

ANDROID STATIC ANALYSIS REPORT



• NayaPay (2.3.4)

File Name:

NayaPay.apk

Package Name:

com.nayapay.app

Scan Date:

Oct. 19, 2024, 12:46 p.m.

App Security Score:

50/100 (MEDIUM RISK)

Grade:

B

♣ FINDINGS SEVERITY

兼 HIGH	▲ MEDIUM	i INFO	✓ SECURE	« нотѕрот
1	18	0		2



Size: 96.01MB

MD5: 669cd6d457790cbcd8ca207f858bbe75

SHA1: 66e74ed43e077efbe4da7347cf3e6e8edfe03882

SHA256: 8001e782b272e56203a81f2c85676e79f48b4e589d99918869c87f4c93a83483

i APP INFORMATION

App Name: NayaPay

Package Name: com.nayapay.app

Main Activity: com.nayapay.app.kotlin.SplashActivity

Target SDK: 33 Min SDK: 24 Max SDK:

Android Version Name: 2.3.4 Android Version Code: 184



Activities: 192
Services: 21
Receivers: 20
Providers: 8
Exported Activities: 8
Exported Services: 3
Exported Receivers: 6
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed v1 signature: False v2 signature: True v3 signature: True

v4 signature: False

X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2020-06-06 18:11:21+00:00 Valid To: 2050-06-06 18:11:21+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0x2428b60fbfa688640a199d0804973ec12c81ae4a

Hash Algorithm: sha256

md5: 0ed4c03d7c8a24cabe9d95c9a49adfa3

sha1: 5c0565f9fa9fd3c5e970992829086c5dab9d2c01

sha256: 3231 df 32 dc f1 fa 05994 df cba 6c 566882 d3 cf 80 fa caf 934 a ea 242 b849 d46637 be

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: ff06b37ad3e3eb6da779b08addb1ffd411df95a61da76417632586338f3fbd04

∷ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.

PERMISSION	STATUS	INFO	DESCRIPTION	
android.permission.CAMERA		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.provider.MediaStore.Images.Media.EXTERNAL_CONTENT_URI		Unknown permission	Unknown permission from android reference	
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.	
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.	
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.	
com.android.launcher.permission.INSTALL_SHORTCUT	unknown	Unknown permission	Unknown permission from android reference	
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.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference	
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.	
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.	
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.	
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.nayapay.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference	
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.	

ক্ল APKID ANALYSIS

FILE	I	DETAILS				
classes.dex		FINDINGS		DETAILS		
		Compiler		dexlib 2.x		
lib/arm64-v8a/libvirago.so		FINDINGS DETAILS				
		Protector InsideSecure Verin		natrix		

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.nayapay.app.kotlin.SplashActivity	Schemes: http://, https://, Hosts: *.nayapay.com, Path Prefixes: /inapp,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.nayapay.app,

△ NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

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

Q MANIFEST ANALYSIS

HIGH: 1 | WARNING: 17 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Activity (com.nayapay.app.kotlin.veridium_biometric_verification.VeridiumBioScanActivity) 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.
3	Activity (com.nayapay.app.kotlin.veridium_biometric_verification.FingerPrintsSuccessActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.nayapay.app.payment.updatecnic.UpdateCNICActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (com.nayapay.app.scopestorage.ScopeFilePickerActivity) 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.nayapay.app.kotlin.home.DataReceivingActivity) 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.nayapay.app.kotlin.chat.message.ChatActivity) 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.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.
9	Broadcast Receiver (com.nayapay.app.kotlin.chat.backup.BackupAlarmReceiver) 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.
10	Broadcast Receiver (com.nayapay.app.kotlin.security.NayaPayBootReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
11	Broadcast Receiver (com.nayapay.common.utils.OTPReceiver) 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	Service (com.nayapay.app.kotlin.chat.notifications.fcm.DefaultFirebaseMessagingService) 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.
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	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.
15	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.
16	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
17	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
18	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

NO ISSUE SEVERITY STANDARDS	FILES
-----------------------------	-------

► SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libcryptopp_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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 readonly.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['FD_SET_chk']	False warning Symbols are available.
2	armeabi-v7a/libp7zip.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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 readonly.	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.	False warning Symbols are available.
3	armeabi-v7a/libsodium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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 readonly.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	armeabi-v7a/libcardioDecider.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
5	armeabi-v7a/libvirago.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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 readonly.	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.	False warning Symbols are available.
6	armeabi- v7a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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 readonly.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi-v7a/libcsr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
8	armeabi-v7a/libopencv_core.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
9	armeabi-v7a/libffid_dynamic.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_memcpy_chk', '_memset_chk', '_strlen_chk', '_vsprintf_chk', '_strcpy_chk', '_strcat_chk', '_strchr_chk', '_read_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi-v7a/libfaceoff.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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 readonly.	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.	False warning Symbols are available.
11	armeabi- v7a/libcardioRecognizer_tegra2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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 readonly.	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.	False warning Symbols are available.
12	armeabi-v7a/libveridiumlicensing.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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 readonly.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_memcpy_chk', '_strchr_chk', '_strlen_chk', '_vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	armeabi-v7a/libBlinklD.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_vsnprintf_chk', '_memmove_chk', '_strlen_chk']	False warning Symbols are available.
14	armeabi-v7a/libcardioRecognizer.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
15	armeabi-v7a/libopencv_imgproc.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	armeabi-v7a/libtool-checker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
17	armeabi-v7a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	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.	False warning Symbols are available.
18	arm64-v8a/libcryptopp_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['FD_SET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	arm64-v8a/libp7zip.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
20	arm64-v8a/libsodium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['strlen_chk', 'memcpy_chk']	False warning Symbols are available.
21	arm64-v8a/libcardioDecider.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	arm64-v8a/libvirago.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
23	arm64- v8a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_memcpy_chk']	False warning Symbols are available.
24	arm64-v8a/libcsr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	arm64-v8a/libopencv_core.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
26	arm64-v8a/libffid_dynamic.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_memcpy_chk', '_memmove_chk', '_memset_chk', '_strlen_chk', '_vsprintf_chk', '_strcpy_chk', '_strcat_chk', '_strchr_chk', '_read_chk']	False warning Symbols are available.
27	arm64-v8a/libfaceoff.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	arm64-v8a/libcardioRecognizer_tegra2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
29	arm64-v8a/libveridiumlicensing.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_memcpy_chk', '_strchr_chk', '_strlen_chk', '_vsnprintf_chk']	False warning Symbols are available.
30	arm64-v8a/libBlinklD.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['read_chk', 'strlen_chk', 'vsnprintf_chk', 'memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	arm64-v8a/libcardioRecognizer.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
32	arm64-v8a/libopencv_imgproc.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
33	arm64-v8a/libtool-checker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	arm64-v8a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_vsnprintf_chk', '_strlen_chk', '_read_chk', '_memmove_chk']	False warning Symbols are available.
35	armeabi-v7a/libcryptopp_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['FD_SET_chk']	False warning Symbols are available.
36	armeabi-v7a/libp7zip.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
37	armeabi-v7a/libsodium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
38	armeabi-v7a/libcardioDecider.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
39	armeabi-v7a/libvirago.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
40	armeabi- v7a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
41	armeabi-v7a/libcsr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
42	armeabi-v7a/libopencv_core.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
43	armeabi-v7a/libffid_dynamic.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_memcpy_chk', '_memset_chk', '_strlen_chk', '_vsprintf_chk', '_vsnprintf_chk', '_strcpy_chk', '_strcat_chk', '_strchr_chk', '_read_chk']	False warning Symbols are available.
44	armeabi-v7a/libfaceoff.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
45	armeabi- v7a/libcardioRecognizer_tegra2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
46	armeabi-v7a/libveridiumlicensing.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_memcpy_chk', '_strchr_chk', '_strlen_chk', '_vsnprintf_chk']	False warning Symbols are available.
47	armeabi-v7a/libBlinklD.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_vsnprintf_chk', '_memmove_chk', '_strlen_chk']	False warning Symbols are available.
48	armeabi-v7a/libcardioRecognizer.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
49	armeabi-v7a/libopencv_imgproc.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as readonly.	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.	False warning Symbols are available.
50	armeabi-v7a/libtool-checker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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 readonly.	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.	False warning Symbols are available.
51	armeabi-v7a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	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 readonly.	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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
52	arm64-v8a/libcryptopp_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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 readonly.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['FD_SET_chk']	False warning Symbols are available.
53	arm64-v8a/libp7zip.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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 readonly.	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.	False warning Symbols are available.
54	arm64-v8a/libsodium.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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 readonly.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['strlen_chk', 'memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
55	arm64-v8a/libcardioDecider.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
56	arm64-v8a/libvirago.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
57	arm64- v8a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
58	arm64-v8a/libcsr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
59	arm64-v8a/libopencv_core.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
60	arm64-v8a/libffid_dynamic.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_memcpy_chk', '_memmove_chk', '_memset_chk', '_strlen_chk', '_vsprintf_chk', '_vsprintf_chk', '_strcpy_chk', '_strcat_chk', '_strchr_chk', '_read_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
61	arm64-v8a/libfaceoff.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
62	arm64-v8a/libcardioRecognizer_tegra2.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
63	arm64-v8a/libveridiumlicensing.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_memcpy_chk', '_strchr_chk', '_strlen_chk', '_vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
64	arm64-v8a/libBlinkID.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['read_chk', 'strlen_chk', 'vsnprintf_chk', 'memmove_chk']	False warning Symbols are available.
65	arm64-v8a/libcardioRecognizer.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	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.	False warning Symbols are available.
66	arm64-v8a/libopencv_imgproc.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
67	arm64-v8a/libtool-checker.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as readonly.	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.	False warning Symbols are available.
68	arm64-v8a/libc++_shared.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['vsnprintf_chk', 'strlen_chk', 'read_chk', 'memmove_chk']	False warning Symbols are available.

■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

***: ::** ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/24	android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.READ_CONTACTS, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFL_STATE, android.permission.RECORD_AUDIO, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.READ_PHONE_STATE

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	7/45	android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.MODIFY_AUDIO_SETTINGS, com.android.launcher.permission.INSTALL_SHORTCUT, android.permission.FLASHLIGHT, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
DOMAIN	COUNTRY/REGION

© DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
maps.google.com	ok	IP: 142.250.181.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
maps.googleapis.com	ok	IP: 142.250.66.10 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.tensorflow.org	ok	IP: 142.250.181.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
nayapay-206f7.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
journeyapps.com	ok	IP: 108.139.59.96 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
github.com	ok	IP: 20.207.73.82 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS	
https://nayapay-206f7.firebaseio.com	info App talks to a Firebase Database.	



EMAIL	FILE
support@nayapay.com	Android String Resource

₽ HARDCODED SECRETS

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AlzaSyA8ym7tUMyhIMpMYfNY61P_M023NqLVBeE"
"intercom_article_single_author": "DDD{author_first_name}"
"menu_dialogs_block_user" : "Block"
"safety_net_api_key" : "AlzaSyADywzuKfljAQ8J6zwbRsOi3Eh8aq2FSbE"
"com_facebook_device_auth_instructions" : "DD facebook.com/device DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
"recaptcha_site_key" : "6LfxCPoUAAAAAPXjfE4Z5BNe2bHEyJg8nsOMH0fK"
"google_api_key" : "AlzaSyA8ym7tUMyhIMpMYfNY61P_M023NqLVBeE"
"library_zxingandroidembedded_author" : "JourneyApps"
"com_facebook_device_auth_instructions": " facebook.com/device DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD
"intercom_article_double_author" : "DDDD{author_first_name1}D{author_first_name2}"
"intercom_article_double_author" : "DDD{author_first_name1}D{author_first_name2}"
"firebase_database_url" : "https://nayapay-206f7.firebaseio.com"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"user": "%1\$s"
"intercom_api_key" : "android_sdk-4dbd019b35dd8b90bf8c0f2914c28605f391ab34"
"intercom_article_single_author" : "DDDD{author_first_name}"
"intercom_article_multiple_authors": "DDDD{author_first_name1}DD{number_of_other_authors}D"

POSSIBLE SECRETS

"geo api key": "AlzaSyBzr9F8LxYHSduGh2OE9XFlfTm8dERI4Wg"

"digits_password" : "#*\$%^&+=0123456789abcdefghijklmnopqrstuvwxyz!()@#*\$%^&+=ABCDEFGHIJKLMNOPQRSTUVWXYZ._-"

"facebook client token": "3324316e8fcba712249aa56632b79c9c"

"menu_dialogs_unblock_user": "Unblock"

"digits_username": "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ."

► PLAYSTORE INFORMATION

Title: NayaPay

Score: 4.607843 Installs: 1,000,000+ Price: 0 Android Version Support: Category: Finance Play Store URL: com.nayapay.app

Developer Details: NayaPay, NayaPay, None, http://www.nayapay.com, hello@nayapay.com,

Release Date: Feb 23, 2022 Privacy Policy: Privacy link

Description:

Welcome to NayaPay: The financial partner of choice for 1,000,000+ users. One wallet for all your everyday payments. Send money, pay bills, receive remittances from around the world, chat with friends, and shop worldwide with a free Visa debit card. Here's why you'll love NayaPay: GET STARTED INSTANTLY Download the app and set up your account right away - no wait, no fees. All you need is your CNIC and a few minutes of your time. We'll take care of the rest. FREE MEANS FREE Say goodbye to surprises (read: shocks) and unnecessary charges. No hidden fees, no annual charges and no SMS surcharge to worry about. Enjoy a free Visa card, seamless fee-free money transfers to one another and complete transparency about your money. GO INTERNATIONAL WITH VISA You'll get your FREE Visa Virtual debit card on your phone immediately upon account creation. Get a physical Visa debit card delivered to your doorstep for in-store shopping and cash withdrawals from ATMs anywhere in the world. YOU'RE IN CONTROL Order a new card, set spending limits, freeze or unfreeze your card, change your PIN, enable or disable international transactions, online payments and contactless payments - all from within your app. SEAMLESS MONEY TRANSFERS Make free, instant money transfers to any bank. Your mobile number serves as your NayaPay account number, easy to remember and share with anyone to receive funds. Connect your Raast ID to your NayaPay account to send and receive money through Raast. BILL PAYMENTS MADE EASY Manage all your bills in one place. Pay hundreds of merchants from K-Electric, LESCO, and MEPCO to SNGPL, SSGC, and StormFiber right through the app. We'll also send you reminders when your bill is due, helping you avoid pesky late payment penalties. GLOBAL REMITTANCES Looking to receive home remittance or freelance payments from abroad? Simply share your NayaPay IBAN, and our global remittance partners, including Payoneer, Western Union, Wise, Remitly, RIA, ACE, and more, will handle the rest. Your funds will be deposited directly in your account. ADD MONEY TO START SPENDING Link your bank account to effortlessly add funds to your NayaPay app. Deposit cash at partner banks or transfer money from any bank to NayaPay to load up your account and get cracking. TOP UP AND MORE Whether it's Prepaid, Postpaid, or handy bundles, we've got you covered for Ufone, Telenor, Zong, and Jazz. From call packages to data bundles for Whatsapp, Facebook, Youtube, Tiktok, and PUBG, find all your mobile top-up needs in one place. WE'LL TAKE YOU PLACES Catching a flight? Pay for your Fly Jinnah ticket directly through the NayaPay app. Would you rather go on a road trip? We've got you there too. Ditch the toll queues, recharge your M-Tag using the app and have a smooth journey! CHAT YOUR PAYMENTS AWAY Add meaning to money transfers with payment notes. Chat with your friends, share photos, send voice notes, and much more. When words fall short, use our fun stickers to express yourself. STAY ON TOP OF YOUR FINANCES Track all your transactions with detailed, easy-to-understand transaction history. Manage your finances with digital receipts, making record-keeping a breeze. NEVER LOSE SIGHT OF YOUR MONEY You know what's come in and what's gone out instantly. Receive instant push notifications for every transaction - we'll update you as soon as you send, receive and spend money so you're always in the know. YOU'RE SAFE WITH US Enjoy secure transactions. NayaPay is PCI DSS and ISO 27001 certified. Each transaction is protected by fingerprint/Face ID or MPIN verification, ensuring only you can authorize payments. NayaPay has been featured internationally by Forbes, TechCrunch, Nikkei Asia, Fintech Finance, Tech in Asia, Tech Node Global, The Asian Banker and more. We are here to help, 24/7. Reach out to us via in-app chat, email at support@nayapay.com or give us a call on +(9221) 111-222-729.

⋮≡ SCAN LOGS

Timestamp	Event	Error
-----------	-------	-------

2024-10-19 12:46:35	Generating Hashes	ОК
2024-10-19 12:46:35	Extracting APK	ОК
2024-10-19 12:46:35	Unzipping	ОК
2024-10-19 12:46:36	Getting Hardcoded Certificates/Keystores	ОК
2024-10-19 12:46:42	Parsing AndroidManifest.xml	ОК
2024-10-19 12:46:42	Parsing APK with androguard	ОК
2024-10-19 12:46:44	Extracting Manifest Data	ОК
2024-10-19 12:46:44	Performing Static Analysis on: NayaPay (com.nayapay.app)	ОК
2024-10-19 12:46:44	Fetching Details from Play Store: com.nayapay.app	ОК
2024-10-19 12:46:47	Manifest Analysis Started	ОК
2024-10-19 12:46:47	Checking for Malware Permissions	ОК
2024-10-19 12:46:47	Fetching icon path	ОК
2024-10-19 12:46:47	Library Binary Analysis Started	ОК
2024-10-19 12:46:47	Analyzing apktool_out/lib/armeabi-v7a/libcryptopp_shared.so	ОК

2024-10-19 12:46:51	Analyzing apktool_out/lib/armeabi-v7a/libp7zip.so	ОК
2024-10-19 12:46:54	Analyzing apktool_out/lib/armeabi-v7a/libsodium.so	OK
2024-10-19 12:46:54	Analyzing apktool_out/lib/armeabi-v7a/libcardioDecider.so	OK
2024-10-19 12:46:54	Analyzing apktool_out/lib/armeabi-v7a/libvirago.so	ОК
2024-10-19 12:46:54	Analyzing apktool_out/lib/armeabi-v7a/libimage_processing_util_jni.so	ОК
2024-10-19 12:46:54	Analyzing apktool_out/lib/armeabi-v7a/libcsr.so	ОК
2024-10-19 12:46:56	Analyzing apktool_out/lib/armeabi-v7a/libopencv_core.so	ОК
2024-10-19 12:46:56	Analyzing apktool_out/lib/armeabi-v7a/libffid_dynamic.so	ОК
2024-10-19 12:46:57	Analyzing apktool_out/lib/armeabi-v7a/libfaceoff.so	ОК
2024-10-19 12:46:57	Analyzing apktool_out/lib/armeabi-v7a/libcardioRecognizer_tegra2.so	ОК
2024-10-19 12:46:57	Analyzing apktool_out/lib/armeabi-v7a/libveridiumlicensing.so	ОК
2024-10-19 12:46:58	Analyzing apktool_out/lib/armeabi-v7a/libBlinkID.so	ОК
2024-10-19 12:46:58	Analyzing apktool_out/lib/armeabi-v7a/libcardioRecognizer.so	ОК
2024-10-19 12:46:58	Analyzing apktool_out/lib/armeabi-v7a/libopencv_imgproc.so	ОК

2024-10-19 12:46:59	Analyzing apktool_out/lib/armeabi-v7a/libtool-checker.so	ОК
2024-10-19 12:46:59	Analyzing apktool_out/lib/armeabi-v7a/libc++_shared.so	ОК
2024-10-19 12:47:00	Analyzing apktool_out/lib/arm64-v8a/libcryptopp_shared.so	ОК
2024-10-19 12:47:03	Analyzing apktool_out/lib/arm64-v8a/libp7zip.so	ОК
2024-10-19 12:47:06	Analyzing apktool_out/lib/arm64-v8a/libsodium.so	ОК
2024-10-19 12:47:06	Analyzing apktool_out/lib/arm64-v8a/libcardioDecider.so	ОК
2024-10-19 12:47:06	Analyzing apktool_out/lib/arm64-v8a/libvirago.so	OK
2024-10-19 12:47:06	Analyzing apktool_out/lib/arm64-v8a/libimage_processing_util_jni.so	ОК
2024-10-19 12:47:06	Analyzing apktool_out/lib/arm64-v8a/libcsr.so	ОК
2024-10-19 12:47:08	Analyzing apktool_out/lib/arm64-v8a/libopencv_core.so	ОК
2024-10-19 12:47:09	Analyzing apktool_out/lib/arm64-v8a/libffid_dynamic.so	OK
2024-10-19 12:47:09	Analyzing apktool_out/lib/arm64-v8a/libfaceoff.so	OK
2024-10-19 12:47:09	Analyzing apktool_out/lib/arm64-v8a/libcardioRecognizer_tegra2.so	ОК
2024-10-19 12:47:09	Analyzing apktool_out/lib/arm64-v8a/libveridiumlicensing.so	ОК

2024-10-19 12:47:10	Analyzing apktool_out/lib/arm64-v8a/libBlinkID.so	ОК
2024-10-19 12:47:10	Analyzing apktool_out/lib/arm64-v8a/libcardioRecognizer.so	ОК
2024-10-19 12:47:10	Analyzing apktool_out/lib/arm64-v8a/libopencv_imgproc.so	OK
2024-10-19 12:47:11	Analyzing apktool_out/lib/arm64-v8a/libtool-checker.so	ОК
2024-10-19 12:47:11	Analyzing apktool_out/lib/arm64-v8a/libc++_shared.so	ОК
2024-10-19 12:47:12	Analyzing lib/armeabi-v7a/libcryptopp_shared.so	ОК
2024-10-19 12:47:16	Analyzing lib/armeabi-v7a/libp7zip.so	OK
2024-10-19 12:47:19	Analyzing lib/armeabi-v7a/libsodium.so	ОК
2024-10-19 12:47:19	Analyzing lib/armeabi-v7a/libcardioDecider.so	ОК
2024-10-19 12:47:19	Analyzing lib/armeabi-v7a/libvirago.so	ОК
2024-10-19 12:47:19	Analyzing lib/armeabi-v7a/libimage_processing_util_jni.so	OK
2024-10-19 12:47:19	Analyzing lib/armeabi-v7a/libcsr.so	OK
2024-10-19 12:47:20	Analyzing lib/armeabi-v7a/libopencv_core.so	ОК
2024-10-19 12:47:21	Analyzing lib/armeabi-v7a/libffid_dynamic.so	ОК

2024-10-19 12:47:22	Analyzing lib/armeabi-v7a/libfaceoff.so	OK
2024-10-19 12:47:22	Analyzing lib/armeabi-v7a/libcardioRecognizer_tegra2.so	OK
2024-10-19 12:47:22	Analyzing lib/armeabi-v7a/libveridiumlicensing.so	ОК
2024-10-19 12:47:22	Analyzing lib/armeabi-v7a/libBlinkID.so	OK
2024-10-19 12:47:23	Analyzing lib/armeabi-v7a/libcardioRecognizer.so	ОК
2024-10-19 12:47:23	Analyzing lib/armeabi-v7a/libopencv_imgproc.so	OK
2024-10-19 12:47:24	Analyzing lib/armeabi-v7a/libtool-checker.so	OK
2024-10-19 12:47:24	Analyzing lib/armeabi-v7a/libc++_shared.so	OK
2024-10-19 12:47:25	Analyzing lib/arm64-v8a/libcryptopp_shared.so	ОК
2024-10-19 12:47:28	Analyzing lib/arm64-v8a/libp7zip.so	ОК
2024-10-19 12:47:31	Analyzing lib/arm64-v8a/libsodium.so	OK
2024-10-19 12:47:31	Analyzing lib/arm64-v8a/libcardioDecider.so	ОК
2024-10-19 12:47:31	Analyzing lib/arm64-v8a/libvirago.so	ОК
2024-10-19 12:47:31	Analyzing lib/arm64-v8a/libimage_processing_util_jni.so	ОК

2024-10-19 12:47:31	Analyzing lib/arm64-v8a/libcsr.so	ОК
2024-10-19 12:47:32	Analyzing lib/arm64-v8a/libopencv_core.so	ОК
2024-10-19 12:47:33	Analyzing lib/arm64-v8a/libffid_dynamic.so	ОК
2024-10-19 12:47:34	Analyzing lib/arm64-v8a/libfaceoff.so	ОК
2024-10-19 12:47:34	Analyzing lib/arm64-v8a/libcardioRecognizer_tegra2.so	ОК
2024-10-19 12:47:34	Analyzing lib/arm64-v8a/libveridiumlicensing.so	ОК
2024-10-19 12:47:34	Analyzing lib/arm64-v8a/libBlinkID.so	ОК
2024-10-19 12:47:35	Analyzing lib/arm64-v8a/libcardioRecognizer.so	ОК
2024-10-19 12:47:35	Analyzing lib/arm64-v8a/libopencv_imgproc.so	ОК
2024-10-19 12:47:36	Analyzing lib/arm64-v8a/libtool-checker.so	ОК
2024-10-19 12:47:36	Analyzing lib/arm64-v8a/libc++_shared.so	ОК
2024-10-19 12:47:36	Reading Code Signing Certificate	ОК
2024-10-19 12:47:37	Running APKiD 2.1.5	ОК
2024-10-19 12:47:42	Detecting Trackers	ОК

2024-10-19 12:47:42	Decompiling APK to Java with jadx	ОК
2024-10-19 12:47:47	Converting DEX to Smali	ОК
2024-10-19 12:47:47	Code Analysis Started on - java_source	ОК
2024-10-19 12:47:55	Android SAST Completed	ОК
2024-10-19 12:47:55	Android API Analysis Started	ОК
2024-10-19 12:47:59	Android Permission Mapping Started	ОК
2024-10-19 12:48:03	Android Permission Mapping Completed	ОК
2024-10-19 12:48:07	Finished Code Analysis, Email and URL Extraction	ОК
2024-10-19 12:48:07	Extracting String data from APK	ОК
2024-10-19 12:48:07	Extracting String data from SO	ОК
2024-10-19 12:48:08	Extracting String data from Code	ОК
2024-10-19 12:48:08	Extracting String values and entropies from Code	ОК
2024-10-19 12:48:11	Performing Malware check on extracted domains	ОК
2024-10-19 12:48:15	Saving to Database	ОК

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. © 2024 Mobile Security Framework - MobSF Ajin Abraham OpenSecurity.