



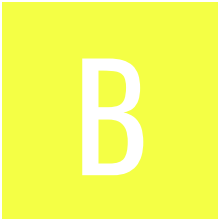
ANDROID STATIC ANALYSIS REPORT








 Nursegrid (8.2.2)

File Name:

com.hct2.nursegrid.android.web_2024112200.apk

| | |
|---------------------|---|
| Package Name: | com.hct2.nursegrid.android.web |
| Scan Date: | Aug. 29, 2025, 11:35 p.m. |
| App Security Score: | 48/100 (MEDIUM RISK) |
| Grade: |  |
| Trackers Detection: | 9/432 |

FINDINGS SEVERITY

|  HIGH |  MEDIUM |  INFO |  SECURE |  HOTSPOT |
|--|--|--|--|---|
| 4 | 24 | 4 | 2 | 1 |

FILE INFORMATION

File Name: com.hct2.nursegrid.android.web_2024112200.apk

Size: 46.73MB

MD5: 9a71227aae797616a515912312909cb0

SHA1: 39a6a4f15fe1ce48fc9ea05edc6b91837e0be92b

SHA256: 73db26cb91881abe3f37ad0c427de071657adcb2b983625093d64dc1035b07aa

APP INFORMATION

App Name: Nursegrid

Package Name: com.hct2.nursegrid.android.web

Main Activity: com.hct2.nursegrid.android.web.ui.carousel.CarouselActivity

Target SDK: 34

Min SDK: 26

Max SDK:

Android Version Name: 8.2.2

Android Version Code: 2024112200

APP COMPONENTS

Activities: 100

Services: 15

Receivers: 14
Providers: 5
Exported Activities: 7
Exported Services: 2
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=Oregon, L=Portland, O=HCT2 Co., CN=Joshua Ellington
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-08-10 07:48:54+00:00
Valid To: 2040-08-03 07:48:54+00:00
Issuer: C=US, ST=Oregon, L=Portland, O=HCT2 Co., CN=Joshua Ellington
Serial Number: 0x55c85766
Hash Algorithm: sha1
md5: f3704dcdbd259bab24ff0a5f1c031ffcd
sha1: 4668904e2d524bdd676665dc2326c9f2948191a2
sha256: 0f096cc8e40d5c8e062cf97f942a4b09a98cd7b4617ed2962d0302b947ead83c
sha512: ac0c8ffb6d31d5d041bd7e5ab867b7b24c6ec9d044418bb2cb96201352cf40d67b4d1e8a6b5b625f8ea8bf81abc68de1e32b73f2fedb498e07aa31fdf4f519ab
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 4670aae884dc3444d485741e50e41d1a0ee07c49b5065b865d8629dfead81ef3
Found 1 unique certificates

APPLICATION PERMISSIONS

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|--------|---------------------|---|
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|-----------|---------------------------------------|---|
| android.permission.ACCESS_WIFI_STATE | normal | view Wi-Fi status | Allows an application to view the information about the status of Wi-Fi. |
| android.permission.CHANGE_NETWORK_STATE | normal | change network connectivity | Allows applications to change network connectivity state. |
| android.permission.CAMERA | dangerous | take pictures and videos | Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time. |
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. |
| 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.WAKE_LOCK | normal | prevent phone from sleeping | Allows an application to prevent the phone from going to sleep. |
| android.permission.READ_EXTERNAL_STORAGE | dangerous | read external storage contents | Allows an application to read from external storage. |
| 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.GET_ACCOUNTS | dangerous | list accounts | Allows access to the list of accounts in the Accounts Service. |
| android.permission.READ_PROFILE | dangerous | read the user's personal profile data | Allows an application to read the user's personal profile data. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|-----------|---|--|
| android.permission.READ_CONTACTS | dangerous | read contact data | Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people. |
| 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.ACCESS_COARSE_LOCATION | dangerous | coarse (network-based) location | Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are. |
| android.permission.ACCESS_FINE_LOCATION | dangerous | fine (GPS) location | Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power. |
| android.permission.READ_PHONE_STATE | dangerous | read phone state and identity | Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on. |
| android.permission.SCHEDULE_EXACT_ALARM | normal | permits exact alarm scheduling for background work. | Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work. |
| android.permission.VIBRATE | normal | control vibrator | Allows the application to control the vibrator. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|-----------|--------------------------------------|---|
| android.permission.POST_NOTIFICATIONS | dangerous | allows an app to post notifications. | Allows an app to post notifications |
| com.google.android.c2dm.permission.RECEIVE | normal | recieve push notifications | Allows an application to receive push notifications from cloud. |
| com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE | normal | permission defined by google | A custom permission defined by Google. |
| com.hct2.nursegrid.android.web.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | unknown | Unknown permission | Unknown permission from android reference |

APKID ANALYSIS

| FILE | DETAILS | |
|-------------|--------------|--|
| classes.dex | FINDINGS | DETAILS |
| | Anti-VM Code | Build.FINGERPRINT check Build.MANUFACTURER check network operator name check |
| | Compiler | r8 without marker (suspicious) |

| FILE | DETAILS | |
|--------------|--------------|--|
| classes2.dex | FINDINGS | DETAILS |
| | Anti-VM Code | Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check ro.hardware check ro.kernel.qemu check possible VM check |
| | Compiler | r8 without marker (suspicious) |
| classes3.dex | FINDINGS | DETAILS |
| | Anti-VM Code | Build.MANUFACTURER check network operator name check |
| | Compiler | r8 without marker (suspicious) |

| FILE | DETAILS | |
|--------------|-----------------|--|
| classes4.dex | FINDINGS | DETAILS |
| | Anti-VM Code | Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible VM check |
| | Anti Debug Code | Debug.isDebuggerConnected() check |
| | Compiler | r8 without marker (suspicious) |
| | | |
| classes5.dex | FINDINGS | DETAILS |
| | Compiler | r8 without marker (suspicious) |

BROWSABLE ACTIVITIES

| ACTIVITY | INTENT |
|---|---|
| com.hct2.nursegrid.android.web.ui.calendar.CalendarActivity | Schemes: nursegrid://, Hosts: @string/uri_open_shifts, |
| com.hct2.nursegrid.android.web.ui.add_edit_shift.AddEditShiftActivity | Schemes: nursegrid://, Hosts: @string/uri_add_shifts, |
| com.facebook.CustomTabActivity | Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.hct2.nursegrid.android.web, |

| ACTIVITY | INTENT |
|--|---|
| com.hct2.nursegrid.android.web.ui.carousel.CarouselActivity | Schemes: https://, Hosts: nursegrid.onelink.me, Path Prefixes: /zdVY, |
| com.hct2.nursegrid.android.web.ui.add_worksite.AddWorksiteActivity | Schemes: nursegrid://, Hosts: @string/uri_add_worksite, |

NETWORK SECURITY

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

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

| TITLE | SEVERITY | DESCRIPTION |
|--|----------|--|
| Signed Application | info | Application is signed with a code signing certificate |
| Certificate algorithm vulnerable to hash collision | high | Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. |

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 16 | INFO: 0 | SUPPRESSED: 0

| NO | ISSUE | SEVERITY | DESCRIPTION |
|----|-------|----------|-------------|
|----|-------|----------|-------------|

| NO | ISSUE | SEVERITY | DESCRIPTION |
|----|--|----------|--|
| 1 | App can be installed on a vulnerable Android version Android 8.0, minSdk=26] | warning | This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates. |
| 2 | 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 | Activity (com.hct2.nursegrid.android.web.ui.calendar.CalendarActivity) is not Protected. [android:exported=true] | warning | An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. |
| 4 | Service (com.hct2.nursegrid.android.web.data.remote.WatchListenerService) 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. |
| 5 | Activity (com.hct2.nursegrid.android.web.ui.add_edit_shift.AddEditShiftActivity) is not Protected. [android:exported=true] | warning | An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. |
| 6 | Activity (com.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. |
| 7 | Activity (com.hct2.nursegrid.android.web.ui.worksites_list.WorksitesListActivity) 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. |
| 8 | Activity (com.hct2.nursegrid.android.web.ui.personal_calendar.PersonalCalendarsActivity) 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. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|----|--|----------|---|
| 9 | Activity (com.hct2.nursegrid.android.web.ui.shift_reflections.ShiftReflectionsLogActivity) 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.hct2.nursegrid.android.web.notifications.DailySummaryBroadcastReceiver) 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. |
| 11 | Broadcast Receiver (com.hct2.nursegrid.android.web.notifications.AlarmReceiver) is not Protected. [android:exported=true] | warning | A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. |
| 12 | Broadcast Receiver (com.hct2.nursegrid.android.web.notifications.ShiftReflectionAlarmReceiver) 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. |
| 13 | 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. |
| 14 | TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity) | warning | If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|----|---|----------|--|
| 15 | 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. |
| 16 | Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true] | warning | An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. |
| 17 | Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true] | warning | A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission. |

</> CODE ANALYSIS

HIGH: 1 | WARNING: 7 | INFO: 3 | SECURE: 1 | SUPPRESSED: 0

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|--|
| | | | | A0/g.java A1/f.java A2/e.java G0/E.java G0/d0.java M1/a.java M3/c.java O0/a.java O0/b.java P2/a.java P2/b.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|---|
| | | | | <p> R2/b.java P2/d.java Q2/b.java Q2/d.java Q2/h.java Q2/j.java R3/a.java T0/b.java T0/d.java T1/M.java T1/o.java W0/c.java W0/d.java X1/b.java Y0/a.java Y1/a.java Z0/c.java a/AbstractC0161a.java a1/AsyncTaskC0168a.java a2/AbstractC0172c.java a2/m.java b0/AbstractC0463c.java butterknife/ButterKnife.java butterknife/internal/a.java c/C0483a.java com/appsflyer/AFLogger.java com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFa1bSDK.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1eSDK.java com/appsflyer/internal/AFc1hSDK.java com/appsflyer/internal/AFc1mSDK.java com/appsflyer/internal/AFc1nSDK.java com/appsflyer/internal/AFc1xSDK.java com/appsflyer/internal/AFd1eSDK.java com/appsflyer/internal/AFd1gSDK.java com/appsflyer/internal/AFd1kSDK.java com/appsflyer/internal/AFd1tSDK.java com/appsflyer/internal/AFd1uSDK.java com/appsflyer/internal/AFd1vSDK.java com/appsflyer/internal/AFd1wSDK.java com/appsflyer/internal/AFd1zSDK.java com/appsflyer/share/CrossPromotionHelper.java com/appsflyer/share/LinkGenerator.java com/braze/support/BrazeLogger.java </p> |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|---|
| | | | | com/bumptech/glide/Glide.java com/bumptech/glide/disklruCache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/d.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/model/g.java com/bumptech/glide/load/resource/b.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java |

| 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/bumptechnology/manager/DefaultConnectivityMonitorFactory.java com/bumptechnology/manager/RequestManagerFragment.java com/bumptechnology/manager/RequestManagerRetriever.java com/bumptechnology/manager/RequestTracker.java com/bumptechnology/manager/SupportRequestManagerFragment.java com/bumptechnology/manager/a.java com/bumptechnology/manager/b.java com/bumptechnology/module/ManifestParser.java com/bumptechnology/request/SingleRequest.java com/bumptechnology/request/target/a.java com/bumptechnology/request/target/b.java com/bumptechnology/request/target/d.java com/bumptechnology/signature/ApplicationVersionSignature.java com/bumptechnology/util/ContentLengthInputStream.java com/bumptechnology/util/pool/d.java com/github/barteksc/pdfviewer/PDFView.java com/hct2/nursegrid/android/web/data/model/Requirement.java com/hct2/nursegrid/android/web/data/remote/NGDataManager.java com/hct2/nursegrid/android/web/data/remote/NetworkConnectionInterceptor.java com/hct2/nursegrid/android/web/data/room_database/AppDatabase.java com/hct2/nursegrid/android/web/notifications/AlarmReceiver.java com/hct2/nursegrid/android/web/notifications/GcmPubNubSubscriber.java com/hct2/nursegrid/android/web/notifications/NGGcmIntentService.java com/hct2/nursegrid/android/web/notifications/NotificationScheduler.java com/hct2/nursegrid/android/web/notifications/NurseGridApplication.java com/hct2/nursegrid/android/web/notifications/ShareIntentReceiver.java com/hct2/nursegrid/android/web/notifications/ShiftReflectionAlarmReceiver.java com/hct2/nursegrid/android/web/ui/base/BaseActivity.java com/hct2/nursegrid/android/web/ui/braze/NursegridContentCardAdapter.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|---|
| | | | | com/hct2/nursegrid/android/web/ui/calendar/list_view/CalendarListFragment.java com/hct2/nursegrid/android/web/ui/calendar/list_view/CalendarListViewModel.java com/hct2/nursegrid/android/web/ui/calendar_component/SimpleMonthView.java com/hct2/nursegrid/android/web/ui/inbox/InboxTabActivity.java com/hct2/nursegrid/android/web/ui/inbox/InboxUpdatesAdapter.java com/hct2/nursegrid/android/web/ui/inbox/UpdatesTabFragment.java com/hct2/nursegrid/android/web/ui/inbox/customviews/CustomExpandableTextView.java com/hct2/nursegrid/android/web/ui/landing/HStreamSignupActivity.java com/hct2/nursegrid/android/web/ui/landing/LandingActivity.java com/hct2/nursegrid/android/web/ui/landing/s_s_o/SSOActivity.java com/hct2/nursegrid/android/web/ui/landing/sign_in/email_password_input/EmailPasswordInputFragment\$activateUserEventCall\$1.java com/hct2/nursegrid/android/web/ui/landing/sign_in/email_password_input/EmailPasswordViewModel.java com/hct2/nursegrid/android/web/ui/messages_tab/conversation/ConversationFragment.java com/hct2/nursegrid/android/web/ui/messages_tab/message_inbox/MessagingActivity.java com/hct2/nursegrid/android/web/ui/messages_tab/pubnub_api_controller/PubNubDataTask.java com/hct2/nursegrid/android/web/ui/my_account/MyAccountFragment.java com/hct2/nursegrid/android/web/ui/my_profile/MyProfileActivity.java com/hct2/nursegrid/android/web/ui/my_profile/portfolios/qualifications/CredentialsTabActivity.java com/hct2/nursegrid/android/web/ui/notification_options/AlarmReceiverActivity.java com/hct2/nursegrid/android/web/ui/notification_options/reminder_times/ReminderTimesViewModel.java com/hct2/nursegrid/android/web/ui/reusable_components/colleagues/header_colleagues_view/HeaderColleaguesAdapter.java com/hct2/nursegrid/android/web/ui/reusable_components/fa |

| NO | ISSUE | SEVERITY | STANDARDS | <div> <div> cility/FacilitySearchFragment.java</div> <div>FILES</div> <div>com/hct2/nursegrid/android/web/ui/reusable_components/facility/search_by_location/PlacesAutoCompleteAdapter.java</div> <div>com/hct2/nursegrid/android/web/ui/swap_giveaway/swap_giveaway_details/give_away/CreateGiveAwayFragment.java</div> <div>com/hct2/nursegrid/android/web/util/AlarmNotificationHelper.java</div> <div>com/hct2/nursegrid/android/web/util/AnalyticsUtils.java</div> <div>com/hct2/nursegrid/android/web/util/AppLifecycleListener\$onStart\$1.java</div> <div>com/hct2/nursegrid/android/web/util/AppLifecycleListener.java</div> <div>com/hct2/nursegrid/android/web/util/CalendarUtils.java</div> <div>com/hct2/nursegrid/android/web/util/ErrorUtils.java</div> <div>com/hct2/nursegrid/android/web/util/MessageAES256EncryptDecrypt.java</div> <div>com/intercom/twig/Twig.java</div> <div>com/mixpanel/android/mpmetrics/MPConfig.java</div> <div>com/mixpanel/android/mpmetrics/MixpanelAPI.java</div> <div>com/mixpanel/android/mpmetrics/ResourceReader.java</div> <div>com/mixpanel/android/mpmetrics/a.java</div> <div>com/mixpanel/android/mpmetrics/c.java</div> <div>com/mixpanel/android/util/HttpService.java</div> <div>com/mixpanel/android/util/MPLLog.java</div> <div>com/shockwave/pdfium/PdfiumCore.java</div> <div>com/wdullaer/materialdatetimepicker/date/DayPickerView.java</div> <div>com/wdullaer/materialdatetimepicker/time/AmPmCirclesView.java</div> <div>com/wdullaer/materialdatetimepicker/time/CircleView.java</div> <div>com/wdullaer/materialdatetimepicker/time/RadialPickerLayout.java</div> <div>com/wdullaer/materialdatetimepicker/time/RadialSelectorView.java</div> <div>com/wdullaer/materialdatetimepicker/time/RadialTextView.java</div> <div>com/wdullaer/materialdatetimepicker/time/TimePickerDialog.java</div> <div>com/wdullaer/materialdatetimepicker/time/g.java</div> <div>g/c.java</div> <div>i2/C0869a.java</div> <div>io/embrace/android/embracesdk/logging/AndroidLoggingAction.java</div> <div>io/embrace/android/embracesdk/logging/ReportingLoggerAction.java</div> <div>k/a.java</div> </div> |
|----|-------|----------|-----------|--|
|----|-------|----------|-----------|--|

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|--|----------|---|---|
| | | | | k/h.java l/p.java l/u.java l/w.java l3/RunnableC1167B.java m/l.java n2/RunnableC1289a.java n3/BinderC1290a.java n3/HandlerC1292c.java o3/H.java o3/s0.java o3/t0.java o3/x0.java org/slf4j/helpers/Util.java p0/C1366d.java p0/f.java p0/h.java r0/AbstractC1455f.java r0/r.java r0/t.java rx/plugins/RxJavaHooks.java u2/l.java w0/AbstractC1629c.java x4/AbstractC1704d.java x4/HandlerC1707g.java x4/i.java x4/j.java x4/k.java x4/l.java x4/o.java x4/p.java x4/r.java |
| 2 | 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 | X5/l.java Z0/c.java Z5/n.java coil/graphics/ImageDecoderDecoder.java coil/graphics/VideoFrameDecoder.java com/hct2/nursegrid/android/web/util/BitmapUtils.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|---|----------|--|--|
| 3 | The App uses an insecure Random Number Generator. | warning | CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6 | M5/AbstractC0142h.java R3/a.java b5/EnumC0477a.java bo/app/e20.java c6/C0517a.java c6/C0518b.java com/appsflyer/internal/AFa1ySDK.java com/braze/support/IntentUtils.java com/pubnub/api/vendor/Crypto.java io/embrace/android/embracesdk/anr/ndk/EmbraceNativeThreadSamplerService.java io/opentelemetry/sdk/internal/RandomSupplier.java io/opentelemetry/sdk/metrics/internal/exemplar/ExemplarReservoir.java r5/f.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 | T1/C0153f.java T1/D.java T1/I.java X4/f.java coil/fetch/VideoFrameFetcher.java coil/graphics/GifDecoder.java coil/graphics/ImageDecoderDecoder.java coil/graphics/VideoFrameDecoder.java coil/request/ImageRequest.java coil/request/Parameters.java com/braze/Constants.java com/braze/configuration/BrazeConfig.java com/braze/models/inappmessage/InAppMessageHtml.java com/braze/support/StringUtils.java com/bumptech/glide/load/Option.java com/hct2/nursegrid/android/web/BuildConfig.java com/hct2/nursegrid/android/web/Constants.java com/hct2/nursegrid/android/web/data/model/ColleagueShiftDetail.java com/hct2/nursegrid/android/web/ui/braze/ContentCardsFragment.java com/hct2/nursegrid/android/web/ui/calendar/list_view/CalendarListFragment.java com/hct2/nursegrid/android/web/ui/calendar/tabs/calendar_fragments/my_events/MyEventsCalendarFragment.java com/hct2/nursegrid/android/web/ui/calendar/tabs/calendar_fragments/my_swaps/SwapsCalendarFragment.java com/hct2/nursegrid/android/web/ui/calendar/tabs/calendar_fragments/open_shifts/OpenShiftsCalendarFragment.java com/hct2/nursegrid/android/web/ui/inbox/UpdatesTabFragment.java com/hct2/nursegrid/android/web/util/NGSharedPreferencesHelper.java io/embrace/android/embracesdk/capture/crumbs/PushNotificationCaptureService.java io/embrace/android/embracesdk/payload/UserInfo.java io/embrace/android/embracesdk/prefs/EmbracePreferencesService.java p/C1340C.java rx/internal/schedulers/NewThreadWorker.java z/P0.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|--|----------|--|--|
| 5 | App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database. | warning | CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality | A1/c.java G2/c.java H2/g.java H2/h.java H2/j.java H2/n.java e1/C0768b.java g1/C0809i.java l2/C1164c.java l3/U.java l3/V.java x4/j.java x4/k.java |
| 6 | App can write to App Directory. Sensitive Information should be encrypted. | info | CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14 | bo/app/af0.java bo/app/dm.java bo/app/fe0.java bo/app/g50.java bo/app/gx.java bo/app/id0.java bo/app/m30.java bo/app/nr.java bo/app/oc.java bo/app/pw.java bo/app/q.java bo/app/q50.java bo/app/qp.java bo/app/v70.java bo/app/vt.java bo/app/xb0.java bo/app/yp.java bo/app/ys.java bo/app/zp.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/location/GooglePlayLocationUtils.java com/braze/managers/BrazeGeofenceManager.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|--|----------|---|---|
| 7 | MD5 is a weak hash known to have hash collisions. | warning | CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4 | com/appsflyer/internal/AFb1rSDK.java com/braze/support/StringUtils.java com/pubnub/api/vendor/Crypto.java io/embrace/android/embracesdk/capture/metadata/EmbraceMetadataService.java |
| 8 | SHA-1 is a weak hash known to have hash collisions. | warning | CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4 | com/appsflyer/internal/AFb1rSDK.java com/pubnub/api/vendor/FileEncryptionUtil.java |
| 9 | 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 | k/f.java |
| 10 | The file or SharedPreferences 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/AFa1aSDK.java |
| 11 | App can read/write to External Storage. Any App can read data written to External Storage. | warning | CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2 | com/hct2/nursegrid/android/web/util/BitmapUtils.java z0/f.java |
| 12 | This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. | secure | OWASP MASVS: MSTG-NETWORK-4 | com/hct2/nursegrid/android/web/data/remote/NGApiService.java com/pubnub/api/managers/RetrofitManager.java |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------------|---|--|---|--|---|---|--|---|
| 1 | arm64-v8a/libmodpng.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['__strlen_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

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

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------------|---|--|---|--|---|---|--|---|
| 3 | arm64-v8a/libmodpdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['_strlen_chk', '_snprintf_chk', '_strchr_chk', '_vsnprintf_chk', '_read_chk', '_sprintf_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--------------------------------|---|--|---|--|---|---|---|---|
| 4 | arm64-v8a/libembrace-native.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['_vsprintf_chk', '__memmove_chk', '__strchr_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------------|---|--|---|--|---|---|---|---|
| 5 | arm64-v8a/libmodft2.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--------------------------------------|---|--|---|--|---|---|--|---|
| 6 | arm64-v8a/libpl_droidsonroids_gif.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------|---|--|---|--|---|---|--|---|
| 7 | x86_64/libmodpng.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['__strlen_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------------|---|--|---|--|---|---|--|---|
| 8 | x86_64/libjniPdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------------|---|--|---|--|---|---|--|---|
| 9 | x86_64/libmodpdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['_strlen_chk', '_snprintf_chk', '_strchr_chk', '_vsnprintf_chk', '_read_chk', '_sprintf_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------------|---|--|---|--|---|---|---|---|
| 10 | x86_64/libembrace-native.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__read_chk', '__memmove_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------|---|--|---|--|---|---|---|---|
| 11 | x86_64/libmodft2.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------------------|---|--|---|--|---|---|--|---|
| 12 | x86_64/libpl_droidsonroids_gif.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--------------------------|---|--|---|--|---|---|--|---|
| 13 | armeabi-v7a/libmodpng.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------------|---|--|---|--|---|---|--|---|
| 14 | armeabi-v7a/libjniPdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------------|---|--|---|--|---|---|--|---|
| 15 | armeabi-v7a/libmodpdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|----------------------------------|---|--|---|--|---|---|--|---|
| 16 | armeabi-v7a/libembrace-native.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__read_chk', '__memcpy_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--------------------------|---|--|---|--|---|---|--|---|
| 17 | armeabi-v7a/libmodft2.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--|---|--|---|--|---|---|--|---|
| 18 | armeabi-v7a/libpl_droidsonroids_gif.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|----------------------|---|--|---|--|---|---|--|---|
| 19 | armeabi/libmodpng.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-------------------------|---|--|---|--|---|---|--|---|
| 20 | armeabi/libjniPdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-------------------------|---|--|---|--|---|---|--|---|
| 21 | armeabi/libmodpdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|----------------------|---|--|---|--|---|---|--|---|
| 22 | armeabi/libmodft2.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------------------------|---|--|---|--|---|---|--|---|
| 23 | armeabi/libpl_droidsonroids_gif.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------|---|--|---|--|---|---|--|---|
| 24 | x86/libmodpng.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------|---|--|---|--|---|---|--|---|
| 25 | x86/libjniPdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------|---|--|---|--|---|---|--|---|
| 26 | x86/libmodpdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--------------------------|---|--|---|--|---|---|--|---|
| 27 | x86/libembrace-native.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__read_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------|---|--|---|--|---|---|--|---|
| 28 | x86/libmodft2.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--------------------------------|---|--|---|--|---|---|--|---|
| 29 | x86/libpl_droidsonroids_gif.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-------------------|---|--|---|--|---|---|--|---|
| 30 | mips/libmodpng.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|----------------------|---|--|---|--|---|---|--|---|
| 31 | mips/libjniPdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|----------------------|---|--|---|--|---|---|--|---|
| 32 | mips/libmodpdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-------------------|---|--|---|--|---|---|--|---|
| 33 | mips/libmodft2.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------------------|---|--|---|--|---|---|--|---|
| 34 | mips/libpl_droidsonroids_gif.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------------------|---|--|---|--|---|---|--|---|
| 35 | mips64/libpl_droidsonroids_gif.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------------|---|--|---|--|---|---|--|---|
| 36 | arm64-v8a/libmodpng.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['__strlen_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------------|---|--|---|--|---|---|--|---|
| 37 | arm64-v8a/libjniPdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------------|---|--|---|--|---|---|--|---|
| 38 | arm64-v8a/libmodpdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['_strlen_chk', '_snprintf_chk', '_strchr_chk', '_vsnprintf_chk', '_read_chk', '_sprintf_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--------------------------------|---|--|---|--|---|---|---|---|
| 39 | arm64-v8a/libembrace-native.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['_vsprintf_chk', '__memmove_chk', '__strchr_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------------|---|--|---|--|---|---|---|---|
| 40 | arm64-v8a/libmodft2.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--------------------------------------|---|--|---|--|---|---|--|---|
| 41 | arm64-v8a/libpl_droidsonroids_gif.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------|---|--|---|--|---|---|--|---|
| 42 | x86_64/libmodpng.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['__strlen_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------------|---|--|---|--|---|---|--|---|
| 43 | x86_64/libjniPdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------------|---|--|---|--|---|---|--|---|
| 44 | x86_64/libmodpdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['_strlen_chk', '_snprintf_chk', '_strchr_chk', '_vsnprintf_chk', '_read_chk', '_sprintf_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------------|---|--|---|--|---|---|---|---|
| 45 | x86_64/libembrace-native.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__read_chk', '__memmove_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------|---|--|---|--|---|---|---|---|
| 46 | x86_64/libmodft2.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['__strcat_chk', '__strlen_chk', '__strrchr_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------------------|---|--|---|--|---|---|--|---|
| 47 | x86_64/libpl_droidsonroids_gif.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--------------------------|---|--|---|--|---|---|--|---|
| 48 | armeabi-v7a/libmodpng.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------------|---|--|---|--|---|---|--|---|
| 49 | armeabi-v7a/libjniPdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------------|---|--|---|--|---|---|--|---|
| 50 | armeabi-v7a/libmodpdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|----------------------------------|---|--|---|--|---|---|--|---|
| 51 | armeabi-v7a/libembrace-native.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__read_chk', '__memcpy_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--------------------------|---|--|---|--|---|---|--|---|
| 52 | armeabi-v7a/libmodft2.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--|---|--|---|--|---|---|--|---|
| 53 | armeabi-v7a/libpl_droidsonroids_gif.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|----------------------|---|--|---|--|---|---|--|---|
| 54 | armeabi/libmodpng.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-------------------------|---|--|---|--|---|---|--|---|
| 55 | armeabi/libjniPdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-------------------------|---|--|---|--|---|---|--|---|
| 56 | armeabi/libmodpdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|----------------------|---|--|---|--|---|---|--|---|
| 57 | armeabi/libmodft2.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------------------------|---|--|---|--|---|---|--|---|
| 58 | armeabi/libpl_droidsonroids_gif.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------|---|--|---|--|---|---|--|---|
| 59 | x86/libmodpng.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------|---|--|---|--|---|---|--|---|
| 60 | x86/libjniPdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------|---|--|---|--|---|---|--|---|
| 61 | x86/libmodpdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--------------------------|---|--|---|--|---|---|--|---|
| 62 | x86/libembrace-native.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__strchr_chk', '__strlen_chk', '__vsprintf_chk', '__memcpy_chk', '__read_chk']</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|------------------|---|--|---|--|---|---|--|---|
| 63 | x86/libmodft2.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|--------------------------------|---|--|---|--|---|---|--|---|
| 64 | x86/libpl_droidsonroids_gif.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-------------------|---|--|---|--|---|---|--|---|
| 65 | mips/libmodpng.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|----------------------|---|--|---|--|---|---|--|---|
| 66 | mips/libjniPdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>False high</p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|----------------------|---|--|---|--|---|---|--|---|
| 67 | mips/libmodpdfium.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-------------------|---|--|---|--|---|---|--|---|
| 68 | mips/libmodft2.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|---------------------------------|---|--|---|--|---|---|--|---|
| 69 | mips/libpl_droidsonroids_gif.so | <p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO) info</p> <p>The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.</p> | <p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p> | <p>Full RELRO info</p> <p>This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.</p> | <p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None info</p> <p>The binary does not have RUNPATH set.</p> | <p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p> | <p>True info</p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT | NX | PIE | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|----|-----------------------------------|---|---|---|---|---|---|--|---|
| 70 | mips64/libpl_droidsonroids_gif.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 |
|---------|--|-------|--|
| 00022 | Open a file from given absolute path of the file | file | Z0/c.java bo/app/da.java bo/app/ea.java bo/app/eb0.java bo/app/hg0.java bo/app/wc.java bo/app/zn.java coil/util/Utils.java com/appsflyer/internal/AFa1aSDK.java com/braze/d0.java com/braze/support/BrazelImageUtils.java com/braze/support/WebContentUtils.java com/fasterxml/jackson/databind/ser/std/FileSerializer.java io/embrace/android/embracesdk/ndk/EmbraceNdkService.java io/embrace/android/embracesdk/ndk/EmbraceNdkServiceRepository.java io/embrace/android/embracesdk/samples/AutomaticVerificationChecker.java pl/droidsonroids/gif/GifInfoHandle.java pl/droidsonroids/gif/n.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|---|---------|--|
| 00063 | Implicit intent(view a web page, make a phone call, etc.) | control | com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFc1fSDK.java com/braze/Braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/inappmessage/views/InAppMessageHtmlBaseView.java com/braze/ui/support/UriUtils.java com/hct2/nursegrid/android/web/notifications/DailySummaryBroadcastReceiver.java com/hct2/nursegrid/android/web/ui/base/BaseActivity.java com/hct2/nursegrid/android/web/ui/calendar/CalendarActivity.java com/hct2/nursegrid/android/web/ui/carousel/CarouselActivity.java com/hct2/nursegrid/android/web/ui/jobs/job_details/JobDetailsActivity.java com/hct2/nursegrid/android/web/ui/landing/HStreamSignupActivity.java com/hct2/nursegrid/android/web/ui/landing/LandingActivity.java com/hct2/nursegrid/android/web/ui/my_profile/portfolios/certifications/add_certification/AddCertificationActivity.java com/hct2/nursegrid/android/web/ui/my_profile/portfolios/certifications/certification_details/CertificationDetailsFragment.java com/hct2/nursegrid/android/web/ui/my_profile/portfolios/licenses/add_license/AddLicenseActivity.java com/hct2/nursegrid/android/web/ui/my_profile/portfolios/licenses/license_details/LicenseDetailsFragment.java com/hct2/nursegrid/android/web/ui/my_profile/portfolios/qualifications/qualification_details/QualificationsDetailsFragment.java com/hct2/nursegrid/android/web/ui/staff_pool_details/StaffPoolDetailsActivity.java com/hct2/nursegrid/android/web/ui/worksite_detail/WorksiteDetailFragment.java com/hct2/nursegrid/android/web/util/DialogBuilder.java io/embrace/android/embracesdk/EmbraceAutomaticVerification.java u2/o.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|--|------------|--|
| 00091 | Retrieve data from broadcast | collection | com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFa1uSDK.java com/braze/push/BrazeNotificationUtils.java com/hct2/nursegrid/android/web/ui/base/BaseActivity.java com/hct2/nursegrid/android/web/ui/my_profile/MyProfileActivity.java com/hct2/nursegrid/android/web/ui/my_profile/portfolios/file_attachment/PortfolioFileAttachmentFragment.java com/hct2/nursegrid/android/web/ui/notification_options/AlarmReceiverActivity.java com/hct2/nursegrid/android/web/ui/reusable_components/colleagues/scheduled_unscheduled_colleagues_fragment/ColleagueTabActivity.java io/embrace/android/embracesdk/capture/crumbs/PushNotificationCaptureService.java |
| 00036 | Get resource file from res/raw directory | reflection | coil/map/ResourceIntMapper.java com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFb1oSDK.java com/appsflyer/internal/AFe1kSDK.java com/appsflyer/internal/AFe1mSDK.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java com/hct2/nursegrid/android/web/ui/my_profile/portfolios/certifications/add_certification/AddCertificationActivity.java com/hct2/nursegrid/android/web/ui/my_profile/portfolios/licenses/add_license/AddLicenseActivity.java com/hct2/nursegrid/android/web/ui/my_profile/portfolios/licenses/license_details/LicenseDetailsFragment.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|---|-----------------|---|
| 00013 | Read file and put it into a stream | file | Q1/c.java X5/j.java X5/l.java a/AbstractC0161a.java a2/m.java b1/g.java bo/app/ca0.java bo/app/fq.java com/braze/support/BrazelImageUtils.java com/braze/support/WebContentUtils.java com/bumptechnology/glide/disklru/DiskLruCache.java com/bumptechnology/glide/load/ImageHeaderParserUtils.java com/bumptechnology/glide/load/model/h.java com/fasterxml/jackson/core/JsonFactory.java com/fasterxml/jackson/databind/ObjectReader.java com/hct2/nursegrid/android/web/util/BitmapUtils.java io/embrace/android/embracesdk/capture/metadata/EmbraceMetadataService.java io/embrace/android/embracesdk/comms/delivery/EmbraceCacheService.java io/embrace/android/embracesdk/ndk/EmbraceNdkService.java okio/Okio_JvmOkioKt.java |
| 00012 | Read data and put it into a buffer stream | file | com/hct2/nursegrid/android/web/util/BitmapUtils.java io/embrace/android/embracesdk/comms/delivery/EmbraceCacheService.java |
| 00089 | Connect to a URL and receive input stream from the server | command network | M1/a.java c/C0483a.java com/appsflyer/internal/AFc1vSDK.java com/bumptechnology/glide/load/data/HttpUrlFetcher.java com/mixpanel/android/util/HttpService.java io/embrace/android/embracesdk/samples/VerificationActions.java |
| 00030 | Connect to the remote server through the given URL | network | com/appsflyer/internal/AFa1mSDK.java com/bumptechnology/glide/load/data/HttpUrlFetcher.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|--|----------------------|---|
| 00109 | Connect to a URL and get the response code | network command | c/C0483a.java com/appsflyer/internal/AFa1mSDK.java com/appsflyer/internal/AFc1aSDK.java com/appsflyer/internal/AFc1vSDK.java com/bumptechnology/load/data/HttpUrlFetcher.java com/mixpanel/android/util/HttpService.java io/embrace/android/embracesdk/samples/VerificationActions.java |
| 00112 | Get the date of the calendar event | collection calendar | com/fasterxml/jackson/databind/ser/std/StdKeySerializers.java com/fasterxml/jackson/databind/util/StdDateFormat.java com/hct2/nursegrid/android/web/data/remote/NGDataManager.java com/hct2/nursegrid/android/web/ui/swap_details/swap_available/partial_shift/PartialShiftFragment.java com/hct2/nursegrid/android/web/ui/swap_giveaway/swap_giveaway_details/give_away/CreateGiveAwayFragment.java com/hct2/nursegrid/android/web/ui/swap_giveaway/swap_giveaway_details/swap/CreateSwapDetailsFragment.java com/hct2/nursegrid/android/web/util/CalendarUtils.java |
| 00078 | Get the network operator name | collection telephony | bo/app/yp.java com/appsflyer/internal/AFa1iSDK.java x4/HandlerC1707g.java |
| 00009 | Put data in cursor to JSON object | file | a/AbstractC0161a.java l2/C1164c.java x4/j.java x4/k.java |
| 00004 | Get filename and put it to JSON object | file collection | a/AbstractC0161a.java com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFa1iSDK.java x4/j.java x4/k.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|--|---------------------------------|--|
| 00189 | Get the content of a SMS message | sms | com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java com/hct2/nursegrid/android/web/util/BitmapUtils.java |
| 00188 | Get the address of a SMS message | sms | com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java com/hct2/nursegrid/android/web/util/BitmapUtils.java |
| 00011 | Query data from URI (SMS, CALLLOGS) | sms calllog collection | com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java com/appsflyer/internal/AFe1mSDK.java |
| 00191 | Get messages in the SMS inbox | sms | com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java |
| 00200 | Query data from the contact list | collection contact | com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java com/hct2/nursegrid/android/web/util/BitmapUtils.java |
| 00201 | Query data from the call log | collection calllog | com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java com/hct2/nursegrid/android/web/util/BitmapUtils.java |
| 00077 | Read sensitive data(SMS, CALLLOG, etc) | collection sms calllog calendar | O0/b.java a/AbstractC0161a.java com/appsflyer/internal/AFb1ySDK.java com/appsflyer/internal/AFe1jSDK.java com/appsflyer/internal/AFe1kSDK.java com/appsflyer/internal/AFe1mSDK.java com/hct2/nursegrid/android/web/util/BitmapUtils.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|---|---------------------------------|--|
| 00051 | Implicit intent(view a web page, make a phone call, etc.) via setData | control | com/hct2/nursegrid/android/web/notifications/DailySummaryBroadcastReceiver.java com/hct2/nursegrid/android/web/ui/base/BaseActivity.java io/embrace/android/embracesdk/EmbraceAutomaticVerification.java |
| 00014 | Read file into a stream and put it into a JSON object | file | a/AbstractC0161a.java |
| 00010 | Read sensitive data(SMS, CALLLOG) and put it into JSON object | sms calllog collection | a/AbstractC0161a.java |
| 00104 | Check if the given path is directory | file | a/AbstractC0161a.java |
| 00016 | Get location info of the device and put it to JSON object | location collection | com/braze/models/outgoing/BrazeLocation.java |
| 00015 | Put buffer stream (data) to JSON object | file | k4/c.java |
| 00187 | Query a URI and check the result | collection sms calllog calendar | O0/b.java |
| 00005 | Get absolute path of file and put it to JSON object | file | com/appsflyer/internal/AFa1aSDK.java |
| 00125 | Check if the given file path exist | file | com/appsflyer/internal/AFa1aSDK.java |
| 00096 | Connect to a URL and set request method | command network | c/C0483a.java com/appsflyer/internal/AFa1mSDK.java com/appsflyer/internal/AFc1vSDK.java com/mixpanel/android/util/HttpService.java |
| 00094 | Connect to a URL and read data from it | command network | com/mixpanel/android/util/HttpService.java |
| 00108 | Read the input stream from given URL | network command | com/mixpanel/android/util/HttpService.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|----------------------------------|---------------------|---|
| 00079 | Hide the current app's icon | evasion | com/hct2/nursegrid/android/web/notifications/NotificationScheduler.java |
| 00147 | Get the time of current location | collection location | com/braze/location/BrazeInternalLocationApi.java |
| 00075 | Get location of the device | collection location | com/braze/location/BrazeInternalLocationApi.java |

FIREBASE DATABASES ANALYSIS

| TITLE | SEVERITY | DESCRIPTION |
|----------------------------------|----------|--|
| App talks to a Firebase database | info | The app talks to Firebase database at https://nursegrid-production.firebaseio.com |
| Firebase Remote Config disabled | secure | Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/335733987920/namespaces/firebase:fetch?key=AlzaSyAdUbVgMd-Zolu-Wn60u41U_QLpza10CEw . This is indicated by the response: The response code is 403 |

ABUSED PERMISSIONS

| TYPE | MATCHES | PERMISSIONS |
|--------------------------|---------|--|
| Malware Permissions | 13/25 | android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.CAMERA, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.GET_ACCOUNTS, android.permission.READ_CONTACTS, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_PHONE_STATE, android.permission.VIBRATE |
| Other Common Permissions | 4/44 | android.permission.CHANGE_NETWORK_STATE, android.permission.READ_CALENDAR, 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 |
|-------------------------------------|--------|---|
| app.nursegrid.com | ok | IP: 3.214.135.73 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map |
| nursegrid-production.firebaseio.com | ok | IP: 34.120.206.254 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map |
| sinapps.s | ok | No Geolocation information available. |

| DOMAIN | STATUS | GEOLOCATION |
|--------------------------|--------|---|
| sdk.iad-01.braze.com | ok | IP: 104.18.39.68 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map |
| www.nursegrid.com | ok | IP: 141.193.213.10 Country: United States of America Region: Texas City: Austin Latitude: 30.271158 Longitude: -97.741699 View: Google Map |
| play.google.com | ok | IP: 172.253.124.113 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map |
| scheduling.nursegrid.com | ok | IP: 44.229.220.222 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map |
| sdlsdk.s | ok | No Geolocation information available. |

| DOMAIN | STATUS | GEOLOCATION |
|-------------------------|--------|---|
| app-stage.nursegrid.com | ok | IP: 52.4.202.70 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map |
| github.com | ok | IP: 140.82.113.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |
| sconversions.s | ok | No Geolocation information available. |
| simpression.s | ok | No Geolocation information available. |
| smonitorsdk.s | ok | No Geolocation information available. |
| sgcdsdk.s | ok | No Geolocation information available. |
| cdn-testsettings.s | ok | No Geolocation information available. |
| www.slf4j.org | ok | IP: 31.97.181.89 Country: United Kingdom of Great Britain and Northern Ireland Region: England City: Bowness-on-Windermere Latitude: 54.363312 Longitude: -2.918590 View: Google Map |
| sattr.s | ok | No Geolocation information available. |

| DOMAIN | STATUS | GEOLOCATION |
|-------------------------|--------|---|
| www.braze.com | ok | IP: 104.17.227.60 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |
| ssdk-services.s | ok | No Geolocation information available. |
| sadrevenue.s | ok | No Geolocation information available. |
| developers.facebook.com | ok | IP: 31.13.70.1 Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 View: Google Map |
| sars.s | ok | No Geolocation information available. |
| api.mixpanel.com | ok | IP: 35.186.241.51 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map |
| sondheim.braze.com | ok | IP: 172.64.144.252 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|-------------------------------|--------|--|
| dash-api.embrace.io | ok | IP: 44.231.235.50 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map |
| app-dev-foxtrot.nursegrid.com | ok | IP: 34.225.0.21 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map |
| cdn-settings.s | ok | No Geolocation information available. |
| sregister.s | ok | No Geolocation information available. |
| javax.xml.xmlconstants | ok | No Geolocation information available. |
| httpbin.org | ok | IP: 44.195.242.49 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map |
| iamcache.braze | ok | No Geolocation information available. |

| DOMAIN | STATUS | GEOLOCATION |
|-------------------------------------|--------|---|
| embrace.io | ok | IP: 18.238.109.106 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map |
| maps.google.com | ok | IP: 173.194.219.101 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map |
| sonelink.s | ok | No Geolocation information available. |
| sstats.s | ok | No Geolocation information available. |
| slaunches.s | ok | No Geolocation information available. |
| app-dev-whiskey.nursegrid.com | ok | IP: 34.225.0.21 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map |
| dust.k8s.test-001.d-usw-2.braze.com | ok | No Geolocation information available. |

| DOMAIN | STATUS | GEOLOCATION |
|----------------------|--------|--|
| taps.io | ok | IP: 167.114.34.171 Country: Canada Region: Quebec City: Beauharnois Latitude: 45.316780 Longitude: -73.865898 View: Google Map |
| nursegrid.onelink.me | ok | IP: 18.238.109.68 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map |
| www.googleapis.com | ok | IP: 74.125.21.95 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map |
| sapp.s | ok | No Geolocation information available. |
| nursegrid.com | ok | IP: 141.193.213.10 Country: United States of America Region: Texas City: Austin Latitude: 30.271158 Longitude: -97.741699 View: Google Map |
| schemas.android.com | ok | No Geolocation information available. |
| sviap.s | ok | No Geolocation information available. |

| DOMAIN | STATUS | GEOLOCATION |
|-----------------------------|--------|--|
| intercom.help | ok | IP: 18.97.36.99 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map |
| www.googletagmanager.com | ok | IP: 74.125.21.97 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map |
| www.google | ok | No Geolocation information available. |
| app-dev-tango.nursegrid.com | ok | IP: 34.225.0.21 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map |
| svalidate.s | ok | No Geolocation information available. |

EMAILS

| EMAIL | FILE |
|---|-----------|
| u0013android@android.com0 u0013android@android.com | Q2/f.java |

| EMAIL | FILE |
|---|---|
| support@embrace.io | io/embrace/android/embracesdk/EmbraceAutomaticVerification.java |
| support@embrace.io | io/embrace/android/embracesdk/ndk/EmbraceNdkService.java |
| automated@embrace.io | io/embrace/android/embracesdk/samples/VerificationActions.java |
| newworksite@nursegrid.com support@nursegrid.com support@embrace.io email@address.com | Android String Resource |

TRACKERS

| TRACKER | CATEGORIES | URL |
|---|----------------|---|
| AppsFlyer | Analytics | https://reports.exodus-privacy.eu.org/trackers/12 |
| Facebook Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/66 |
| Facebook Login | Identification | https://reports.exodus-privacy.eu.org/trackers/67 |
| Facebook Share | | https://reports.exodus-privacy.eu.org/trackers/70 |
| Google Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/48 |
| Google Firebase Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/49 |
| Google Tag Manager | Analytics | https://reports.exodus-privacy.eu.org/trackers/105 |
| MixPanel | Analytics | https://reports.exodus-privacy.eu.org/trackers/118 |
| OpenTelemetry (OpenCensus, OpenTracing) | Analytics | https://reports.exodus-privacy.eu.org/trackers/412 |

HARDCODED SECRETS

POSSIBLE SECRETS

"com_facebook_device_auth_instructions" : "facebook.com/deviceXXXXXXXXXXXXXXXXXXXXXXXXXXXX"

"com_facebook_device_auth_instructions" : "XXfacebook.com/deviceXXXXXXXXXXXX"

"pubnub_subscribe_key_dev_tango" : "sub-c-efaf3770-48a7-4cb2-b62b-590608983ab1"

"oauth" : "oauth"

"intercom_key" : "android_sdk-7ae433b0dde4028602cbbeddf41d0a2f343525b30"

"auth_token" : "auth_token"

"pubnub_publish_key_dev_foxtrot" : "pub-c-81d23387-d4b2-40a0-8192-8f7e1a31a8af"

"pubnub_publish_key_prod" : "pub-c-b73e1a2e-e813-4b13-8229-85700ffd72ef"

"client_token" : "clientToken"

"user" : "user"

"intro_slides_credentials" : "intro_slides-credentials"

"credentials" : "Credentials"

"intercom_secret" : "l64ekbj1"

"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"

"not_authenticated" : "Not_Authenticated"

"pubnub_publish_key_stage" : "pub-c-c96ddc18-4e49-4ce3-ad69-5b30b40bcd38"

| POSSIBLE SECRETS |
|---|
| "mix_panel_token" : "375b177bb9d4f9d4b1f3c92be96f3229" |
| "google_crash_reporting_api_key" : "AlzaSyAdUbVgMd-Zolu-Wn60u41U_QLpza10CEw" |
| "pubnub_publish_key_dev_whiskey" : "pub-c-b71da29c-f360-4a15-bc8f-5871a65d4b16" |
| "appsflyer_dev_key" : "Geuyz59RSdrq2R6cYBVSyX" |
| "credential" : "Credential" |
| "pubnub_subscribe_key_dev_foxtrot" : "sub-c-6a6ef25f-968e-474c-b5b7-02a4b2b99d80" |
| "com_braze_api_key" : "0d0cd702-edac-4675-b2e9-ce27e3eab32f" |
| "uri_credentials" : "credentials" |
| "whiskey_dev" : "whiskey" |
| "branch_key_test" : "key_test_oesdPm4GxbNDvunPzY2l6ajmzslMRZsS" |
| "com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key" |
| "pubnub_encryption_secret_key" : "6oxO9RNdpwKfKJnWke0HsOrLePGEY+pk1ZB+Pb6zL7s=" |
| "credentials_abbreviations" : "credentialsAbbreviations" |
| "branch_key" : "key_live_cnqIsh1NCiPzwsaMq6XeRmpuxjJG0tB" |
| "firebase_database_url" : "https://nursegrid-production.firebaseio.com" |
| "google_api_key" : "AlzaSyAdUbVgMd-Zolu-Wn60u41U_QLpza10CEw" |
| "pubnub_subscribe_key_prod" : "sub-c-8bd03214-9a8c-11e4-a626-02ee2ddab7fe" |

| POSSIBLE SECRETS |
|---|
| "pubnub_subscribe_key_stage" : "sub-c-a54f2778-bd2c-11e4-a594-0619f8945a4f" |
| "password" : "Password" |
| "pubnub_publish_key_dev_tango" : "pub-c-57975308-ec82-4f22-a8b0-0e6758755108" |
| "mdtp_deleted_key" : "%1\$s□□□□□□□" |
| "com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key" |
| "com_braze_firebase_cloud_messaging_sender_id" : "335733987920" |
| "notify_about_jobs_key" : "notifyAboutJobsInMyArea" |
| "pubnub_subscribe_key_dev_whiskey" : "sub-c-31602db8-1964-11eb-9b79-2636081330fc" |
| 16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a |
| 23456789abcdefghijklmnopqrstuvwxyz |
| 8dfa20b5701df6c17fe2a45f93fede32 |
| 258EAF45-E914-47DA-95CA-C5AB0DC85B11 |
| E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1 |
| a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc |
| 83b8a711842ed5d1672eb9e450081123 |
| FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901 |
| c56fb7d591ba6704df047fd98f535372fea00211 |

| POSSIBLE SECRETS |
|--|
| 8a3c4b262d721acd49a4bf97d5213199c86fa2b9 |
| 37a6259cc0c1dae299a7866489dff0bd |
| W1zcp5YuPDw8mIQDVCH2uQY7qs2ejdZj5LIglz4CbQ0wg53rlwE7DDQM6MNUgZLnzNmMSMfFrpE7 |
| eWzIsJF4PExQap9HK6Vlz8DGlgGwoiLCtyOEK0Bfu |
| 9b8f518b086098de3d77736f9458a3d2f6f95a37 |
| FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212 |
| 85053bf24bba75239b16a601d9387e17 |
| yHTAZeApn5rh6Uzfx06Gv6eHdM34YL |
| 2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3 |
| tgLRb4bjuZVA8xvQ9uHNS8UtpBIOiUcagzvtKyyfCofk5U5sNb54GgVvYxa6p4A1ObdJv1jjlUOnzR8keX5LsAM4Ia7xeqiFh0GER4I0uIVChy |

| |
|--|
| POSSIBLE SECRETS |
| eyJhbGciOiJSUzI1NiIsIng1Yyl6WyJNSUIDNIRDQ0FkRUNBU293RFFZSktvWklodmNOQVFFTEJRQXdEekVOTUFzR0ExVUVBd3dFWW05dmREQWVGdzB4TkRFeE1UZ3hOalUwTUROYUZ3MHpOR EV4TVRNeE5qVTBNRE5hTudZeEN6QUpCZ05WQkFZVEFsVIRNUk13RVFZRFZRUUIEQXBewVd4cFptOXlibWxoTVJZd0ZBWURWUVFIREExTmIzVnVkr0ZwYmlCV2FXVjNNUIF3RWdZRFZRUUtE QXRIYjI5bmJhVWdTVzVqTGpFVU1CSUdBMVVFQXd3TFptOXZMbUpoY2k1amlyMHdnZ0VpTUEwR0NTcUdTSWlzfRFFQkFRVUFBNICRhdBd2dnRUTBb0lCVFDekZWS0pPa3FubXI5ak1lV0JP ckxkcFltYzBFY3ZHM01vaGFWK1VKclZySTJTRHlrWthZV1NrVet6OUJLbUY4SFAvR2pQUERzME4NENlajIiMVdleXZWQjhSajNndUgzb0wrc0pUM3U5VjJ5NHp5bzV4TzZGV01CWUVRNlg4RGtHb FI0VHA1dGhlWWJScihORUx1bDRsRitMdEhUQ2FBQU5STWtPbDBORW9MYTZCUmhPRzY4Z0ZmSUF4eDVsVDhSRUU5dXR2UHV5K3JdYUJlbnZIT1BmOHBUmExTdmNIQmlqU0lGb1MzWTVj cmpQVmp5aVBBWIVIV25IVEZBaWxmSG5wTEJsR3hwQ3lsZVBRaE1LclBjZ3E0Q5bmQwTEE2eFIMRjdEUfhYU2E4RkxPK2ZQVjhdTkpDQXNGdXE5UmxmMIR0M1NqTHR XU1l1aDVMdWN0U DdBZ01CQUFFd0RRWUpLb1pjaHZjTkFRRUxCUUFEZ2dFQkFFc01BQlpsKzhSbGswaHFCa3RzRHVycmk0bkYvMDdDbINCZS96VWJUaVloTXByN1ZSSURsSExvZTVsc2xMaWxmWHp2YXltY01GZ UgxdUj4TndoZjdJtZdXdkl3UWVVSFNWK3JleU55Z1RUaWVPMepuOEh3KzRTQ29oSEFkTXENXVXRxdum0x2K1c0eTdPaGFTYnpsaFZDVkNuRkxWS2ljQmF5VWhldGRKWEplQ29rUjQraC9XTk0 3ZzBpS1RoYWtaT3lmYjhoMXBoeTdUTVRWbFBGS3JjYkRvNW05K0dodFBDNFBOakdMb2s2ci9qeDIDSU9DYXBJcWk4ZlhKRu94S3ZpbFIQVlxZmpXdmh4MDBqdUVVQkhycENROhdUNFRBK0 xsSTAYy1J6NXj4VzRGUUF6MU5kb0c5SFpEWldhK05ORIRaZEFtdFdQSk1MZCs4TDhzbDQ9liwiTUIJQzhUQ0NBZG1nQXdjQkFnSupBTU5JMTVickd5bGtNQTbHQ1Nxr1NJYjNEUUVQC3dVQU1 BOHhEVEFMQmdOVkjBTU1CRkp2YjNRd0hoY05NVFF4TVRFNE1UWTFOREF6V2hjTk16UXhNVEV6TVRZMU5EQXpXakFQTVewd0N3WURWUVFEREFsU2lyOTBNSUICSWpBTkja3Foa2IHOXcw QkFRRUZBQU9DQVE4QU1JSUJdZ0tDQVFFQXplVU5jNGJTV0hoT1RVKzVNUS9sT21talFXcGZCaStGSnV4dm9lT21Rd2k2ZnJS0tZyUtlWUdmQ1RQbEtFMGRtckVQOTVibmkvcUw1eEFwUDE3b 3jqVWU2S1J0SkF3Rk5JNUVaYWRJZmpiaC9xKzg1QzFdcDlCUzJZbXVaUXpyWkhQNjN5eUJwMDVZY2JNS3dDQkhYYUFnWWJtVFRrKzQrMXBqTnBIUDZZaUYyZ0NQdlNmem9rR3loYnZCcW5QY m5UZEK5dzZmak5CWUFici91Qk9UVTB2SzRrdHpsV2s1bHZzbTUxZTh2c0xTcVdob0hBRHEwQXJpQWVsVTRTSHNTQUNrUIVRU3hXVjBLNWh6VHY0ZWN2Q2JHOWRza2lEQ3dXZyt1VFJTb0FG ZVpPaE9OTDAwMHE3VmV5M0RaVGNMbDgvTzROUVZhWlI1aUFnVldsV2Nzd0lEQVFBQm8xQXdUakFkQmdOVkhRNEVGZ1Fvc2ltbEISRGNKUjBvZlI3b004S3dIRk9lK3Njd0h3WURWUjBqQk nd0ZvQVvZaW1sSVJEY0pSMG9mUjdvTThLd0hGT0grc0l3REFZRFZSMFRcQV3QXdFQj96QU5CZ2txaGtpRzI3MEJBUXNGQUFPQ0FRRUFXUWw4U21iUW9CVjN0ak9KOHpNbGNOMHhPUHBT U05ieDBnN0VML2RRZ0pwZXQwTWNXNjSSGxnUUFPS2JTM1BSZW8ybnNSQi9aUnlZRHU0aTEzWkhaOGJNc0dPRVM0QlFweJEzbXRtWGc5UmhZWVhFMGMGEVWwZCY2pqdGxydVwieGhuQUx wNfZOMXpWZHIXQVBDajBldTNNehBnTvdjeW41MFFtaUpTai9FcXUvbExodmUvd0t2akc1V2huVjh1UktSdUZRmN0MERlQUhNblpxRkhjR1M1U28wY1luU2ZLNWZiQlJOZWxHZmxocGJiUHA wVjBhWGlxaW5xRDBZTNPYVpkRnErMnJQMW9DL2E1L091NExzcFkyjVvRDlyRU5keTdicTBLZXdQRnRnUHZVa0pySjNuemjpd3ZwZ2haN3pHMjZibko1STd1YzR5MVZ1anFhT0E9PSJdfQ |
| AlzaSyAp1AXQI1fjOww5IOWGfXotvhCJKIT6Oxk |
| cc2751449a350f668590264ed76692694a80308a |
| 3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F |
| df6b721c8b4d3b6eb44c861d4415007e5a35fc95 |

PLAYSTORE INFORMATION

Title: NurseGrid: Nursing Calendar

Score: 4.1513762 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.hct2.nursegrid.android.web

Developer Details: HealthStream Inc, HealthStream+Inc, None, <http://nursegrid.com>, support@nursegrid.com,

Release Date: Aug 13, 2015 **Privacy Policy:** [Privacy link](#)

Description:

Organize. Connect. Reflect - and Get Hired. #1 shift calendar app and social networking for nurses! Take control of your schedule by balancing work and personal life like never before. NurseGrid™ lets you take control of your career with on-the-go access to organize your work, discover new job opportunities, and manage individual events. Stay connected to nursing friends through your phone or smartwatch, and share your calendar with friends, family, and colleagues. NurseGrid is used by 1 in 8 US nurses! Every day, nurses across the country trust NurseGrid to: - Carry their work calendar everywhere they go - Swap shifts with other nurses - Compare calendars with colleagues for swaps or off-duty plans - See who they are working with before their shift - Signal availability for additional shifts, swaps, and flex-offs - Manage shift calendar at multiple worksites - Add personal calendar for better life management - Discover new job opportunities - Send group and private messages to colleagues - Share your shift schedule with family and friends ... and much more! The NurseGrid Wear OS app lets you see your calendar, shift details and available swaps. It's now even easier to connect with your schedule, wherever and whenever you need it. Now available on Wear OS - View Shifts weekly - View Shift details - View Available Swaps and Giveaways - Pick up Open Shifts Getting started is easy. Find help documentation and support right in the app! ("Me" tab - "Help Center") We'd love to hear how we can help you restore your nurse life balance. Contact us at support@nursegrid.com.

☰ SCAN LOGS

| Timestamp | Event | Error |
|---------------------|--|-------|
| 2025-08-29 23:35:15 | Generating Hashes | OK |
| 2025-08-29 23:35:16 | Extracting APK | OK |
| 2025-08-29 23:35:16 | Unzipping | OK |
| 2025-08-29 23:35:17 | Parsing APK with androguard | OK |
| 2025-08-29 23:35:17 | Extracting APK features using aapt/aapt2 | OK |
| 2025-08-29 23:35:18 | Getting Hardcoded Certificates/Keystores | OK |
| 2025-08-29 23:35:21 | Parsing AndroidManifest.xml | OK |

| | | |
|---------------------|---|----|
| 2025-08-29 23:35:21 | Extracting Manifest Data | OK |
| 2025-08-29 23:35:21 | Manifest Analysis Started | OK |
| 2025-08-29 23:35:22 | Performing Static Analysis on: Nursegrid (com.hct2.nursegrid.android.web) | OK |
| 2025-08-29 23:35:23 | Fetching Details from Play Store: com.hct2.nursegrid.android.web | OK |
| 2025-08-29 23:35:23 | Checking for Malware Permissions | OK |
| 2025-08-29 23:35:23 | Fetching icon path | OK |
| 2025-08-29 23:35:23 | Library Binary Analysis Started | OK |
| 2025-08-29 23:35:23 | Analyzing lib/arm64-v8a/libmodpng.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/arm64-v8a/libjniPdfium.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/arm64-v8a/libmodpdfium.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/arm64-v8a/libembrace-native.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/arm64-v8a/libmodft2.so | OK |

| | | |
|---------------------|--|----|
| 2025-08-29 23:35:23 | Analyzing lib/arm64-v8a/libpl_droidsonroids_gif.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/x86_64/libmodpng.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/x86_64/libjniPdfium.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/x86_64/libmodpdfium.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/x86_64/libembrace-native.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/x86_64/libmodft2.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/x86_64/libpl_droidsonroids_gif.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/armeabi-v7a/libmodpng.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/armeabi-v7a/libjniPdfium.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/armeabi-v7a/libmodpdfium.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/armeabi-v7a/libembrace-native.so | OK |
| 2025-08-29 23:35:23 | Analyzing lib/armeabi-v7a/libmodft2.so | OK |

| | | |
|---------------------|--|----|
| 2025-08-29 23:35:23 | Analyzing lib/armeabi-v7a/libpl_droidsonroids_gif.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/armeabi/libmodpng.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/armeabi/libjniPdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/armeabi/libmodpdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/armeabi/libmodft2.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/armeabi/libpl_droidsonroids_gif.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/x86/libmodpng.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/x86/libjniPdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/x86/libmodpdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/x86/libembrace-native.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/x86/libmodft2.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/x86/libpl_droidsonroids_gif.so | OK |

| | | |
|---------------------|--|----|
| 2025-08-29 23:35:24 | Analyzing lib/mips/libmodpng.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/mips/libjniPdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/mips/libmodpdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/mips/libmodft2.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/mips/libpl_droidsonroids_gif.so | OK |
| 2025-08-29 23:35:24 | Analyzing lib/mips64/libpl_droidsonroids_gif.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/arm64-v8a/libmodpng.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/arm64-v8a/libjniPdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/arm64-v8a/libmodpdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/arm64-v8a/libembrace-native.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/arm64-v8a/libmodft2.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/arm64-v8a/libpl_droidsonroids_gif.so | OK |

| | | |
|---------------------|--|----|
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/x86_64/libmodpng.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/x86_64/libjniPdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/x86_64/libmodpdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/x86_64/libembrace-native.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/x86_64/libmodft2.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/x86_64/libpl_droidsonroids_gif.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/armeabi-v7a/libmodpng.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/armeabi-v7a/libjniPdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/armeabi-v7a/libmodpdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/armeabi-v7a/libembrace-native.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/armeabi-v7a/libmodft2.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/armeabi-v7a/libpl_droidsonroids_gif.so | OK |

| | | |
|---------------------|--|----|
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/armeabi/libmodpng.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/armeabi/libjniPdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/armeabi/libmodpdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/armeabi/libmodft2.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/armeabi/libpl_droidsonroids_gif.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/x86/libmodpng.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/x86/libjniPdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/x86/libmodpdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/x86/libembrace-native.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/x86/libmodft2.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/x86/libpl_droidsonroids_gif.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/mips/libmodpng.so | OK |

| | | |
|---------------------|---|----|
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/mips/libjniPdfium.so | OK |
| 2025-08-29 23:35:24 | Analyzing apktool_out/lib/mips/libmodpdfium.so | OK |
| 2025-08-29 23:35:25 | Analyzing apktool_out/lib/mips/libmodft2.so | OK |
| 2025-08-29 23:35:25 | Analyzing apktool_out/lib/mips/libpl_droidsonroids_gif.so | OK |
| 2025-08-29 23:35:25 | Analyzing apktool_out/lib/mips64/libpl_droidsonroids_gif.so | OK |
| 2025-08-29 23:35:25 | Reading Code Signing Certificate | OK |
| 2025-08-29 23:35:25 | Running APKID 2.1.5 | OK |
| 2025-08-29 23:35:33 | Detecting Trackers | OK |
| 2025-08-29 23:35:39 | Decompiling APK to Java with JADX | OK |
| 2025-08-29 23:36:11 | Converting DEX to Smali | OK |
| 2025-08-29 23:36:11 | Code Analysis Started on - java_source | OK |
| 2025-08-29 23:36:18 | Android SBOM Analysis Completed | OK |

| | | |
|---------------------|---|----|
| 2025-08-29 23:36:31 | Android SAST Completed | OK |
| 2025-08-29 23:36:31 | Android API Analysis Started | OK |
| 2025-08-29 23:36:45 | Android API Analysis Completed | OK |
| 2025-08-29 23:36:45 | Android Permission Mapping Started | OK |
| 2025-08-29 23:36:55 | Android Permission Mapping Completed | OK |
| 2025-08-29 23:36:56 | Android Behaviour Analysis Started | OK |
| 2025-08-29 23:37:11 | Android Behaviour Analysis Completed | OK |
| 2025-08-29 23:37:11 | Extracting Emails and URLs from Source Code | OK |
| 2025-08-29 23:37:20 | Email and URL Extraction Completed | OK |
| 2025-08-29 23:37:20 | Extracting String data from APK | OK |
| 2025-08-29 23:37:20 | Extracting String data from SO | OK |
| 2025-08-29 23:37:20 | Extracting String data from Code | OK |

| | | |
|---------------------|--|----|
| 2025-08-29 23:37:20 | Extracting String values and entropies from Code | OK |
| 2025-08-29 23:37:29 | Performing Malware check on extracted domains | OK |
| 2025-08-29 23:37:31 | Saving to Database | OK |

Report Generated by - MobSF v4.4.0

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

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).