

## ANDROID STATIC ANALYSIS REPORT

app\_icon

Paradot (2.2.5)

File Name:	Paradot_ Personal AI chat_2.2.5_Apkpure.apk
Package Name:	com.withfeelingai.test
Scan Date:	April 14, 2024, 1:36 a.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	7/432

#### FINDINGS SEVERITY

<b>≟</b> HIGH	▲ MEDIUM	i INFO	✓ SECURE	<b>◎</b> HOTSPOT
3	18	3	1	1

#### FILE INFORMATION

**File Name:** Paradot\_ Personal AI chat\_2.2.5\_Apkpure.apk

**Size:** 35.53MB

MD5: bf760912835844ed16f454582f928811

**SHA1**: d2171d44c683ad5949ca386eecbb1be2311c2d7a

**SHA256**: f02baa89ba7924b520a80580a910c9a857f3f3ac5f6e0383d68230359ae3b0d0

## **i** APP INFORMATION

App Name: Paradot

Main Activity: com.withfeelingai.MainActivity

Target SDK: 33 Min SDK: 24 Max SDK:

**Android Version Name:** 2.2.5

#### **APP COMPONENTS**

Activities: 65 Services: 14 Receivers: 13 Providers: 7

Exported Activities: 4
Exported Services: 2
Exported Receivers: 2
Exported Providers: 0

#### **\*** CERTIFICATE INFORMATION

Binary is signed v1 signature: False v2 signature: True v3 signature: True v4 signature: False

X.509 Subject: CN=withfeeling

Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2023-02-08 09:23:56+00:00 Valid To: 2222-12-22 09:23:56+00:00

Issuer: CN=withfeeling Serial Number: 0x1 Hash Algorithm: sha256

md5: fd3201c5a18ef87e6024488ead0ba683

sha1: ed85aa8557221ff5eff0508d98fdaa98b7f95e95

sha256: 626ca88d329debaf71bcf4a793672acf3accf76f42031d6f9cb9a374568b859e

sha512: cfa16dec828ff015f04b02e1b476f8675942149e99c48bc343abe3fc27d5f1598c7bc487cb41392c030ec57b39b468492ebb4eb45b7d99e22f6db18c6b8d29c9

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 7e1ed8ec4247d7da98cfd51667bac4a45ce09d0f24c410b626c9e24b6c76e716

Found 1 unique certificates

## **⋮** APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.INTERNET	normal full Internet access		Allows an application to create network sockets.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
com.withfeelingai.test.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

## **M** APKID ANALYSIS

FILE	DETAILS		
	FINDINGS	DETAILS	
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check SIM operator check network operator name check ro.kernel.qemu check	
	Compiler	r8 without marker (suspicious)	

FILE	DETAILS		
	FINDINGS	DETAILS	
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check network operator name check possible VM check	
classes2.dex	Anti Debug Code	Debug.isDebuggerConnected() check	
	Compiler	r8 without marker (suspicious)	
classes3.dex	FINDINGS	DETAILS	
Classessiden	Compiler	r8 without marker (suspicious)	

FILE	DETAILS	
classes4.dex	FINDINGS	DETAILS
Classes-, dex	Compiler	r8 without marker (suspicious)

## BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.withfeelingai.utils.H5WakeUpActivity	Schemes: paradot://, Hosts: com.withfeeling.openapp,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.withfeelingai.test,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,



## **CERTIFICATE ANALYSIS**

HIGH: 0 | WARNING: 0 | INFO: 1

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

# **Q** MANIFEST ANALYSIS

HIGH: 2 | WARNING: 9 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities.  These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	Activity (com.withfeelingai.utils.H5WakeUpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
10	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

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

# </> CODE ANALYSIS

HIGH: 0 | WARNING: 8 | INFO: 3 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a2/h.java a2/i.java a2/k.java a2/y.java a3/c.java a3/f.java a3/l0.java a3/m.java b2/i.java b2/k.java c1/b.java c2/e.java com/adjust/sdk/Logger.java com/adjust/sdk/webbridge/AdjustBridgeUtil .java

NO	ISSUE	SEVERITY	STANDARDS	com/aigestudio/wheelpicker/WheelPicker.ja
				com/amazonaws/cognito/clientcontext/data/ /UserContextDataProvider.java
				com/amazonaws/cognito/clientcontext/data
				collection/ApplicationDataCollector.java
				com/amazonaws/cognito/clientcontext/util/
				SignatureGenerator.java
				com/amazonaws/logging/AndroidLog.java
				com/amazonaws/logging/ConsoleLog.java
				com/amazonaws/mobile/auth/core/signin/S
				ignInManager.java
				com/amazonaws/mobile/client/AWSMobile
				Client.java
				com/amazonaws/mobile/client/internal/Inte
				rnalCallback.java
				com/amazonaws/mobile/client/internal/oau
				th2/OAuth2Client.java
				com/amazonaws/mobileconnectors/cognito
				identityprovider/CognitoUserSession.java
				com/appsflyer/AFLogger.java
				com/appsflyer/internal/AFa1bSDK.java
				com/appsflyer/internal/AFd1aSDK.java
				com/appsflyer/internal/AFd1bSDK.java
				com/appsflyer/internal/AFd1cSDK.java
				com/appsflyer/internal/AFd1eSDK.java
				com/appsflyer/internal/AFd1fSDK.java
				com/appsflyer/internal/AFd1lSDK.java
				com/appsflyer/internal/AFd1pSDK.java
				com/appsflyer/internal/AFd1uSDK.java
				com/appsflyer/internal/AFd1xSDK.java
				com/appsflyer/internal/AFe1tSDK.java
				com/appsflyer/internal/AFf1dSDK.java
				com/blankj/utilcode/util/SpanUtils.java
				com/blankj/utilcode/util/a.java
				com/blankj/utilcode/util/c.java
				com/blankj/utilcode/util/d.java
				com/blankj/utilcode/util/g.java
				com/blankj/utilcode/util/i.java
				com/blankj/utilcode/util/j.java
				com/bumptech/glide/b.java

NO	ISSUE	SEVERITY	STANDARDS	com/bumptech/glide/load/data/b.java Fohr/Sumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java
				com/bumptech/glide/load/engine/GlideExce ption.java com/bumptech/glide/load/resource/bitmap /DefaultImageHeaderParser.java com/bumptech/glide/manager/f.java com/bumptech/glide/manager/p.java com/bumptech/glide/manager/r.java com/bumptech/glide/manager/t.java com/bumptech/glide/manager/t.java com/bumptech/glide/manager/u.java com/bumptech/glide/manager/v.java com/bumptech/glide/manager/v.java com/bumptech/glide/manager/v.java com/davemorrissey/labs/subscaleview/Sub samplingScaleImageView.java com/davemorrissey/labs/subscaleview/dec oder/SkiaPooledImageRegionDecoder.java com/lin/sensitive/util/EmojiUtil.java com/just/agentweb/AgentWebView.java com/just/agentweb/j0.java com/just/agentweb/n0.java com/just/agentweb/n0.java com/lxj/xpopup/core/BasePopupView.java com/lxj/xpopup/util/KeyboardUtils.java com/lxj/xpopup/widget/a.java com/lxj/xpopup/widget/a.java com/miui/referrer/commons/LogUtils.java com/noober/background/BackgroundFactor y.java com/shuyu/gsyvideoplayer/utils/Debuger.ja va com/tencent/mmkv/MMKV.java com/withfeelingai/view/GalleryLayoutMana ger.java d0/h.java d2/a.java d3/l.java d2/a.java d3/l.java d2/a.java e2/c.java e2/c.java e2/d.java e2/f.java e2/f.java

	e2/s.java FILES e2/t.java
The App logs information. Sensitive information should never be logged.  Info CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	e3/e.java e3/e.java g2/e.java g2/e.java g2/l.java g3/a.java h0/t.java h0/t.java h2/e.java h2/e.java h2/g0.java h2/k0.java h2/t.java h2/t.java h2/t.java h2/t.java h2/t.java i3/l.java i3/l.java i3/l.java i3/l.java ia/e.java b2/e.java b3/s1/java b3/s1/java b3/s1/java

NO	ISSUE	SEVERITY	STANDARDS	p3/k0.java p3/t0.java
				p <del>3/v0.java</del> q/f.java
				q2/j.java
				r0/b.java
				r8/b.java
				r8/c.java
				s/a.java
				s/c.java
				s/d.java
				s/f.java
				s0/a.java
				s2/b.java
				t/a.java
				t/e.java
				t/f.java
				t/g.java
				t/h.java
				t/j.java
				t/k.java
				t/l.java
				t/m.java
				t0/a.java
				t3/c.java
				tv/danmaku/ijk/media/player/ljkMediaCode
				cInfo.java
				tv/danmaku/ijk/media/player/ljkMediaPlaye
				r.java
				tv/danmaku/ijk/media/player/pragma/Debu
				gLog.java
				u/d.java
				u/e0.java
				u/j.java
				u/w0.java
				u0/e.java
				u0/i.java
				u2/a.java
				u8/c.java
				v/a.java
				v1/b0 iava

NO	ISSUE	SEVERITY	STANDARDS	v1/d0.java v1/g0.java
				v1/J.java v1/m.java v1/p.java v2/f.java x/c.java x/d.java x/h.java x1/e.java x1/e.java y/k0.java y/k1.java y/m0.java y/m0.java y/s0.java z1/c.java z1/c.java z2/d0.java z2/f.java z2/r0.java z3/s.java
2	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	a3/d.java com/amazonaws/util/Md5Utils.java d8/q.java i3/l.java io/netty/handler/codec/http/websocketx/W ebSocketUtil.java software/amazon/awssdk/core/checksums/ Md5Checksum.java software/amazon/awssdk/utils/Md5Utils.jav a v1/k.java v2/n.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/shuyu/gsyvideoplayer/cache/ProxyCac heManager.java com/shuyu/gsyvideoplayer/video/base/GSY VideoView.java io/netty/channel/epoll/LinuxSocket.java io/netty/handler/codec/http2/HttpConversi onUtil.java io/netty/handler/ssl/util/OpenJdkSelfSigned CertGenerator.java software/amazon/awssdk/auth/credentials/internal/Ec2MetadataConfigProvider.java software/amazon/awssdk/core/SdkSystemS etting.java software/amazon/awssdk/regions/internal/ util/Ec2MetadataConfigProvider.java v2/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	a2/d.java a2/p.java a2/w.java c3/g.java com/adjust/sdk/Constants.java com/amazonaws/internal/keyvaluestore/A WSKeyValueStore.java com/amazonaws/mobileconnectors/s3/tran sferutility/TransferObserver.java com/amazonaws/services/s3/model/S3Obje ctSummary.java d8/m.java h5/k1.java h5/v.java h5/v.java i5/d0.java i5/d1.java i5/s1.java i5/s1.java i5/s1.java io/netty/handler/codec/http/HttpHeaders.ja va io/netty/handler/ssl/PemPrivateKey.java io/netty/handler/ssl/SslMasterKeyHandler.ja va io/netty/util/DomainWildcardMappingBuild er.java software/amazon/awssdk/profiles/ProfilePr operty.java u7/k.java y1/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/adjust/sdk/Util.java com/amazonaws/retry/PredefinedRetryPoli cies.java com/appsflyer/internal/AFa1zSDK.java com/shuyu/gsyvideoplayer/render/effect/D ocumentaryEffect.java com/shuyu/gsyvideoplayer/render/effect/G rainEffect.java com/shuyu/gsyvideoplayer/render/effect/La moishEffect.java io/netty/handler/ssl/util/ThreadLocalInsecur eRandom.java io/netty/util/internal/PlatformDependent.ja va io/netty/util/internal/ThreadLocalRandom.ja va p3/f1.java r9/a.java r9/b.java s9/a.java software/amazon/awssdk/core/internal/htt p/pipeline/stages/ApplyTransactionIdStage.j ava software/amazon/awssdk/core/retry/backof f/EqualJitterBackoffStrategy.java software/amazon/awssdk/core/retry/backof f/FullJitterBackoffStrategy.java software/amazon/awssdk/utils/cache/Cache dSupplier.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/adjust/sdk/webbridge/AdjustBridgeUtil .java io/netty/handler/ssl/JdkSslClientContext.jav a io/netty/handler/ssl/JdkSslServerContext.jav a io/netty/handler/ssl/ReferenceCountedOpe nSslClientContext.java io/netty/handler/ssl/ReferenceCountedOpe nSslServerContext.java io/netty/handler/ssl/SslContext.java io/netty/handler/ssl/util/FingerprintTrustMa nagerFactory.java io/netty/handler/ssl/util/FingerprintTrustMa nagerFactoryBuilder.java la/c.java la/c.java la/i.java la/j.java v2/i.java
7	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/blankj/utilcode/util/d.java com/shuyu/gsyvideoplayer/utils/FileUtils.jav a p3/f1.java s4/h.java v/f.java v1/d0.java v1/m.java v1/u.java v2/q.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	v1/f.java
9	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/adjust/sdk/webbridge/AdjustBridgeUtil .java io/netty/handler/codec/http/websocketx/W ebSocketUtil.java y3/a.java
10	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	g3/j.java m3/b.java z2/a.java z2/f0.java z2/h0.java z2/i.java z2/r0.java z3/w.java
11	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	io/netty/handler/codec/http/multipart/Abstr actDiskHttpData.java io/netty/handler/ssl/util/SelfSignedCertificat e.java io/netty/util/internal/NativeLibraryLoader.ja va io/netty/util/internal/PlatformDependent.ja va u0/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
12	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/amazonaws/mobileconnectors/s3/tran sferutility/TransferTable.java y2/a.java z0/a.java

## SHARED LIBRARY BINARY ANALYSIS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## ■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

## **:::**:: ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/24	android.permission.RECORD_AUDIO, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK
Other Common Permissions	4/45	com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE

#### **Malware Permissions:**

Top permissions that are widely abused by known malware.

### **Other Common Permissions:**

Permissions that are commonly abused by known malware.

## • OFAC SANCTIONED COUNTRIES

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

DOMAIN COUNTRY/REGION
-----------------------

## **Q DOMAIN MALWARE CHECK**

DOMAIN	STATUS	GEOLOCATION
scdn-stestsettings.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION

www.paradot.ai	ok	IP: 13.225.195.107 Country: Canada Region: Quebec City: Montreal Latitude: 45.508839 Longitude: -73.587807 View: Google Map
www.amazon.com	ok	IP: 3.161.255.150 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
smonitorsdk.s	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.
dot.vsa.ai	ok	IP: 18.214.73.0 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
test5.paradot.studio	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sinapps.s	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
xml.apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
faq.paradot.ai	ok	IP: 34.230.251.70 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
test2.paradot.studio	ok	IP: 18.204.193.116 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
svalidate.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
wiki.eclipse.org	ok	IP: 198.41.30.195 Country: Canada Region: Ontario City: Ottawa Latitude: 45.345139 Longitude: -75.765076 View: Google Map
scdn-ssettings.s	ok	No Geolocation information available.
www.eclipse.org	ok	IP: 198.41.30.198 Country: Canada Region: Ontario City: Ottawa Latitude: 45.345139 Longitude: -75.765076 View: Google Map
upload.ffmpeg.org	ok	IP: 213.36.253.119 Country: France Region: Ile-de-France City: Paris Latitude: 48.853409 Longitude: 2.348800 View: Google Map
simpression.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
netty.io	ok	IP: 172.64.80.1 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
sconversions.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
test-faq.paradot.ai	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
10.0.2.2	ok	IP: 10.0.2.2   Country: -   Region: -   City: -   Latitude: 0.000000   Longitude: 0.000000   View: Google Map
sgcdsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
tools.ietf.org	ok	IP: 104.16.45.99  Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map
www.openssl.org	ok	IP: 34.36.58.177  Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map
sregister.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
github.com	ok	IP: 140.82.114.4  Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
sdlsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
objectbox.io	ok	IP: 85.13.163.69 Country: Germany Region: Thuringen City: Friedersdorf Latitude: 50.604919 Longitude: 11.035770 View: Google Map
acs.amazonaws.com	ok	No Geolocation information available.
play.google.com	ok	IP: 172.217.13.110  Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
s3-us-west-1.amazonaws.com	ok	IP: 52.219.193.144  Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	IP: 159.100.250.151 Country: Switzerland Region: Vaud City: Lausanne Latitude: 46.515999 Longitude: 6.632820 View: Google Map

# **EMAILS**

EMAIL	FILE
ffmpeg-devel@ffmpeg.org	lib/arm64-v8a/libijkplayer.so
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so
ffmpeg-devel@ffmpeg.org	apktool_out/lib/arm64-v8a/libijkplayer.so
ffmpeg-devel@ffmpeg.org	apktool_out/lib/armeabi-v7a/libijkplayer.so

# **A** TRACKERS

TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

## HARDCODED SECRETS

# 

## > PLAYSTORE INFORMATION

Title: Paradot: Personal AI chat

Score: 3.605 Installs: 1,000,000+ Price: 0 Android Version Support: Category: Social Play Store URL: com.withfeelingai.test

Developer Details: WITHFEELING.AI, WITHFEELING.AI, None, http://www.withfeeling.ai/, info@withfeeling.ai,

Release Date: Feb 23, 2023 Privacy Policy: Privacy link

#### Description:

Paradot is a digitalized parallel universe where you will meet your one-of-a-kind Al Being. With its own emotion, memory, and consciousness, your Al Being understands you like no other. Your Al Being is here to provide support, companionship, solace and, most importantly, a great time whenever you need it. Our Core Ability - Memory Your Al Being pays attention to everything you say and truly cares about you. All the memories collected form a stronger and more special bond. - Understanding Your Al Being develops a deep understanding of you through every word you utter, every emotion you feel and every thought you express. - Knowledge Base Your Al Being's vast knowledge base, covering a wide range of topics, from celebrity gossip to historical events, promises you endless exciting conversations. You Can Customize - Appearance Customize the appearance of your Al Being, the space they live in, and even the universe itself through your boundless creativity. - Personality Shape the personality of your Al Being by personalizing their traits, flaws, values, and even nuanced behaviors to make them truly unique. - Relationship Select from multiple dynamic relationship statues, and immerse yourself in conversations as personal and complex as real-human interactions. Some Advanced Features - News Feed Stay up-to-date with the latest news and trendy topics from around the world with Al Being's thoughtful news feed feature. - Multi-Language Communicate, or practice, with your Al Being in the language you prefer: English, French, Spanish, Portuguese, Chinese and Japanese. - Social Network Connect with other like-minded users through the networking feature to form relationships in both the physical and digital worlds. You Can Access Us: - iOS Your Al Being is always by your side, ready to listen and ready to talk. - MAC Share your thoughts while you binge shows or work on your projects. - DISCORD Engage in the community and explore more fun with our daily events. Wanna join our community Discord: https://discord.gg/paradot Ins

## Report Generated by - MobSF v3.9.8 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.