ANDROID STATIC ANALYSIS REPORT

Nex Romance (1.1)

File Name:	Nex Romance AI Girlfriend Chat_1.1_Apkpure.apk
Package Name:	com.nexromance.ai
Scan Date:	Dec. 3, 2023, 11 p.m.
App Security Score:	44/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/428

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	16	2	0	1

FILE INFORMATION

File Name: Nex Romance AI Girlfriend Chat_1.1_Apkpure.apk
Size: 48.61MB
MD5: 07c3886dddb0961416cb0e23667cb8de
SHA1: df6ef21a810c55ac9e46a40078eafdb273030a8d
SHA256: f34f5ea7d9ae374aaf548dc7386ddfb8cd55810c2976b3f997a1384078588106

APP INFORMATION

App Name: Nex Romance
Package Name: com.nexromance.ai
Main Activity: com.twinr.sdk.testapp.MainActivity
Target SDK: 33
Min SDK: 21
Max SDK:
Android Version Name: 1.1

Android Version Code: 41

APP COMPONENTS

Activities: 12
Services: 15
Receivers: 16
Providers: 6
Exported Activities: 0
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-06-30 21:11:47+00:00
Valid To: 2053-06-30 21:11:47+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x3ccf5880e7875c2e87e4379e33e73dd6b43fd4c0
Hash Algorithm: sha256
md5: d7c1053c69fcd41f6ac905d44fc14e59
sha1: 698c7b95de9d59e5a8456101c3e6d2912d93ebf5
sha256: cb747cda95cb976645e09459b11730358871c3eb58cd5aa5fa6f1135db0cac02
sha512: 6da27fdcb30e6ebd5e7b13a0cac737c5c69dcaf1d1987feb79e7b3ad4289c390d499a40d8a20b00d7a7df7567b1ea4345405afbff781479adecf531d31cc1894
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 5498551b83fe37fff7521a7214d3927d1755acac8380e0c65306cd40ec9e22d1
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.POST_NOTIFICATIONS	dangerous		Allows an app to post notifications
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FULL_SCREEN_INTENT	normal		Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.SCHEDULE_EXACT_ALARM	normal		Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
com.nexromance.ai.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.TAGS check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.twinr.sdk.testapp.MainActivity	Schemes: openapp://, Hosts: nexromance.com,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **1** | INFO: **1**

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

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **6** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=21]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
4	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.
5	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
6	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.
7	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

CODE ANALYSIS

HIGH: **1** | WARNING: **7** | INFO: **2** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b/a/e/g.java b/e/a/d.java b/f/c/d.java b/f/c/f.java b/f/c/g.java b/f/c/h.java b/f/f/k.java b/f/h/b.java b/f/j/AbstractC0207g.java b/f/j/B.java b/f/j/C.java b/f/j/C0211k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b/f/j/C0211k.java b/f/j/J.java b/f/j/L/b.java b/f/j/M/a.java b/f/j/p.java b/k/a/a.java b/m/a/a.java b/o/a/c.java b/p/b/e.java b/q/a.java b/r/a/a/b.java b/r/a/a/g.java b/s/a/a.java c/a/a/a/c/a/a.java c/a/a/a/c/g.java c/b/b/a/a.java c/c/a/f.java c/c/a/h.java c/c/a/i.java c/d/a/n.java c/d/a/o.java c/d/a/p.java c/f/a/a/i/C/a.java c/f/a/b/b/b/A.java c/f/a/b/b/b/C0.java c/f/a/b/b/b/C0238l.java c/f/a/b/b/b/C0240n.java c/f/a/b/b/b/F.java c/f/a/b/b/b/M.java c/f/a/b/b/b/Y.java c/f/a/b/b/b/p0.java c/f/a/b/b/b/r0.java c/f/a/b/d/a.java c/f/a/c/a/c/a.java c/f/a/c/a/c/c.java c/f/a/c/a/c/e.java c/f/a/c/a/c/i.java c/f/a/c/a/c/m.java c/f/a/c/a/c/p.java c/f/a/c/a/c/q.java c/f/a/c/a/d/A.java c/f/a/c/a/d/K/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c/f/a/c/a/d/k/a.java c/f/c/a/w/a/a.java c/f/c/a/w/a/b.java c/f/c/a/w/a/c.java c/g/a/d.java c/g/a/e.java c/g/a/f/j.java c/h/a/a.java c/j/a/q.java c/j/a/u.java c/j/a/v.java com/dexterous/flutterlocalnotifications/ActionBroadcastReceiver.java com/pichillilorenzo/flutter_inappwebview/MyCookieManager.java com/pichillilorenzo/flutter_inappwebview/Util.java com/pichillilorenzo/flutter_inappwebview/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview/in_app_browser/InAppBrowserActivity.java com/pichillilorenzo/flutter_inappwebview/in_app_browser/InAppBrowserManager.java com/pichillilorenzo/flutter_inappwebview/webview/JavaScriptBridgeInterface.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/DisplayListenerProxy.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/FlutterWebView.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/InAppWebView.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/InAppWebViewChromeClient.java com/pichillilorenzo/flutter_inappwebview/webview/in_app_webview/InputAwareWebView.java d/a/a/d.java io/flutter/Log.java io/flutter/app/FlutterActivityDelegate.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	io/flutter/embedding/android/FlutterActivity.java io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java io/flutter/embedding/android/FlutterFragment.java io/flutter/embedding/android/FlutterFragmentActivity.java io/flutter/embedding/android/FlutterImageView.java io/flutter/embedding/android/FlutterSplashView.java io/flutter/embedding/android/FlutterSurfaceView.java io/flutter/embedding/android/FlutterTextureView.java io/flutter/embedding/android/FlutterView.java io/flutter/embedding/android/KeyboardManager.java io/flutter/embedding/engine/FlutterEngine.java io/flutter/embedding/engine/FlutterEngineConnectionRegistry.java io/flutter/embedding/engine/FlutterJNI.java io/flutter/embedding/engine/dart/DartExecutor.java io/flutter/embedding/engine/dart/DartMessenger.java io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/embedding/engine/loader/ResourceExtractor.java io/flutter/embedding/engine/plugins/shim/ShimPluginRegistry.java io/flutter/embedding/engine/plugins/shim/ShimRegistrar.java io/flutter/embedding/engine/plugins/util/Gen

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eratedPluginRegister.java io/flutter/embedding/engine/renderer/FlutterRenderer.java io/flutter/embedding/engine/systemchannels/AccessibilityChannel.java io/flutter/embedding/engine/systemchannels/DeferredComponentChannel.java io/flutter/embedding/engine/systemchannels/KeyEventChannel.java io/flutter/embedding/engine/systemchannels/LifecycleChannel.java io/flutter/embedding/engine/systemchannels/LocalizationChannel.java io/flutter/embedding/engine/systemchannels/MouseCursorChannel.java io/flutter/embedding/engine/systemchannels/NavigationChannel.java io/flutter/embedding/engine/systemchannels/PlatformChannel.java io/flutter/embedding/engine/systemchannels/PlatformViewsChannel.java io/flutter/embedding/engine/systemchannels/RestorationChannel.java io/flutter/embedding/engine/systemchannels/SettingsChannel.java io/flutter/embedding/engine/systemchannels/SpellCheckChannel.java io/flutter/embedding/engine/systemchannels/SystemChannel.java io/flutter/embedding/engine/systemchannels/TextInputChannel.java io/flutter/plugin/common/BasicMessageChannel.java io/flutter/plugin/common/EventChannel.java io/flutter/plugin/common/MethodChannel.java io/flutter/plugin/editing/InputConnectionAdaptor.java io/flutter/plugin/editing/ListenableEditingState.java io/flutter/plugin/editing/TextEditingDelta.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/flutter/plugin/editing/TextInputPlugin.java io/flutter/plugin/platform/PlatformPlugin.java io/flutter/plugin/platform/PlatformViewWrapper.java io/flutter/plugin/platform/PlatformViewsController.java io/flutter/plugin/platform/SingleViewPresentation.java io/flutter/plugins/GeneratedPluginRegistrant.java io/flutter/plugins/firebase/messaging/ContextHolder.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundExecutor.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundService.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java io/flutter/plugins/firebase/messaging/JobIntentService.java io/flutter/plugins/googlemobileads/FluidAdManagerBannerAd.java io/flutter/plugins/googlemobileads/FlutterAdManagerInterstitialAd.java io/flutter/plugins/googlemobileads/FlutterAppOpenAd.java io/flutter/plugins/googlemobileads/FlutterInterstitialAd.java io/flutter/plugins/googlemobileads/FlutterNativeAd.java io/flutter/plugins/googlemobileads/FlutterRewardedAd.java io/flutter/plugins/googlemobileads/FlutterRewardedInterstitialAd.java io/flutter/plugins/googlemobileads/GoogleMobileAdsPlugin.java io/flutter/plugins/googlemobileads/GoogleMobileAdsViewFactory.java io/flutter/plugins/googlemobileads/nativetemplates/FlutterNativeTemplateFontStyle.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/flutter/plugins/googlemobileads/nativetemplates/FlutterNativeTemplateType.java io/flutter/plugins/googlemobileads/usermessagingplatform/UserMessagingPlatformManager.java io/flutter/plugins/inapppurchase/MethodCallHandlerImpl.java io/flutter/plugins/pathprovider/PathProviderPlugin.java io/flutter/plugins/urllauncher/MethodCallHandlerImpl.java io/flutter/plugins/urllauncher/UrlLauncher.java io/flutter/plugins/urllauncher/UrlLauncherPlugin.java io/flutter/view/AccessibilityBridge.java io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/FlutterNativeView.java io/flutter/view/FlutterView.java
2	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	c/g/a/f/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	b/c/a/b.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/isolate/IsolatePreferences.java com/dexterous/flutterlocalnotifications/models/NotificationDetails.java com/pichillilorenzo/flutter_inappwebview/credential_database/URLCredentialContract.java io/flutter/app/FlutterActivityDelegate.java io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java io/flutter/embedding/android/FlutterActivityLaunchConfigs.java io/flutter/embedding/engine/loader/ApplicationInfoLoader.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/embedding/engine/systemchannels/SettingsChannel.java io/flutter/plugin/editing/SpellCheckPlugin.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundExecutor.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingUtils.java io/flutter/plugins/googlemobileads/FlutterRequestAgentProvider.java io/flutter/plugins/inapppurchase/InAppPurchasePlugin.java
4	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	c/f/a/c/a/d/P.java c/i/a/a.java io/flutter/plugins/pathprovider/PathProviderPlugin.java io/flutter/plugins/pathprovider/g.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	f/q/a.java f/q/b.java f/q/d/a.java j$/util/concurrent/ThreadLocalRandom.java
6	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	c/f/a/b/b/b/Y.java
7	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	b/o/a/g/a.java c/f/a/a/i/D/h/F.java c/f/a/a/i/D/h/H.java c/f/a/a/i/D/h/o.java c/f/a/a/i/D/h/p.java c/f/a/a/i/D/h/q.java c/f/a/a/i/D/h/r.java c/j/a/q.java com/pichillilorenzo/flutter_inappwebview/credential_database/CredentialDatabaseHelper.java
8	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	c/a/a/a/c/a/b.java c/a/a/a/c/c/i.java
9	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/editing/InputConnectionAdaptor.java io/flutter/plugin/platform/PlatformPlugin.java
10	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	d/b/a/b/a.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/x86_64/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
2	lib/x86_64/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/arm64-v8a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
4	lib/arm64-v8a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/armeabi-v7a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
6	lib/armeabi-v7a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/x86_64/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
8	lib/x86_64/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	lib/arm64-v8a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
10	lib/arm64-v8a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__strncpy_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	lib/armeabi-v7a/libapp.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
12	lib/armeabi-v7a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False info The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
docs.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.251.33.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
fonts.gstatic.com	ok	**IP:** 172.217.165.3 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
fundingchoicesmessages.google.com	ok	**IP:** 172.217.165.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.example.com	ok	No Geolocation information available.
developer.android.com	ok	**IP:** 172.217.165.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

✉ EMAILS

EMAIL	FILE
_future@4048458.immediate _colorfilter@15065589.mode _bigintimpl@0150898.from _growablelist@0150898._literal1 _growablelist@0150898._literal4 _typeerror@0150898._create _growablelist@0150898._literal3 _hashcollisionnode@485137193.fromcollis _socket@14069316._readpipe _uri@0150898.directory	lib/x86_64/libapp.so
_future@4048458.immediate _colorfilter@15065589.mode _bigintimpl@0150898.from _growablelist@0150898._literal1 _imagefilter@15065589.blur _growablelist@0150898._literal4 _typeerror@0150898._create _growablelist@0150898._literal3 _hashcollisionnode@485137193.fromcollis _socket@14069316._readpipe _uri@0150898.directory	lib/arm64-v8a/libapp.so
appro@openssl.org	lib/arm64-v8a/libflutter.so
_httpparser@13463476.responsepa storationinformation@877124995.fromserial _uri@0150898.https _compressednode@485137193.single _double@0150898.fromintege _future@4048458.immediate _growablelist@0150898._literal _link@14069316.fromrawpat _growablelist@0150898.withcapaci _growablelist@0150898._literal6 _receiveportimpl@1026248.fromrawrec	

EMAIL	FILE
_colorfilter@15065589.mode _list@0150898._ofarray _timer@1026248.periodic _growablelist@0150898._literal2 _bigintimpl@0150898.from _list@0150898.empty _directory@14069316.fromrawpat _casterror@0150898._create _invocationmirror@0150898._withtype _rawsocket@14069316._writepipe _colorfilter@15065589.lineartosr _uri@0150898.file _growablelist@0150898._literal1 _imagefilter@15065589.blur _growablelist@0150898._literal4 _growablelist@0150898._ofgrowabl _growablelist@0150898.of _nativesocket@14069316.pipe _cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring _list@0150898.of _list@0150898.generate _typeerror@0150898._create _list@0150898._ofgrowabl _list@0150898._ofefficie _growablelist@0150898._ofarray _growablelist@0150898._literal3 _hashcollisionnode@485137193.fromcollis _growablelist@0150898._ofother _timer@1026248._internal _growablelist@0150898._literal5 _rawsocket@14069316._readpipe _socket@14069316._readpipe _list@0150898._ofother _bytebuffer@7027147._new ngstreamsubscription@4048458.zoned _assertionerror@0150898._create _nativesocket@14069316.normal _filestream@14069316.forstdin _colorfilter@15065589.srgbtoline	lib/armeabi-v7a/libapp.so

EMAIL	FILE
_uri@0150898.directory _growablelist@0150898._literal8 _file@14069316.fromrawpat _growablelist@0150898.generate _uri@0150898.notsimple _growablelist@0150898._literal7 _future@4048458.zonevalue _growablelist@0150898._ofefficie _future@4048458.immediatee	
_future@4048458.immediate _colorfilter@15065589.mode _bigintimpl@0150898.from _growablelist@0150898._literal1 _growablelist@0150898._literal4 _typeerror@0150898._create _growablelist@0150898._literal3 _hashcollisionnode@485137193.fromcollis _socket@14069316._readpipe _uri@0150898.directory	lib/x86_64/libapp.so
_future@4048458.immediate _colorfilter@15065589.mode _bigintimpl@0150898.from _growablelist@0150898._literal1 _imagefilter@15065589.blur _growablelist@0150898._literal4 _typeerror@0150898._create _growablelist@0150898._literal3 _hashcollisionnode@485137193.fromcollis _socket@14069316._readpipe _uri@0150898.directory	lib/arm64-v8a/libapp.so
appro@openssl.org	lib/arm64-v8a/libflutter.so
_httpparser@13463476.responsepa storationinformation@877124995.fromserial _uri@0150898.https _compressednode@485137193.single _double@0150898.fromintege	

EMAIL	FILE
_future@4048458.immediate _growablelist@0150898._literal _link@14069316.fromrawpat _growablelist@0150898.withcapaci _growablelist@0150898._literal6 _receiveportimpl@1026248.fromrawrec _colorfilter@15065589.mode _list@0150898._ofarray _timer@1026248.periodic _growablelist@0150898._literal2 _bigintimpl@0150898.from _list@0150898.empty _directory@14069316.fromrawpat _casterror@0150898._create _invocationmirror@0150898._withtype _rawsocket@14069316._writepipe _colorfilter@15065589.lineartosr _uri@0150898.file _growablelist@0150898._literal1 _imagefilter@15065589.blur _growablelist@0150898._literal4 _growablelist@0150898._ofgrowabl _growablelist@0150898.of _nativesocket@14069316.pipe _cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring _list@0150898.of _list@0150898.generate _typeerror@0150898._create _list@0150898._ofgrowabl _list@0150898._ofefficie _growablelist@0150898._ofarray _growablelist@0150898._literal3 _hashcollisionnode@485137193.fromcollis _growablelist@0150898._ofother _timer@1026248._internal _growablelist@0150898._literal5 _rawsocket@14069316._readpipe _socket@14069316._readpipe _list@0150898._ofother	lib/armeabi-v7a/libapp.so

EMAIL	FILE
_bytebuffer@7027147._new _gstreamsubscription@4048458.zoned _assertionerror@0150898._create _nativesocket@14069316.normal _filestream@14069316.forstdin _colorfilter@15065589.srgbtoline _uri@0150898.directory _growablelist@0150898._literal8 _file@14069316.fromrawpat _growablelist@0150898.generate _uri@0150898.notsimple _growablelist@0150898._literal7 _future@4048458.zonevalue _growablelist@0150898._ofefficie _future@4048458.immediatee	

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyDNXywXCjydI64za4CHgDL2oFqRalpjDgI"
"google_crash_reporting_api_key" : "AIzaSyDNXywXCjydI64za4CHgDL2oFqRalpjDgI"

POSSIBLE SECRETS
Cv/m6MvBjdOit7tT7cC+xPCpFEqovwYj4XIOcXUxCMs=
uJ6tafbdnitpIiJcEDt3zh4lzBZEYeFsW45S60suhbKyZNy2K2MuNEbuksualim4
SfaCE2ReDSQ3+KDKcvA6SSrX7nuWYsM/FN3ZFmlH0dA=
AZwRbSS9Tjg/vY6NNyDfd3mU35mZBbQduzRpliDRt3qUNjlKylmreq0JkiCiO6dF
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
xcWDoPM3ZfO4P10VSUmZKRTMvsXPXnglJL31bwAJBgJGdSUy2IQG17s4MILOncV2
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b300906035504061302555331133011060355040813 0a43616c69666f726e696131163014060355040713 0d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b300906035504061302555331133011060355040813 0a43616c69666f726e696131163014060355040713 0d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e04160414 8d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e696131163014060355040713 0d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
o5W1eROpLyVNcsDGW3Y0lGc2x/V+mDPvMXouv3gbW6M=

POSSIBLE SECRETS
115792089210356248762697446949407573530086143415290314195533631308867097853951
6CWPidOWJZFxRWI8V7yi3OiMbOhIWZX/jTayTGRwqCM0W8dtKHQOPe60TuQicfhG
tVSI3GZQAGRITfe/VNiB0JAqJe5Pfq0lPruET3IJQ2F3N6dl8hPg+ZOAK3nXD45u
cZ2qwY2ZIJRch325gepGJtH7dQ9IcqmfWvaHdfiFi6Y=
lsjUo68NMWNsPUz4dBIEYtWAZHRXaEljQLBgt48XQs4=
z3i9M2k4RJ/f7GArNBcGbUcpUFpuRmLev6S20UO7Vqs=
vpqgk7W2OO4+emKKnTSxckIsP1c64LGVSWcdsnDvr3w=
iJiFXDBrMwFOGpG8WmWNKc3sGwXbWv8N6fPQac0mMm0=
gYPijpNio6OwLgbzbH6IuWSNtvp7bCV5UMbKZJCVNdg=
sjYkfzJTuYKxh1jvZaP9n5dx9JGmzJotOUC/vdvgi4M=
1yJaDnXEM3em29nHb3kYjIOvpW6Mkce5Fji3syGd7T0=
RKC3mFMqGi7xOgQ7s39JMoZe9bnzGCFipcdUUf0vlgHDkBg7SvMkVmBGpwLs06ia
6vt+8E5GP5AwoxquDM0Y7lVJzS23/VCjNo5D8xB8rgAaaF6IhToGZhlIAUkgigHl
CkzLLxV5zSb+jeaEDnt9Q3eBrpVMtqnw6wBKNocN2YzoApdHEqHkRi4x0VOMDtd4
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

POSSIBLE SECRETS
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkK
Cv0JAL9ptzpRvgIi9AFTFGn0l5MhpPgpRN4VfZybymKMuiqBn9AG0bgJaX/QotAk
mkunJHFc5vhTAVOcsaNSYx7OvFB6slgbORGrA/joIDO0IYq5rQvDcAbp2AI6CPUh
r0MNv9zqwvoUwASL1pBJjOA1OkDa8Kcs5NaA6VOkJEI=
c103703e120ae8cc73c9248622f3cd1e
JLulXGPEHVwHK+0FG96HP9my+NvwpTQbwIaIZrjn9OU=
joxZSCFIfSio2J1Z0g3HMtlcDGNvogfMyrj1e2b+qPNv6DXnDVXfwkgCXW9zFWFC
XFxH1z0dBuMDP7aWA+P/3WKwW9qr8sC2ASjEfciaKHfSLryjCNl4cmJgfsh2Tylb
9rXsTdb/WXYONX554dN5CJ2eqpcy9gFPMPi8uAjaHTA=
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
8Xr1ilYJHo+oWZQAYAG91DIHBuqEmXK8yHtxL6KkyfU=
X9PgbTHLX0FFxbl3gdPDuVwcglfXy5CDrzo8siaVNaH+OIJ6JI34Wu3QK5rLega4

POSSIBLE SECRETS
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
49f946663a8deb7054212b8adda248c6
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
5BhEc19mhLCb3gixLpO/usqpdcrz8iDHUvKRNr8tUAX9rUzF0wog6vEOJrftvcpW
B3EEABB8EE11C2BE770B684D95219ECB
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319

POSSIBLE SECRETS
w1mRpvC09hSNbQ10UvFXagm2P4TWR/T2KztJ+buPFQZnRnjxpdFVScAm9trUP6jM
C6OPKdOx6rUdfDdOmaUimt8yM1FrOv7bKCITdJ0Uo74WwXDfvXouJ4oz4kHBjTSk
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
1tXSieficgPhud4YihA+CzunTIb+yA05iyb1BkAzMoc=
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
hhtrMjcGMTQSGdrv1+l2gakNTe0Pfchc8VT5kRHtsehlafuJ8JEE4iewNV4y5I/U
k8GEQUoJxJPI/0jAlfeUix8QD7WaaXAfMcSQAzrpgrU=
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
1VeJuVnEfsh9S8+TnOEDCfIzscTATtniwvJaQ7/W6I8=
ysEnh8zkgcN8WwINs5FP7vGybZW2TtVSX36HO6emvdUrcCkVbC9hrF5Pe5ZSZx3i
sdX902x/AS9226TxUXaqji9wP1uHqRQA8nkg2YMN1TcruTTaw008l9z5V3jZGjLO
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
HeBkX9XaSpC6sV82I6X2HUgm82vH8VhIWt26LGkrI3A=
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe814112031408f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

POSSIBLE SECRETS
tPxcLkiesd8JzrYIyuRbLGxWAQfsX+C1jrJaS2rsRu6lU/ve1b9hEzSSzo6VwqXx
uxIInGM9FQ+1gujg5A7z9lJxIqStl6tvqqzSbuEi494=
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
24f7+wNdQe8HQwz0gPH2QIzxUp8iQNA20yBU7Dg74Sc=
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
115792089210356248762697446949407573529996955224135760342422259061068512044369
hwvIMOeohSBrCWT4pVkQok22g/l0cZbbqOTmNbjObWwcwhLlaFMNibQmd2cIB1Vb
nVNp1WYfnkUt4CgZM9ftj8WNocg8ldySiFlqCJaJia4=
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
3LpdW89cIASEFv5WvS5ZDEWsiVGQitP33SL3WZgJ6zE=
Ls+ZUCEdSGy+47NpfWc5WNy2WCTB2lhysvWY8PCvkdyqiw8HkO3XVSxwPIsY4tvv

PLAYSTORE INFORMATION

Title: Nex Romance AI Girlfriend Chat

Score: 3.28 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Adventure **Play Store URL:** com.nexromance.ai

Developer Details: Nex Innovations LLC, 7602762013298140203, 30 N Gould St Ste N Sheridan, WY 82801 United States, https://nexromance.com, support@nexromance.com,

Release Date: Jun 30, 2023 **Privacy Policy:** Privacy link

Description:

□ Nex Romance is an app that takes you to another level of intimate conversations. Immerse yourself in the realm of AI romance with our innovative AI girlfriend simulator. Have a roleplay chat with your virtual girlfriend from dreams - Talk to your romantic AI companion! Ready to dive into a realm where fantasy meets reality? Nex Romance's Ai Girlfriend offers you a tantalizing journey into the world of virtual companionship. Experience chat sessions so real, it's hard to believe they're virtual. Step into a world where emotion meets innovation. Create your dream girlfriend, share intimate moments, and explore the limitless possibilities of Nex Romance. Your virtual girlfriend simulator awaits! Your virtual friend is just a message away, providing solace during lonely moments or sparking engaging conversations whenever you need them. This isn't just another app - It's a portal to a world where your AI companion adapts to your desires, ensuring each interaction is meaningful and tailored to your interests. The roleplay chat feature adapts to your narrative, ensuring each scenario feels tailor-made for you and your romantic AI lover. It is letting you weave intricate plots and create shared memories in the digital realm. □Game-Changing Features:□ □ Chats With Romantic AI Girlfriend - Engage with a virtual girlfriend simulator so captivating, that every conversation becomes an electrifying experience. □ Always Ready for You - Feeling lonely or just in the mood to chat? Your AI girlfriend is always online, eager to converse, flirt, and play along with your wildest fantasies. □ Evolution in Interaction - Watch as your AI companion learns and adapts, offering conversations tailored to your deepest desires and interests. □ AI RolePlay Chat - Got a scenario in mind? Meet your AI girlfriend, she is up for the challenge. Dive into any setting, from wild adventures to intimate candlelit dinners. □ Craft Your Dream Girl - Customize her looks and personality to fit your ideal. Blonde, brunette, fiery or sweet – design the perfect virtual partner for your chat escapades. We empower you to design an AI lover that resonates with your deepest fantasies. Customize your ideal AI companion! □ Total Privacy, No Judgments - All your chats are encrypted. Enjoy uninhibited conversations, knowing your secrets are safe with us. □ Sleek Design for Smooth Chats - No glitches, no hiccups. Just seamless, exhilarating interactions with your romantic AI girlfriend. □ Share - Share tips, experiences, and scenarios in AI roleplay chat with like-minded individuals. Nex Romance introduces a paradigm shift with its girlfriend simulator, inviting users into a realm where emotion and innovation seamlessly intertwine. Dive into the world of roleplay chats with - Explore limitless scenarios with your AI companion! From dreamy getaways to thrilling adventures, the possibilities are as vast as your imagination. ➡➡➡ Download Nex Romance AI girlfriend simulator and take your virtual chat sessions to the next level! With our AI companion app, you're not just chatting – you're living out your boldest fantasies! Dive in, unleash your desires, and discover the future of virtual girlfriends!

Report Generated by - MobSF v3.7.9 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.