5db@o1107917.ingest	
_invocationmirror@0150898._withtype	
4ec1be07746efb6a205b@o1107917.ingest	
offeringimpl@1964197943.fromjson	
_future@4048458.zonevalue	
_growablelist@0150898.withcapaci	
_recipecontentmodel@1226008229.fromjson	
_growablelist@0150898._ofarray	
_imagefilter@15065589.blur	
4a7e8c1fe83b6ff1a123@o1107917.ingest	
_list@0150898.empty	

EMAIL	FILE
47a4bc21f1b3de2921ff@o1107917.ingest 7cb2a798b556c77805a1@o1107917.ingest 493281f15a31e4bfe49a@o1107917.ingest 45b8835a11064bad0b0e@o1107917.ingest 3b235c9d068ebbf8e260@o1107917.ingest 431785eee658a72051aa@o1107917.ingest _link@14069316.fromrawpat 484ab3ee6002779d883d@o1107917.ingest 49128c1438d6247a2ee7@o1107917.ingest _growablelist@0150898._ofother _uri@0150898.https _future@4048458.immediatee _list@0150898._ofefficie _httpparser@13463476.responsepa 17a3810769a36f1687e7@o1107917.ingest priceimpl@1968459876.fromjson _growablelist@0150898._literal8 49d0b9a7605cb4103d1f@o1107917.ingest storeproductimpl@1650169359.fromjson _recipecategory@1196063334.fromjson eproductdiscountimpl@1972036751.fromjson 452b97d809fd1ddf9b3d@o1107917.ingest _assertionerror@0150898._create _list@0150898._ofother _nativesocket@14069316.listen _growablelist@0150898._literal4 _appuser@1202499523.fromjson	
appro@openssl.org	lib/arm64-v8a/libflutter.so
4b74a941a5ca8ffa6b81@o1107917.ingest	lib/arm64-v8a/libapp.so
appro@openssl.org	lib/x86_64/libflutter.so
4b74a941a5ca8ffa6b81@o1107917.ingest	lib/x86_64/libapp.so

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
CleverTap	Location, Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/174
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b>□□□□□□□□□□□□□□□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b>□□□□□□□□□□□□"
"library_zxingandroidembedded_author" : "JourneyApps"
"google_crash_reporting_api_key" : "AIzaSyDE57iPO-KSoiyCyV8tBLowo9199fZq7cE"
"google_api_key" : "AIzaSyDE57iPO-KSoiyCyV8tBLowo9199fZq7cE"

POSSIBLE SECRETS
470fa2b4ae81cd56ecbcda9735803434cec591fa
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
115792089210356248762697446949407573530086143415290314195533631308867097853951
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
115792089210356248762697446949407573529996955224135760342422259061068512044369
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
c103703e120ae8cc73c9248622f3cd1e
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
49f946663a8deb7054212b8adda248c6
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3

POSSIBLE SECRETS
9b8f518b086098de3d77736f9458a3d2f6f95a37
e2719d58-a985-b3c9-781a-b030af78d30e
cc2751449a350f668590264ed76692694a80308a
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
c56fb7d591ba6704df047fd98f535372fea00211
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
df6b721c8b4d3b6eb44c861d4415007e5a35fc95

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
9a04f079-9840-4286-ab92-e65be0885f95

PLAYSTORE INFORMATION

Title: Wheel With Me Adapt Fit

Score: 4.029412 **Installs:** 1,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** [breakthroughapps.com.wheelwithme]

Developer Details: Breakthrough Apps Inc, Breakthrough+Apps+Inc, 1390 Market St Apt 2523, San Francisco, California, None, bappsinc@gmail.com,

Release Date: Apr 25, 2022 **Privacy Policy:** Privacy link

Description:

Wheel With Me Adapt Fit is the Fitness App for wheelchair users created by Jesi Stracham & Nikki Walsh. Jesi & Nikki were tired of having to piece together workouts from nondisabled trainers, and came together to create a better fitness resource for seated workouts! This app provides customized programs and workouts to help you push past your limits to achieve independence as a wheelchair user. Wheel With Me Adapt Fit was designed to be convenient and easy to use. We focus solely on the fitness experience, so you have confidence when you work out. We are excited to work together on improving and evolving our app with our Wheel With Me Adapt Fit Community. The app was built by wheelchair users for wheelchair users. The Wheel With Me Adapt Fit App features -Strength Programs -Functional Mobility -Bands -Floor workouts -Cardio -Strength -Daily Inspiration -Private Facebook Group -Community -& so much more! Improve your fitness and support your independence from anywhere with the Wheel With Me Fit App! Terms of this product: http://www.breakthroughapps.io/terms Privacy Policy: http://www.breakthroughapps.io/privacypolicy

SCAN LOGS

Timestamp	Event	Error

2024-11-29 22:15:05	Generating Hashes	OK
2024-11-29 22:15:06	Extracting APK	OK
2024-11-29 22:15:06	Unzipping	OK
2024-11-29 22:15:08	Parsing APK with androguard	OK
2024-11-29 22:15:09	Extracting APK features using aapt/aapt2	OK
2024-11-29 22:15:09	Getting Hardcoded Certificates/Keystores	OK
2024-11-29 22:15:15	Parsing AndroidManifest.xml	OK
2024-11-29 22:15:15	Extracting Manifest Data	OK
2024-11-29 22:15:15	Manifest Analysis Started	OK
2024-11-29 22:15:15	Performing Static Analysis on: Wheel With Me (breakthroughapps.com.wheelwithme)	OK
2024-11-29 22:15:15	Fetching Details from Play Store: breakthroughapps.com.wheelwithme	OK

2024-11-29 22:15:16	Checking for Malware Permissions	OK
2024-11-29 22:15:16	Fetching icon path	OK
2024-11-29 22:15:16	Library Binary Analysis Started	OK
2024-11-29 22:15:16	Analyzing apktool_out/lib/armeabi-v7a/libsentry-android.so	OK
2024-11-29 22:15:16	Analyzing apktool_out/lib/armeabi-v7a/libflutter.so	OK
2024-11-29 22:15:16	Analyzing apktool_out/lib/armeabi-v7a/libmodpng.so	OK
2024-11-29 22:15:16	Analyzing apktool_out/lib/armeabi-v7a/libsentry.so	OK
2024-11-29 22:15:16	Analyzing apktool_out/lib/armeabi-v7a/libmodpdfium.so	OK
2024-11-29 22:15:16	Analyzing apktool_out/lib/armeabi-v7a/libc++_shared.so	OK
2024-11-29 22:15:16	Analyzing apktool_out/lib/armeabi-v7a/libapp.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/armeabi-v7a/libmodft2.so	OK

2024-11-29 22:15:17	Analyzing apktool_out/lib/armeabi-v7a/libjniPdfium.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/x86/libsentry-android.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/x86/libmodpng.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/x86/libsentry.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/x86/libmodpdfium.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/x86/libc++_shared.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/x86/libmodft2.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/x86/libjniPdfium.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/arm64-v8a/libsentry-android.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/arm64-v8a/libflutter.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/arm64-v8a/libmodpng.so	OK

2024-11-29 22:15:17	Analyzing apktool_out/lib/arm64-v8a/libsentry.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/arm64-v8a/libmodpdfium.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/arm64-v8a/libc++_shared.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/arm64-v8a/libapp.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/arm64-v8a/libmodft2.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/arm64-v8a/libjniPdfium.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/x86_64/libsentry-android.so	OK
2024-11-29 22:15:17	Analyzing apktool_out/lib/x86_64/libflutter.so	OK
2024-11-29 22:15:18	Analyzing apktool_out/lib/x86_64/libmodpng.so	OK
2024-11-29 22:15:18	Analyzing apktool_out/lib/x86_64/libsentry.so	OK
2024-11-29 22:15:18	Analyzing apktool_out/lib/x86_64/libmodpdfium.so	OK

2024-11-29 22:15:18	Analyzing apktool_out/lib/x86_64/libc++_shared.so	OK
2024-11-29 22:15:18	Analyzing apktool_out/lib/x86_64/libapp.so	OK
2024-11-29 22:15:18	Analyzing apktool_out/lib/x86_64/libmodft2.so	OK
2024-11-29 22:15:18	Analyzing apktool_out/lib/x86_64/libjniPdfium.so	OK
2024-11-29 22:15:18	Analyzing lib/armeabi-v7a/libsentry-android.so	OK
2024-11-29 22:15:18	Analyzing lib/armeabi-v7a/libflutter.so	OK
2024-11-29 22:15:18	Analyzing lib/armeabi-v7a/libmodpng.so	OK
2024-11-29 22:15:18	Analyzing lib/armeabi-v7a/libsentry.so	OK
2024-11-29 22:15:18	Analyzing lib/armeabi-v7a/libmodpdfium.so	OK
2024-11-29 22:15:18	Analyzing lib/armeabi-v7a/libc++_shared.so	OK
2024-11-29 22:15:18	Analyzing lib/armeabi-v7a/libapp.so	OK

2024-11-29 22:15:19	Analyzing lib/armeabi-v7a/libmodft2.so	OK
2024-11-29 22:15:19	Analyzing lib/armeabi-v7a/libjniPdfium.so	OK
2024-11-29 22:15:19	Analyzing lib/x86/libsentry-android.so	OK
2024-11-29 22:15:19	Analyzing lib/x86/libmodpng.so	OK
2024-11-29 22:15:19	Analyzing lib/x86/libsentry.so	OK
2024-11-29 22:15:19	Analyzing lib/x86/libmodpdfium.so	OK
2024-11-29 22:15:19	Analyzing lib/x86/libc++_shared.so	OK
2024-11-29 22:15:19	Analyzing lib/x86/libmodft2.so	OK
2024-11-29 22:15:19	Analyzing lib/x86/libjniPdfium.so	OK
2024-11-29 22:15:19	Analyzing lib/arm64-v8a/libsentry-android.so	OK
2024-11-29 22:15:19	Analyzing lib/arm64-v8a/libflutter.so	OK

2024-11-29 22:15:19	Analyzing lib/arm64-v8a/libmodpng.so	OK
2024-11-29 22:15:19	Analyzing lib/arm64-v8a/libsentry.so	OK
2024-11-29 22:15:20	Analyzing lib/arm64-v8a/libmodpdfium.so	OK
2024-11-29 22:15:20	Analyzing lib/arm64-v8a/libc++_shared.so	OK
2024-11-29 22:15:20	Analyzing lib/arm64-v8a/libapp.so	OK
2024-11-29 22:15:20	Analyzing lib/arm64-v8a/libmodft2.so	OK
2024-11-29 22:15:20	Analyzing lib/arm64-v8a/libjniPdfium.so	OK
2024-11-29 22:15:20	Analyzing lib/x86_64/libsentry-android.so	OK
2024-11-29 22:15:20	Analyzing lib/x86_64/libflutter.so	OK
2024-11-29 22:15:20	Analyzing lib/x86_64/libmodpng.so	OK
2024-11-29 22:15:20	Analyzing lib/x86_64/libsentry.so	OK

2024-11-29 22:15:20	Analyzing lib/x86_64/libmodpdfium.so	OK
2024-11-29 22:15:20	Analyzing lib/x86_64/libc++_shared.so	OK
2024-11-29 22:15:20	Analyzing lib/x86_64/libapp.so	OK
2024-11-29 22:15:21	Analyzing lib/x86_64/libmodft2.so	OK
2024-11-29 22:15:21	Analyzing lib/x86_64/libjniPdfium.so	OK
2024-11-29 22:15:21	Reading Code Signing Certificate	OK
2024-11-29 22:15:24	Running APKiD 2.1.5	OK
2024-11-29 22:15:34	Detecting Trackers	OK
2024-11-29 22:15:40	Decompiling APK to Java with JADX	OK
2024-11-29 22:16:42	Converting DEX to Smali	OK
2024-11-29 22:16:42	Code Analysis Started on - java_source	OK

2024-11-29 22:16:48	Android SBOM Analysis Completed	OK
2024-11-29 22:17:02	Android SAST Completed	OK
2024-11-29 22:17:02	Android API Analysis Started	OK
2024-11-29 22:17:09	Android API Analysis Completed	OK
2024-11-29 22:17:10	Android Permission Mapping Started	OK
2024-11-29 22:17:48	Android Permission Mapping Completed	OK
2024-11-29 22:17:49	Android Behaviour Analysis Started	OK
2024-11-29 22:17:58	Android Behaviour Analysis Completed	OK
2024-11-29 22:17:58	Extracting Emails and URLs from Source Code	OK
2024-11-29 22:18:05	Email and URL Extraction Completed	OK
2024-11-29 22:18:05	Extracting String data from APK	OK

2024-11-29 22:18:06	Extracting String data from SO	OK
2024-11-29 22:18:08	Extracting String data from Code	OK
2024-11-29 22:18:08	Extracting String values and entropies from Code	OK
2024-11-29 22:18:15	Performing Malware check on extracted domains	OK
2024-11-29 22:18:19	Saving to Database	OK

Report Generated by - MobSF v4.2.8

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.