




## ANDROID STATIC ANALYSIS REPORT

### BOOKSTORE



 UTPL-TT-BookStoreManager  
(1.0.2)

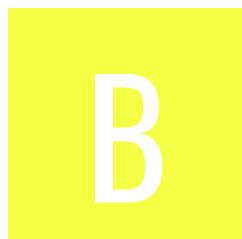
File Name: application-5f7f1f2d-08bc-40e3-99a4-8af9bd808b7d.apk

Package Name: com.daochoa6.bsmanager






Scan Date: Jan. 29, 2024, 12:35 a.m.

App Security Score: **54/100 (MEDIUM RISK)**

Grade:



## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	3	2	1	2

## FILE INFORMATION

**File Name:** application-5f7f1f2d-08bc-40e3-99a4-8af9bd808b7d.apk

**Size:** 25.25MB

**MD5:** 74be89de66750c2793c271c4f05c2372

**SHA1:** 3d535e402223bd8679d4aea0687987e331d33f81

**SHA256:** 822fa2e832c3cecd9ecbf0a7da6cd032727830f8c95dc6c896c620c277a8cc8

## APP INFORMATION

**App Name:** UTPL-TT-BookStoreManager

**Package Name:** com.daochoa6.bsmanager

**Main Activity:** com.daochoa6.bsmanager.MainActivity

**Target SDK:** 33

**Min SDK:** 21

**Max SDK:**

**Android Version Name:** 1.0.2

**Android Version Code:** 1

## APP COMPONENTS

Activities: 2

Services: 0

Receivers: 0

Providers: 2

Exported Activities: 0

Exported Services: 0

Exported Receivers: 0

Exported Providers: 0

## CERTIFICATE INFORMATION

APK is signed

v1 signature: True

v2 signature: True

v3 signature: False

Found 1 unique certificates

Subject: C=, ST=, L=, O=, OU=, CN=

Signature Algorithm: rsassa\_pkcs1v15

Valid From: 2023-07-18 02:54:08+00:00

Valid To: 2050-12-03 02:54:08+00:00

Issuer: C=, ST=, L=, O=, OU=, CN=

Serial Number: 0x7dda4fcf

Hash Algorithm: sha256

md5: 2251338ea7ceddaa6f0a260c222a0bec

sha1: eba303e70899a89b3eb620d7d50003b043126f31

sha256: 4dd8866d3497258ea6621bd043659860b3a75ad49bf54c6e4cf3ff426869e617

sha512: ceac2bc6e206359a549230d383e4d2d979a53d54248dcbf8282cf2eddf42ef7c755ebd18581016cbd43a92379ab6093a9983445f8b7e5d51c308ee36b6a6d791

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 99136db806256349ab53f5ca2186caaea9d16e7901fb5fc1273d9d806e0f3d85

## APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference

## APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check
	Compiler	r8 without marker (suspicious)
classes2.dex	FINDINGS	DETAILS
	Compiler	r8 without marker (suspicious)

## BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.daochoa6.bsmanager.MainActivity	Schemes: com.daochoa6.bsmanager://,

## NETWORK SECURITY

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

## CERTIFICATE ANALYSIS

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

## MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.

## CODE ANALYSIS

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



NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/ImageView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/MaskView.java com/horcrux/svg/PatternView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/swmansion/rnscreens/ScreenStackHeaderC onfigViewManager.java com/th3rdwave/safeareacore/SafeAreaView.ja va expo/modules/ExpoModulesPackage\$Companio n\$packageList\$2.java expo/modules/adapters/react/services/UIManag erModuleWrapper.java expo/modules/adapters/react/views/ViewManag erAdapterUtils.java expo/modules/application/ApplicationModule.jav a expo/modules/apploader/AppLoaderProvider.jav a expo/modules/constants/ConstantsService.java expo/modules/constants/ExponentInstallationId.j ava expo/modules/core/logging/OSLogHandler.java expo/modules/filesystem/FileSystemModule.java expo/modules/securestore/AuthenticationHelper .java expo/modules/securestore/SecureStoreModule.j ava expo/modules/splashscreen/singletons/SplashSc reen\$show\$2.java expo/modules/splashscreen/singletons/SplashSc reen\$show\$4.java expo/modules/splashscreen/singletons/SplashSc

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	<a href="#">MD5 is a weak hash known to have hash collisions.</a>	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	reen\$show\$6.java expo/modules/filesystem/FileSystemModule.java
3	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/constants/ExponentInstallationId.java
4	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	expo/modules/adapters/react/NativeModulesProxy.java expo/modules/constants/ExponentInstallationId.java expo/modules/filesystem/FileSystemModuleKt.java expo/modules/interfaces/permissions/PermissionsResponse.java

## SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	--------------	-------	---------	---------	------------------

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/arm64-v8a/libc++_shared.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk', '__strlen_chk', '__read_chk', '__memmove_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/arm64-v8a/libexpo-modules-core.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/arm64-v8a/libfabricjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/arm64-v8a/libfb.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/arm64-v8a/libfbjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/arm64-v8a/libfolly_runtime.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk', '__memcpy_chk', '__vsnprintf_chk', '__memset_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	lib/arm64-v8a/libgifimage.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk', ['__strlen_chk', ['__memmove_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	lib/arm64-v8a/libglog.so	<p>True</p> <p><a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True</p> <p><a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None</p> <p><a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None</p> <p><a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True</p> <p><a href="#">info</a></p> <p>The shared object has the following fortified functions:</p> <pre>['__memcpy_chk', '__strlen_chk', '__strncat_chk', '__vsnprintf_chk']</pre>	<p>True</p> <p><a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	lib/arm64-v8a/libglog_init.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	lib/arm64-v8a/libhermes.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__strchr_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	lib/arm64-v8a/libhermes_executor.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	lib/arm64-v8a/libimagepipeline.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	lib/arm64-v8a/libjsi.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	lib/arm64-v8a/libjsijniProfiler.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	lib/arm64-v8a/libjsinspector.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	lib/arm64-v8a/liblogger.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	lib/arm64-v8a/libmapbufferjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	lib/arm64-v8a/libnative-filters.so	<p>True <b>info</b></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <b>info</b></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <b>info</b></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <b>info</b></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <b>warning</b></p> <p>The shared object 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.</p>	<p>True <b>info</b></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	lib/arm64-v8a/libnative-image-transcoder.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk', '__strlen_chk', '__memmove_chk', '__vsprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	lib/arm64-v8a/libreactnativeblob.so	<p>True</p> <p><a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True</p> <p><a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None</p> <p><a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None</p> <p><a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True</p> <p><a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True</p> <p><a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	lib/arm64-v8a/libreactnativejni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	lib/arm64-v8a/libreactperloggerjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	lib/arm64-v8a/libreact_codegen_rncore.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	lib/arm64-v8a/libreact_nativemodule_core.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	lib/arm64-v8a/libreact_newarchdefaults.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	lib/arm64-v8a/libreact_render_animations.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	lib/arm64-v8a/libreact_render_attributedstring.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	lib/arm64-v8a/libreact_render_componentregistry.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	lib/arm64-v8a/libreact_render_core.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	lib/arm64-v8a/libreact_render_graphics.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
35	lib/arm64-v8a/libreact_render_imagemanager.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
36	lib/arm64-v8a/libreact_render_leakchecker.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
37	lib/arm64-v8a/libreact_render_mapbuffer.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__memcpy_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
38	lib/arm64-v8a/libreact_render_mounting.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
39	lib/arm64-v8a/libreact_render_runtimescheduler.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
40	lib/arm64-v8a/libreact_render_scheduler.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
42	lib/arm64-v8a/libreact_render_templateprocessor.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
43	lib/arm64-v8a/libreact_render_textlayoutmanager.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
44	lib/arm64-v8a/libreact_render_uimanager.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
46	lib/arm64-v8a/librrc_image.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
47	lib/arm64-v8a/librrc_root.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
48	lib/arm64-v8a/librrc_scrollview.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
49	lib/arm64-v8a/librrc_text.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
50	lib/arm64-v8a/librrc_textinput.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
51	lib/arm64-v8a/librrc_unimplementedview.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
52	lib/arm64-v8a/librrc_view.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
54	lib/arm64-v8a/libstatic-webp.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk', '__strlen_chk', '__memcpy_chk', '__memmove_chk', '__vsprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
55	lib/arm64-v8a/libturbomodulejsijni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
56	lib/arm64-v8a/libyoga.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
57	lib/armeabi-v7a/libc++_shared.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
59	lib/armeabi-v7a/libexpo-modules-core.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
60	lib/armeabi-v7a/libfabricjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
61	lib/armeabi-v7a/libfb.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
62	lib/armeabi-v7a/libfbjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
63	lib/armeabi-v7a/libfolly_runtime.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk', '__memcpy_chk', '__vsnprintf_chk', '__memset_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
64	lib/armeabi-v7a/libgifimage.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
65	lib/armeabi-v7a/libglog.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__memcpy_chk',  '__strlen_chk',  '__strncat_chk',  '__vsnprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
66	lib/armeabi-v7a/libglog_init.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
67	lib/armeabi-v7a/libhermes.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__strchr_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
68	lib/armeabi-v7a/libhermes_executor.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
69	lib/armeabi-v7a/libimagepipeline.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
70	lib/armeabi-v7a/libjsi.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
71	lib/armeabi-v7a/libjsijniProfiler.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
72	lib/armeabi-v7a/libjsinspector.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
73	lib/armeabi-v7a/liblogger.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
74	lib/armeabi-v7a/libmapbufferjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
75	lib/armeabi-v7a/libnative-filters.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
76	lib/armeabi-v7a/libnative-imagetranscoder.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
77	lib/armeabi-v7a/libreactnativeblob.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
78	lib/armeabi-v7a/libreactnativejni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
79	lib/armeabi-v7a/libreactperloggerjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
80	lib/armeabi-v7a/libreact_codegen_rncore.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
83	lib/armeabi-v7a/libreact_nativemodule_core.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
84	lib/armeabi-v7a/libreact_newarchdefaults.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
85	lib/armeabi-v7a/libreact_render_animations.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
86	lib/armeabi-v7a/libreact_render_attributedstring.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
87	lib/armeabi-v7a/libreact_render_componentregistry.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
88	lib/armeabi-v7a/libreact_render_core.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
90	lib/armeabi-v7a/libreact_render_graphics.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
91	lib/armeabi-v7a/libreact_render_imagemanager.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
92	lib/armeabi-v7a/libreact_render_leakchecker.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
93	lib/armeabi-v7a/libreact_render_mapbuffer.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__memcpy_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
94	lib/armeabi-v7a/libreact_render_mounting.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
95	lib/armeabi-v7a/libreact_render_runtimescheduler.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
96	lib/armeabi-v7a/libreact_render_scheduler.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
97	lib/armeabi-v7a/libreact_render_telemetry.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
98	lib/armeabi-v7a/libreact_render_templateprocessor.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
99	lib/armeabi-v7a/libreact_render_textlayoutmanager.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
100	lib/armeabi-v7a/libreact_render_uimanager.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
102	lib/armeabi-v7a/librrc_image.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
103	lib/armeabi-v7a/librrc_root.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
104	lib/armeabi-v7a/librrc_scrollview.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
105	lib/armeabi-v7a/librrc_text.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
106	lib/armeabi-v7a/librrc_textinput.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
107	lib/armeabi-v7a/librrc_unimplementedview.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
108	lib/armeabi-v7a/librrc_view.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
109	lib/armeabi-v7a/libruntimeexecutor.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False <a href="#">high</a></p> <p>This shared object 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.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
110	lib/armeabi-v7a/libstatic-webp.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
111	lib/armeabi-v7a/libturbomodulejsijni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
112	lib/armeabi-v7a/libyoga.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
113	lib/x86/libc++_shared.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
115	lib/x86/libexpo-modules-core.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
116	lib/x86/libfabricjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
117	lib/x86/libfb.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
118	lib/x86/libfbjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
119	lib/x86/libfolly_runtime.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk', '__memcpy_chk', '__vsnprintf_chk', '__memset_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
120	lib/x86/libgifimage.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
121	lib/x86/libglog.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__memcpy_chk',  '__strlen_chk',  '__strncat_chk',  '__vsnprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
122	lib/x86/libglog_init.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
123	lib/x86/libhermes.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__strchr_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
124	lib/x86/libhermes_executor.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
125	lib/x86/libimagepipeline.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
126	lib/x86/libjsi.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
127	lib/x86/libjsijni profiler.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
128	lib/x86/libjsinspector.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
129	lib/x86/liblogger.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
130	lib/x86/libmapbufferjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
131	lib/x86/libnative-filters.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
132	lib/x86/libnative-imagetranscoder.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
133	lib/x86/libreactnativeblob.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
134	lib/x86/libreactnativejni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
135	lib/x86/libreactperfloggerjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
136	lib/x86/libreact_codegen_rncore.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
139	lib/x86/libreact_nativemodule_core.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
140	lib/x86/libreact_newarchdefaults.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
141	lib/x86/libreact_render_animations.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
142	lib/x86/libreact_render_attributedstring.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
143	lib/x86/libreact_render_componentregistry.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
144	lib/x86/libreact_render_core.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
146	lib/x86/libreact_render_graphics.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
147	lib/x86/libreact_render_imagemanager.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
148	lib/x86/libreact_render_leakchecker.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
149	lib/x86/libreact_render_mapbuffer.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__memcpy_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
150	lib/x86/libreact_render_mounting.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
151	lib/x86/libreact_render_runtimescheduler.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
152	lib/x86/libreact_render_scheduler.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
153	lib/x86/libreact_render_telemetry.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
154	lib/x86/libreact_render_templateprocessor.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
155	lib/x86/libreact_render_textlayoutmanager.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
156	lib/x86/libreact_render_uimanager.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
158	lib/x86/librrc_image.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
159	lib/x86/librrc_root.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
160	lib/x86/librrc_scrollview.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
161	lib/x86/librrc_text.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
162	lib/x86/librrc_textinput.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
163	lib/x86/librrc_unimplementedview.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
164	lib/x86/librrc_view.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
166	lib/x86/libstatic-webp.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
167	lib/x86/libturbomodulejsijni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
168	lib/x86/libyoga.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
169	lib/x86_64/libc++_shared.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk', '__strlen_chk', '__read_chk', '__memmove_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
171	lib/x86_64/libexpn-modules-core.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
172	lib/x86_64/libfabricjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
173	lib/x86_64/libfb.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
174	lib/x86_64/libfbjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
175	lib/x86_64/libfolly_runtime.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk', '__memcpy_chk', '__vsnprintf_chk', '__memset_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
176	lib/x86_64/libgifimage.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk', ['__strlen_chk', ['__memmove_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
177	lib/x86_64/libglog.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__memcpy_chk',  '__strlen_chk',  '__strncat_chk',  '__vsnprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
178	lib/x86_64/libglog_init.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
179	lib/x86_64/libhermes.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__vsnprintf_chk', '__strchr_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
180	lib/x86_64/libhermes_executor.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
181	lib/x86_64/libimagepipeline.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
182	lib/x86_64/libjsi.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
183	lib/x86_64/libjsijniProfiler.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
184	lib/x86_64/libjsinspector.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
185	lib/x86_64/liblogger.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
186	lib/x86_64/libmapbufferjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
187	lib/x86_64/libnative-filters.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
188	lib/x86_64/libnative-imagetranscoder.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk', '__memmove_chk', '__strlen_chk', '__vsnprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
189	lib/x86_64/libreactnativeblob.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
190	lib/x86_64/libreactnativejni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
191	lib/x86_64/libreactperloggerjni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
192	lib/x86_64/libreact_codegen_rncore.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
195	lib/x86_64/libreact_nativemodule_core.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
196	lib/x86_64/libreact_newarchdefaults.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
197	lib/x86_64/libreact_render_animations.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
198	lib/x86_64/libreact_render_attributedstring.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
199	lib/x86_64/libreact_render_componentregistry.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
200	lib/x86_64/libreact_render_core.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
202	lib/x86_64/libreact_render_graphics.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
203	lib/x86_64/libreact_render_imagemanager.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
204	lib/x86_64/libreact_render_leakchecker.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
205	lib/x86_64/libreact_render_mapbuffer.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__memcpy_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
206	lib/x86_64/libreact_render_mounting.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
207	lib/x86_64/libreact_render_runtimescheduler.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
208	lib/x86_64/libreact_render_scheduler.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
209	lib/x86_64/libreact_render_telemetry.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False <a href="#">high</a></p> <p>This shared object 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.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
210	lib/x86_64/libreact_render_templateprocessor.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
211	lib/x86_64/libreact_render_textlayoutmanager.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
212	lib/x86_64/libreact_render_uimanager.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__strlen_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
214	lib/x86_64/librrc_image.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
215	lib/x86_64/librrc_root.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
216	lib/x86_64/librrc_scrollview.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
217	lib/x86_64/librrc_text.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
218	lib/x86_64/librrc_textinput.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
219	lib/x86_64/librrc_unimplementedview.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
220	lib/x86_64/librrc_view.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

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

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
222	lib/x86_64/libstatic-webp.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk', '__strlen_chk', '__memmove_chk', '__vsprintf_chk', '__memcpy_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
223	lib/x86_64/libturbomodulejsijni.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>The shared object 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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
224	lib/x86_64/libyoga.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__vsprintf_chk']</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	<a href="#">FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2</a>	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	<a href="#">FCS_COP.1.1(1)</a>	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
12	<a href="#">FCS_COP.1.1(2)</a>	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
13	<a href="#">FCS_HTTPS_EXT.1.2</a>	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
14	<a href="#">FCS_HTTPS_EXT.1.3</a>	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
15	<a href="#">FIA_X509_EXT.2.1</a>	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
16	<a href="#">FCS_CKM.1.1(2)</a>	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

# DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
github.com	ok	<b>IP:</b> 140.82.112.3 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
ns.adobe.com	ok	No Geolocation information available.

---

## Report Generated by - MobSF v3.6.1 Beta

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

© 2024 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).