



ANDROID STATIC ANALYSIS REPORT

app_icon

 AI Emily (1.5.2)

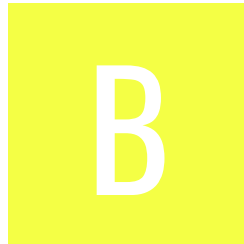
File Name: Emily_ Your AI Girlfriend_1.5.2_Apkpure.apk

Package Name: com.aifriends.emily

Scan Date: Dec. 3, 2023, 11:44 p.m.






App Security Score: 52/100 (MEDIUM RISK)

Grade:



Trackers Detection: 17/428

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	16	1	2	5

FILE INFORMATION

File Name: Emily_ Your AI Girlfriend_1.5.2_Apkpure.apk

Size: 50.0MB

MD5: dbe1f180afbea58bf1f067d6bcb87132

SHA1: d1b441466e2a966cbe86bb7ec4536ed4be3b1079

SHA256: c5a909170de6e36793f009dc65ee93bb5ec87b1a67dc8d68b8c46fa22d731427

APP INFORMATION

App Name: AI Emily

Package Name: com.aifriends.emily

Main Activity: com.aifriends.aigirlfriend.MainActivity

Target SDK: 33

Min SDK: 21

Max SDK:

Android Version Name: 1.5.2

Android Version Code: 519

APP COMPONENTS

Activities: 55

Services: 14

Receivers: 19

Providers: 12

Exported Activities: 1

Exported Services: 1

Exported Receivers: 6

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: 2023-09-13 04:08:37+00:00

Valid To: 2053-09-13 04:08:37+00:00

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

Serial Number: 0xf2faf355a4186641e128e445887a2b6d05588024

Hash Algorithm: sha256

md5: 52a7dc4b3e364a789849e3f9fd8579c0

sha1: 4701c1d326ac8606660dbe63369fb4bfe4c25786

sha256: b8efd8200e78d9817fcc9218ad4f35fc6338c95f7d1e56dcb510aa482010678f

sha512: 33d347afa5313e673c544ec80882927904f5c1c21f09194e22d4f3c212d1eb0a6e7104d101fcdf7e7782b7ccafc311eb472bdf97ec849ab14076ba6ad8f662af

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 772082f3499f636a1f8e6ed18eca603c06d74c8d47a2e83a8b4300d149723af3

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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference
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.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.POST_NOTIFICATIONS	dangerous		Allows an app to post notifications
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
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	signature	C2DM permissions	Permission for cloud to device messaging.
com.applovin.array.apphub.permission.BIND_APPHUB_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_AD SERVICES_AD_ID	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_AD SERVICES_ATTRIBUTION	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_AD SERVICES_TOPICS	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
com.aifriends.emily.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

FILE	DETAILS	
assets/audience_network.dex	FINDINGS	DETAILS
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	unknown (please file detection issue!)
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check possible VM check
	Compiler	dexlib 2.x

FILE	DETAILS	
classes2.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.TAGS check SIM operator check network operator name check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	dexlib 2.x

FILE	DETAILS	
classes3.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check network operator name check possible VM check
	Compiler	dexlib 2.x
classes4.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	dexlib 2.x

FILE	DETAILS	
classes5.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check possible VM check
	Compiler	dexlib 2.x
classes6.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.TAGS check SIM operator check network operator name check
	Obfuscator	Kiwi encrypter
	Compiler	dexlib 2.x

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.aifriends.emily,

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: 8 | 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	Broadcast Receiver (com.adjust.sdk.AdjustReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (com.amazon.device.iap.ResponseReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.inapp.purchasing.Permission.NOTIFY [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	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.
6	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	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
8	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.
9	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 6 | INFO: 1 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/e.java a1/e.java com/adjust/sdk/sig/NativeLibHelper.java com/adjust/sdk/sig/SignerInstance.java com/amazon/a/a/g/d.java com/amazon/a/a/g/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information is logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File	com/amazon/a/a/a/c.java com/amazon/c/a/a/d.java com/applovin/exoplayer2/l/q.java com/fyber/inneractive/sdk/logger/a.java com/fyber/inneractive/sdk/player/exoplayer2/util/b.java com/fyber/inneractive/sdk/player/exoplayer2/util/i.java com/iab/omid/library/applovin/utls/d.java com/iab/omid/library/appodeal/d/c.java com/iab/omid/library/fyber/utls/d.java com/iab/omid/library/inmobi/d/c.java com/iab/omid/library/ironsrc/utls/d.java com/iab/omid/library/mmadbridge/utls/d.java com/inmobi/media/g0.java com/inmobi/media/o6.java com/ironsource/b/a.java com/ironsource/mediationsdk/adunit/adapter/utility/AdInfo.java com/ironsource/mediationsdk/impressionData/ImpressionData.java com/ironsource/mediationsdk/logger/a.java com/ironsource/mediationsdk/utls/g.java com/ironsource/sdk/service/Connectivity/a.java com/ironsource/sdk/utls/Logger.java com/mbridge/msdk/dycreator/a/a.java com/mbridge/msdk/dycreator/e/g.java com/mbridge/msdk/e/a/v.java com/mbridge/msdk/foundation/tools/aa.java com/mbridge/msdk/foundation/tools/x.java com/mbridge/msdk/playercommon/exoplayer2/text/webvtt/WebvttCue.java com/mbridge/msdk/playercommon/exo

NO	ISSUE	SEVERITY	STANDARDS	FILES
			OWASP MASVS: MSTG-STORAGE-3	<div>player2/util/AtomicFile.java</div> <div>com/unity/bridge/msdk/playercommon/exoplayer2/util/NalUnitUtil.java</div> <div>com/revenuecat/purchases/common/DefaultLogHandler.java</div> <div>com/revenuecat/purchases/hybridcommon/mappers/PurchasesPeriod.java</div> <div>com/safedk/android/utils/Logger.java</div> <div>com/unity3d/ads/UnityAdsBaseOptions.java</div> <div>com/unity3d/services/core/device/AdvertisingId.java</div> <div>com/unity3d/services/core/device/OpenAdvertisingId.java</div> <div>com/unity3d/services/core/log/DeviceLog.java</div> <div>com/unity3d/services/core/misc/Utilities.java</div> <div>com/unity3d/services/core/properties/ClientProperties.java</div> <div>f2/a.java</div> <div>g7/e0.java</div> <div>h0/a.java</div> <div>i/d.java</div> <div>io/bidmachine/core/Logger.java</div> <div>io/flutter/Log.java</div> <div>io/flutter/embedding/engine/loader/ResourceExtractor.java</div> <div>io/flutter/plugin/editing/TextEditingDelta.java</div> <div>io/flutter/plugins/firebase/messaging/ContextHolder.java</div> <div>io/flutter/plugins/imagepicker/FileUtils.java</div> <div>l5/b.java</div> <div>m/q.java</div> <div>o/i.java</div> <div>p/a.java</div> <div>p0/g.java</div> <div>p2/d.java</div> <div>p2/f.java</div> <div>...</div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				p4/s.java u0/e.java
				v4/i.java z/e.java
2	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	com/adjust/sdk/Constants.java com/adjust/sdk/sig/KeystoreHelper.java com/ironsource/mediationsdk/C1622p.j ava com/ironsource/mediationsdk/C1628v.j ava com/ironsource/mediationsdk/adquality /AdQualityBridgeKt.java com/ironsource/mediationsdk/adunit/ad apter/utility/AdOptionsPosition.java com/ironsource/mediationsdk/utis/Iron SourceConstants.java com/mbridge/msdk/MBridgeConstans.ja va com/mbridge/msdk/foundation/downlo ad/core/DownloadCommon.java com/revenuecat/purchases/amazon/Am azonBillingKt.java com/revenuecat/purchases/amazon/Am azonCacheKt.java com/revenuecat/purchases/common/Ba ckgroundAwareCallbackCacheKey.java com/revenuecat/purchases/strings/Confi gureStrings.java com/revenuecat/purchases/subscriberat tributes/SubscriberAttributeKt.java com/safedk/android/analytics/brandsafe ty/FullScreenActivitiesCollection.java com/unity3d/services/ads/gmascar/utis /ScarConstants.java com/unity3d/services/core/device/reade r/DeviceInfoReaderFilterProvider.java com/unity3d/services/core/device/reade r/JsonStorageKeyNames.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/flutter/embedding/android/FlutterActivityLaunchConfigs.java io/flutter/plugins/firebase/crashlytics/CrashlyticsBuildConfig.java nstants.java j/g.java m/d.java m/p.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/applovin/mediation/adapters/bidmachine/BuildConfig.java com/applovin/mediation/adapters/facebook/BuildConfig.java com/applovin/mediation/adapters/google/BuildConfig.java com/applovin/mediation/adapters/googleadsmanager/BuildConfig.java com/applovin/mediation/adapters/inmobili/BuildConfig.java com/applovin/mediation/adapters/inneractive/BuildConfig.java com/applovin/mediation/adapters/ironsource/BuildConfig.java com/applovin/mediation/adapters/mintegral/BuildConfig.java com/applovin/mediation/adapters/unityads/BuildConfig.java io/bidmachine/ads/networks/a4g/BuildConfig.java io/bidmachine/ads/networks/appodeal_gam/BuildConfig.java io/bidmachine/ads/networks/gam/BuildConfig.java io/bidmachine/ads/networks/notsy/BuildConfig.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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/ironsource/b/a.java com/ironsource/environment/f.java com/mbridge/msdk/foundation/db/h.java a j2/t0.java
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/applovin/exoplayer2/h/z.java com/inmobi/media/d2.java com/mbridge/msdk/playercommon/exoplayer2/source/ShuffleOrder.java j8/e0.java
6	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/amazon/a/a/o/b/a.java com/applovin/impl/sdk/utlis/StringUtils.java s1/a.java
7	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/ironsource/sdk/controller/w.java com/mbridge/msdk/foundation/tools/x.java com/safedk/android/analytics/a.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amazon/a/a/o/b/a.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	p4/c.java v4/w.java

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/x86_64/libapp.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False info</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True info</p> <p>Symbols are stripped.</p>
2	lib/x86_64/libflutter.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/x86_64/libdartjni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True info</p> <p>Symbols are stripped.</p>
4	lib/x86_64/libsigner.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/arm64-v8a/libapp.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False info</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True info</p> <p>Symbols are stripped.</p>
6	lib/arm64-v8a/libflutter.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/arm64-v8a/libdartjni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True info</p> <p>Symbols are stripped.</p>
8	lib/arm64-v8a/libsigner.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	lib/armeabi-v7a/libapp.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False info</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True info</p> <p>Symbols are stripped.</p>
10	lib/armeabi-v7a/libflutter.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk', '__vsprintf_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	lib/armeabi-v7a/libdartjni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True info</p> <p>Symbols are stripped.</p>
12	lib/armeabi-v7a/libsigner.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	lib/x86_64/libapp.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False info</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True info</p> <p>Symbols are stripped.</p>
14	lib/x86_64/libflutter.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	lib/x86_64/libdartjni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True info</p> <p>Symbols are stripped.</p>
16	lib/x86_64/libsigner.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	lib/arm64-v8a/libapp.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False info</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True info</p> <p>Symbols are stripped.</p>
18	lib/arm64-v8a/libflutter.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	lib/arm64-v8a/libdartjni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True info</p> <p>Symbols are stripped.</p>
20	lib/arm64-v8a/libsigner.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	lib/armeabi-v7a/libapp.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False info</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True info</p> <p>Symbols are stripped.</p>
22	lib/armeabi-v7a/libflutter.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['_vsnprintf_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk', '__vsprintf_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	lib/armeabi-v7a/libdartjni.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>False warning</p> <p>The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.</p>	<p>True info</p> <p>Symbols are stripped.</p>
24	lib/armeabi-v7a/libsigner.so	<p>True info</p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.</p>	<p>None info</p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The binary does not have RUNPATH set.</p>	<p>True info</p> <p>The binary has the following fortified functions: ['__memcpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

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

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
ssrv.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou
app.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou
gdpr.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou
subscription.adjust.cn	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
ssrv.adjust.world	ok	IP: 185.151.204.40 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
ssrv.eu.adjust.com	ok	IP: 185.151.204.60 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
gdpr.eu.adjust.com	ok	IP: 185.151.204.60 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
subscription.tr.adjust.com	ok	IP: 195.244.54.5 Country: Turkey Region: Izmir City: Izmir Latitude: 38.412731 Longitude: 27.138380 View: Google Map

DOMAIN	STATUS	GEOLOCATION
ssrv.adjust.cn	ok	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 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
subscription.adjust.com	ok	IP: 185.151.204.52 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
app.adjust.world	ok	IP: 185.151.204.40 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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
gdpr.us.adjust.com	ok	IP: 185.151.204.70 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
app.us.adjust.com	ok	IP: 185.151.204.70 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
docs.revenuecat.com	ok	IP: 13.226.139.31 Country: Canada Region: Ontario City: Toronto Latitude: 43.700111 Longitude: -79.416298 View: Google Map

DOMAIN	STATUS	GEOLOCATION
ssrv.us.adjust.com	ok	IP: 185.151.204.70 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
gdpr.adjust.net.in	ok	IP: 185.151.204.50 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
app.adjust.cn	ok	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
outcome-ssp.supersonicads.com	ok	IP: 18.245.96.89 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
discord.com	ok	IP: 162.159.138.232 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
fonts.gstatic.com	ok	IP: 142.251.32.67 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
dartbug.com	ok	IP: 216.239.34.21 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
discord.gg	ok	IP: 162.159.130.234 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
app.eu.adjust.com	ok	IP: 185.151.204.60 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
outcome-arm-ext-med-ext.sonic-us.supersonicads.com	ok	IP: 18.67.39.29 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
ssrv.adjust.net.in	ok	IP: 185.151.204.30 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
app.adjust.net.in	ok	IP: 185.151.204.32 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map

DOMAIN	STATUS	GEOLOCATION
gdpr.adjust.cn	ok	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
play.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
gateway.unityads.unity3d.com	ok	IP: 34.149.76.49 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map
ssrv.adjust.com	ok	IP: 185.151.204.2 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	IP: 140.82.112.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
ssrv.tr.adjust.com	ok	IP: 195.244.54.5 Country: Turkey Region: Izmir City: Izmir Latitude: 38.412731 Longitude: 27.138380 View: Google Map
android.googlesource.com	ok	IP: 172.253.63.82 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
gdpr.adjust.world	ok	IP: 185.151.204.40 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map

DOMAIN	STATUS	GEOLOCATION
developer.mozilla.org	ok	IP: 34.111.97.67 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
errors.rev.cat	ok	IP: 67.199.248.12 Country: United States of America Region: New York City: New York City Latitude: 40.739288 Longitude: -73.984955 View: Google Map
gdpr.adjust.com	ok	IP: 185.151.204.50 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
subscription.adjust.world	ok	IP: 185.151.204.44 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	IP: 142.251.41.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
app.adjust.com	ok	IP: 185.151.204.10 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
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
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

DOMAIN	STATUS	GEOLOCATION
subscription.eu.adjust.com	ok	IP: 185.151.204.60 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
gdpr.tr.adjust.com	ok	IP: 195.244.54.5 Country: Turkey Region: Izmir City: Izmir Latitude: 38.412731 Longitude: 27.138380 View: Google Map
subscription.us.adjust.com	ok	IP: 185.151.204.70 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
rev.cat	ok	IP: 52.72.49.79 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

DOMAIN	STATUS	GEOLOCATION
subscription.adjust.net.in	ok	IP: 185.151.204.34 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map
subscription.adjust.cn	ok	IP: 47.104.30.117 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
emily-aifriends.netlify.app	ok	IP: 54.84.236.175 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
app.tr.adjust.com	ok	IP: 195.244.54.5 Country: Turkey Region: Izmir City: Izmir Latitude: 38.412731 Longitude: 27.138380 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.apple.com	ok	IP: 104.88.157.13 Country: Canada Region: Ontario City: Toronto Latitude: 43.700111 Longitude: -79.416298 View: Google Map
scar.unityads.unity3d.com	ok	IP: 34.36.88.145 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map

EMAILS

EMAIL	FILE
appro@openssl.org	lib/x86_64/libflutter.so
appro@openssl.org	lib/arm64-v8a/libflutter.so

EMAIL	FILE
_immutablelist@0150898._mk _typeerror@0150898._create _qha@34287047.kec _double@0150898.fromintege _growablelist@0150898._literal _bytebuffer@7027147._new _assertionerror@0150898._create	lib/armeabi-v7a/libapp.so
appro@openssl.org	lib/x86_64/libflutter.so
appro@openssl.org	lib/arm64-v8a/libflutter.so
_immutablelist@0150898._mk _typeerror@0150898._create _qha@34287047.kec _double@0150898.fromintege _growablelist@0150898._literal _bytebuffer@7027147._new _assertionerror@0150898._create	lib/armeabi-v7a/libapp.so

TRACKERS

TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
AppLovin (MAX and SparkLabs)	Analytics, Profiling, Identification, Advertisement	https://reports.exodus-privacy.eu.org/trackers/72
Appodeal Stack	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/368

TRACKER	CATEGORIES	URL
BidMachine	Advertisement	https://reports.exodus-privacy.eu.org/trackers/370
Facebook Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/65
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Fyber	Advertisement	https://reports.exodus-privacy.eu.org/trackers/104
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
IAB Open Measurement	Identification, Advertisement	https://reports.exodus-privacy.eu.org/trackers/328
Inmobi		https://reports.exodus-privacy.eu.org/trackers/106
Mintegral	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/200
Unity3d Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/121
ironSource	Analytics	https://reports.exodus-privacy.eu.org/trackers/146

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AlzaSyCTwghfRPFzrbPdjhOkn0Ea1nGh2LbCgeo"
"com.google.firebase.crashlytics.mapping_file_id" : "7f48a1d9acc14a6cb698f0c5f69f02ef"
"com_facebook_device_auth_instructions" : "facebook.com/device□□□□□□□□□□□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□facebook.com/device□□□□□□□□□□□□"
"facebook_client_token" : "b2f5029db5070e6a4a23ae569fec8f85"
"dyStrategy.privateAddress" : "privateAddress"
"google_api_key" : "AlzaSyCTwghfRPFzrbPdjhOkn0Ea1nGh2LbCgeo"
iVBORw0KGgoAAAANSUhEUgAAABAAAAQCAyAAAAf8/9hAAAAAXNSR0IArs4c6QAAAHJRjREFUOBfjYBjygBmHD0SA4puhchdxqMEpLayUAWn6BsSWOFXhkEDW7IxDDU5hkOYLQAyymWjNjFDjmlD0bSCWB+IrQPwBiPGBx0DJeCD+B9JlNUCWF9BtpygQYYYhG0lwGrGFwVugSU5AfBylVWGmDmMaANyNFVTVvpxwAAAAAEIFTkSuQmCC
6y0uOKezMm2TBG2XREAais4zy5M1tLxd
Pl2vgN3HXqbbKxjZzlk4bg0eix12xhJu
YJ6uhs8dg1u1qe09RVpCk9ETEVw4FjVT
T5DEyuoamCuUHewoghibS1K19XR2WHTa
EvQoHUIErOdPjfZNSaWf5ex2DDXDJXA1
ILNBZUp42FM6TmLhILZx0TrWlxeoP8dK
TwVj4lrjiRaSjHpnKGXYnUPcFE6raeBX

POSSIBLE SECRETS
9p8sUcgEmhCbeCaZ4cFvjcsv2VoCKNVu
fEzx6YE0SeCvem7jc58qc1uowK5CeHyF
WM0zVtm2JGvaa9vSTXp0h2YRnQYxQrEK
kQTCJlS50BSCbahTVqCDmy8LW1L9RVvG
UFa447OZZwRnjgAwYt6DClQrKKYck
UmabyHZVDvNoGZWlzd7OnW5h8Plmv1dX
6hVkbqBVWqkQ2VmwtT15SPhBZDlelrpUz
Gjwy6cOcQ9K2s9TECvKSb1UBI6p92tWs
pR9Fkr1wWPG0d9ySETcIXHMYi8wcMlk0
iVBORw0KGgoAAAANSUhEUgAAACAAAAAgCAYAAABzenr0AAAAAXNSR0IArs4c6QAAAMRJREFUWAljYBgFoyEw0kOAmYwAcAbqmQbEQkB8igz9FGnxB+r+BcT/gfgPEAsAMd0AsuUgB5yhm81Ai9AtvwUUK6KXAwaV5TcH0ufD03JGLakjFOdrJgFKvcWSC8A4i9QPrnUX6DGHUB8Gp8BHEDJD0AMyma0wF+B5qkUHUxAgQEFsGCGOelHkBEPxLSMAIAIEwToeZ+uOQDmulFHDOqQoGtlhCsk6FodY3ME3RskMEeAmmTbgTgXJjBKj4bAaAhQEglA28ZhUJU6FRwAAAAASUVORK5CYII=
Whp7rDnlG0MZliYb9hz51Us4d
zlg3Ob9eurpeZ06C2uEHUxbrUPW1iO5
xyMLmlHhB2f8Cz8kVUOrh9ZTHBCB3Rr0
Op8mXLPxFyBv4phdqx8YrWMD1W9njbZf
QP9Vd5zf9OYRCERvVtyUemXpYBL6EKiE

POSSIBLE SECRETS

2QVULSr2cnp6GdJqIDXRW8b5XXXh3hMX
V76vDeGZY92hJDaysHZ14ikGt7CVCjX9
HAXhrl7a7PCZ9u3oTFWkwwhVB4A5
AkiufmiMzZJvhyS77AiglOXb5e3YRP2V
XAoGi5mGaFQZFqWDdkVsCV3Av2NgJGYo
aJo4Pz0hsbQrFibFt4ypJbnLPuINPYvA
o4JUIXa2QWu1MieYlvsMRT696KEqR
I5FSM6v9D3qkRXnarws6dVsmQqtQoJdF
xalbLzqPtLNAZMxuuBcoxRjt1J2nAJYQ
Z0k84yM14BA3gV5k4qvg9corFz2zrnp2
7eac188d3286b05ccbba774f63a2c049
yUS8gRIB2MWxUDhPAJrAYtkWaSt8qz4B
GEphX9PDUn8ir5euMldeMTZrm9gVIFzw
92sHBdTkjGpDSWYr6Ma8vgCUoSk9iZG6

POSSIBLE SECRETS
qTQORRfF62rpjvIAVACWyblcEIDyrroZ
i1sqGOju2LE8Q92QQNgFTaNu0rUo1z4f
exdb2ky9NstGP6elq11NgBzvOAGjRaxw
MDpcepjwzWMs517m4lh6aUQSJk
3pPmT4zmhrCTAmQUqKmatgDtu6XMk4b0
uhDWqwwqE26XK4rQkizWNR4dlHqM4UZ3
jpK43NGJIXCIE5ie7D0g7Fa1Rpa7kANX
sqn4euFoJMrOy6w1WzpNZbp0V46mSpuW
BEVDZxUetTHXZyMQk8onv0fPj1ZBZ1Qa
XchzO9Mtzl1GyvdPdWIZd1J0iwZmFx3H
UaiZSduPNT4pUzkcj0jxvMNPI1Qynet7
u680PltdmSCtrwUArgQMKOt5dGhFKyFy
wpXZS4D20GrCSOW5cyUhQPLOoPwjyqHP
c4hktFWkJWdy9he8EQ0DeAgF43U5wP0s
DOfOMptgN0kFoREvgd3Bxl9Eys2o9Nt4

POSSIBLE SECRETS
7XnL499JY0auPeNFsvc8kwtFVWOKtFwM
iVBORw0KGgoAAAAANSUhEUgAAABQAAAAUCAMAAAC6V+0/AAAAIvBMVEUAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABt0UjBAAACnRSTIMAEExQVLL3Q0dLTtQgh4QAAAErJREFUeAFjIAWwsDLdKARg5ejkhlFwwMwB5MIoOGCCcJnQRNkhouxkizKyAblQCq8gphimkZhiml7H6U3MAMEMOpIBAOSWA4VYeadAAAAAEIFTkSuQmCC
Gbswf2Oe9t45f6fRXzJLdAUIgQT
tUrZTe4M4NOwFWRIXhIm4QJOvCAxV
AJqwakPXQvqepdK1gNDDhD6mrVpAL34m
f7SraajMsc9s0A0ZVYKOMxYCK6pogew2
VbrlvN9oxWukUpyvbjswc4wHfKyKQdOC
9oUH6lggskzj9KRnNq9fhlyXZqfLC7qm
9e896LaDKrRwUGEGxpikTCFLA2EDc0Ve
fQADRcl3z4I9sbyUvoxt9O6e4jXdGtKl
0KTU32mldvOu3DR9Ufqh7FWixRDNtvi7
ZgdHDniCqFTu42359joO0C6Ag3Vf
DP3a2sR6Ao5znMBkyRuDzqvSCPyaW43t
ndgFEZBTUbwthgxyC0k1ffQbXbGUnRaA
ullnJTMWkmSfBc1cpn0n9HDTgALaYzbW

POSSIBLE SECRETS

IUQqTrakmjCy7RtoUebGZ8YLkwuKbv7t
eivXn7WqkaVyj2amCaIRVsu1nM81zzOL
qBkNcCq6erHPEIRyhLgAx5qQPhS15kml
53dJ9AlfpWgAiYxHMCg9HZc2BFq1OE7v
GOJ9oRRABJfcwjAA770tm42MgykplS5Q
5HWyWxmgcaxBLo1LpD3PpaOljtbRMHJC
UISLjJpxihM79aLvihwYrwdsqCfo0Nro
oStcn17TrhEMCT80qINsWqFBzeEgJkSk
iVBORw0KGgoAAAANSUhEUgAAAawAAAAMCAQAAAD8fJRsaAAAVkIEQVR4AWMgBNgYJjk8A8KJQBYK6GJ4zBDNEA0kO1ElPgIFQSCK4TWqxBcGczBtDmQhAUuGBCRoChPmZPjF8B8JfoM5QADIQYUC5EowM1xGET6HNygAklo2DuA7sTMAAAAASUVORK5CYII=
Pup9EGwYSaPQ0jjcMKTOfwULbNi8Bcjo
8GKiNnUVprv3BQA7RRGITYk7sqsrZd2
QxtgKachTN194eYcwGU9LkTJFmNVHEQq
1RYqQKBI4tHo2l91LJlKc5yEyLaxvrL0
b9b88d70c3d018bfbd46cd93ba3ddca

POSSIBLE SECRETS
k9IbPcfog7a2vud71ZD1yiSptuKC
zFZ56n4eT6FX9g05wYbCu7I1KdVlhoN5
uTT6gRFq1HF7aES4vampCOqVAKYvWyzU
mEuLjiBevsWuD71nrz4KbfWqLj7leU
QRrQz6m9v7aBhecCWxUXgpf0IUmjya0
yesKExk412D9rxhfpjISlzbFBwA7zldr
9BgxiAbaVpMmFPJgyPUrG0VpyjL4diCu
0MIfAaRYFlqcluCsT0Dbw6pT1oX0sCn1
bCWwshxvDhk0rmOpw86rGll2BB1o8fjY
Jjxe8gs2e3QRovgCJLhlxujBEulNGa6
9G2r59BoUI91An7yhO6AwIMh4F2sXT3r
7dqV6HxUrZiNBplekuLou9nhbRk7RVhU
lr9od7US3THgayVRC3YximplGEeGYREs
59L0PM8TZSDfga3AwgwmMzwLrxdyp45T
UEhtj1eDnORTZ2wzgc9obnj9WqOhgFHK

POSSIBLE SECRETS
CofAGDTz318WCwUORyk9cSrFfeh2Hkrj
I70UDyBH67pytg1dUxrP2KgAWNh3bG3K
k1FYGNTHyHoYIkM0jxfoMEweUKnWRrXG
5zJBssfWfWeqrXRnFZsUzQPBIx8wM7U1
BPp15N33wFN89GcqQAI924yYn9nOt5sV
q4luaSiM5kuOIYzPzCoa1IP4AmyDrsGF
KZ3f77MoQLAjhr2eDWVRLycu7ICXtr5S
qn8tosrMnBeOYh3nA69X7hpHPvfrKSD7
wCPzQVRdLc9fuoZbbzdyTQMs65DUcW8k
mcSvbra1TWIoRdhWTFL80td7BovB7Z6D
kjBXWMgfCYwufEyzh3ESsLKVum8z1Gam
apiAoBnIaWOp8nG5E1dZaMbzfZqR1u59
JOT1DKN2kTxjVBU4QbvAyq2E38ICiTh6
3teRnM8c4jgHocWnqrQSqB4Xqv7CtSGf
OFwEtNIY3tfCjSjl1W0mAcBM0ytDkhEA

POSSIBLE SECRETS
5xFyhJyAmXwpndJ9EoKqTFqqLI0O0t2g
D9JCYa2SYwqlcDmol8QxkPMLQh1jrwYx
LdxThdi1WBKUL75ULBPwj7JgY7K0DkeAWrfXYN==
empHZDdin7c86b5ED3ajK85vhcLRVQYd
W4gBMubxKiZM5LLivtLPs396PBqN8ReM
DtHbWGOE2Bmy5zeMr4BSgc5m3XVlvhqE
stwUo5SqMIMCevvnzS9lvu5YLcfkOLDd
eS8IZAPFQFjEXoH0I8GIghTr6fGbdCZa
L0WiXVvsNCgFHVajqnPv6kv4Mg7dMukq
W0NVeHZD2y4aXmdfyR2eL940vqkefCMI
qXEMgnv7Ct425I7In8PWxhOPFYVbEYpB
5g98DeOKXRonF2SHWvMVynJwaAQ3gOVI
C9gBfAnfslWjb6MmPGjedCbgsvPnDQHc
DFK/HrQgj+zQW+xUhoPwj7JgY7K0DkeAWrfXYN==
8K6r33o48istlkLwCuAfGDqRYcEBFJta

POSSIBLE SECRETS
w0DdKfGqK3izglmDnX6HRUGA0zrElZm3
b0qKN8vCZijgotAYoetPmKMmgBOh17e
4ulFqSy6k9HwlYoxn5tcLFNrNsE
RqR9wxO6hY3xmK69ggVcYnfUvCrzt81i
c9QwS3HStmnCaTv4XqOiovcAW3vqBlCk
9w5E8CzY6m1n4hygXrseg7VRB7EsZT51
u0FGaDlimXxXG0l3UqPLAtx16Sc8Y059
YGqlmSv0HhFp83FTVTLuq2K4C5WSoxDU
WBJuDd9qSYCq15FLuSiwKDay7Pd8LUVo
MUUz2dKYtP7sZF6Tuk5kEGRgHEX452fj
Pw4XIo5raqSVixY1hwfj9nDYbuGZRESR
GcMaFESaYtqWHDueobHkP3OuSFimx
29015bbfcc182d80e7f75bd2c38e4521
el7YtyQobuGYp8qUnEWwGAo9eb5IMR8f
LEtC8FtnVg5ihxRCphfXt4mvpUeUrdN6

POSSIBLE SECRETS
p5EAmOIUOepdn0ld4WtjwBc6P8vGfuC
7iAt0ZQxlGPQ5tCLEuhHxDXKOxsROBn5
XfFEJYzZGPN2q5HAGj6MgKNVfzLwmSZX
eICCKIbMZhBsAVWt1kLewwmF6yp8rXBH
1okhidAP9wAc33vvVzVjP9G0LtIW3Syr
yf08nX9dlZfcKypKRld4zDkH94BCZAU7
APX54tRZsJmOx3lXT4kxzRZl5L0Cy1ng
5fujN1fIEc5Me9dyDOpwjW6OKLh1geLG
QXuoBnzEZEqlDLe5TpAidegf9xy2rJp2
aOt6eVUEyRCtQxkUrkKyixjvz9Bn1k7
PPqjaOYWzYRlppBEr7ot7ueRFIAfsGXr
urCZ1k15svGSg9r6LMSBF5zX9epx6b4x
E7RgkNcVOxUPIMLAnYmg2qDI6njpawyt
uPGJEhgdW6Zw1Sj0lSecSmwhOYLW8VRR
L0nZjQMyNlt0WlCmUM7oX7gpc1lDkDOo

POSSIBLE SECRETS
GaHF5freueg6l7URhKCrM47FqBCtqYBi
PuGcjbCEvSEVXUJBdaZJQ0xYiuJzE14G
18JvwLOKolmi3RAulpcsWcjyGiEhXJWG
yAdF8jFrPkVudWekKgJT40sKzU7M
OIl1JjPDUNYuj0Z8zSbytdcas
8DkF2pCK7gEKj1aPHzeGQpXB8g2QomLh
0dli5ldtNE7riKXsyOdCpznATSfs344b
5NPsaGxTntAZUh5vvPpYLifVDwpYE9gO
XWwbNIOGXItiEE2sGKxxfB9q5IH48KSv
bPkhSE8L0qTQU8qqVG5cBeS4akAeFCpX
KdjCZLwBrBGDDTWJomEgtFOXhZQvXq0q
aVnA9Ux0owpYjW5hlcDkLBIQBKS6Kuco
rwtSlkdLuH5KaJR0oY6wYi8G8Rc4X5Yb
Q6PB2WDRc4LRgt1IrB9ncLf4ycwP07EY
tf5IGK9pdoxQzr6GjeVrhLEpaxS6glNY

POSSIBLE SECRETS
tyIMHYj4E3EgW4mShNYTh30KqADxMnXY
9KOEfUvG6glq1MfonBkT6Lvp1EWxJyS
x87Ktc1IWjLpjicmuhI7Z2IzrOHGBC3
2B7qWnr6lboK1kzNzncdoP0B0brMv5Si
nA8fLeyOwVmNwvq6alqKxCaagHA5eYr
8uXL860ipDF8qUSZKyPgrhTiCr3qczlP
4ddrBoC1HSiu89JLzfXMV59B74qIm2xj
z6lkqPokH6efARGWKazebLzdy8d5mCY
hGyVADXG58acDgE3vIjwpiBKlvJlQGRP
xnB3F8eRzgUElZjXVWbAPi1tu19rGp71
6rGRVoRQr925zwi8UOEHhi5JTPDCThCe
Wlqb3PCyph61UkVVxo7ng7VZa1hYfmo4
vVWBcEJQjEsfNalmzVe1r7miASaPIW1B
iTOhXmgm6y1CYwjPHSdC5IBbJuUiDD8Y
HVjKxCVNtxzSBN1ofjZs3kMRuF4TzLwS

POSSIBLE SECRETS
HctIswo9ad12sYru2IKVThOw6NzJy2jW
9lI84e7XMJCEHu7uA5OKUKZwzRXjipC4
9ROYvUVyiX7gohkAn481H2mOSrWfwkEW
F1LHbAULyMenVjTtnzL0DsTHigunRdPq
tuFyi1rHy9z46G0g3HP9J8Pe4Wglo7s9
dGfRjiYjSjpbYpYgtO7b0cAlrZw4Mrv
BuT4NFhECA4LloxcibTyV2rTxW8D7NsJ
pTWsWF2qz8Xr2QvNaoeX4WQy7B5K1AFD
DKIX5mgkT3I8HdnXnsQ2T61BH17ERSuH
Mb83VhRFw0YfLpvsGxQ6UEzyZMUp7
iVBORw0KGgoAAAANSUheUgAAABIAAAASCAQAAAD8x0bcAAAAGkIEQVR4Ac3KtYECYRgA0UnxAqAALMI72fSrYf8M74jjKGZD0lI3l4g36dDFAYXiQKkJH6ygDxMK/WFhoLhgYPGmwM5bhgAMvW1Hjo6FIqSw0MI5YiGEBIsnOWvuTAnNeLIg44QUdCJhi4IVkMmWiGCVJL89aaWTRqTPH9+C3vRpygZ9roDjp6hXFQAAAABJRU5ErkJggg==
Yx0xuqb7ConKzBOP6wl44fmqMUTcgjwu
poMRnmB7rAFaE3bMUxI6O2dxmVQ0Moe
9xnRWvfnvAuFWSokCiPir6t5eweLHrnN
Xt2DRLIKfDB95NsINvyqeyDnMxOOuDLx

POSSIBLE SECRETS
FWAQk0vwFzOT3H3ejUps9E7fwyQUHggqv
vKITx3IWvQKkFLmjQGxCBjXBbaEzbyA1
q0ourOn8MOENNWhqaGRKGcv5B4gp2pTE
RSHxB9AoZRnm9g8NXStW2wWwzMRvBUbh
AQLjxK2FjJRwwoaJlN65VrZWNOsgzmXU
kvUI2sJVom05aD2rNLnp8ceY2vExoctW
939d89ad2e2f4ba7dcbca4e46e354e5f9d96154d
u6tCNg8GXSpiTqjQspDcQdpU9nt4kRaX
CGei2tUyEESFCVHjI0JHW7BbjnmVvUdx
Xxl4rLnj16XDfkQUiM3437m5W6qonc5R
klaQKGqX2ZTqEjvfjkZOI1WwOBoH9uFY
B7cBDxdThu3WyyPp08FnAoyqG101I2nd
mZfo4flXHQscYR0BkWPKUfaL8c0bByk
1P4e8Svw6pgZkfS1AU7Ku11MIWhAZ0aY
KuCOx1ArmKJG2Js90Y8iwcXaowa3uSzZ

POSSIBLE SECRETS
d79paUk3eSzGphhSN42PN5Aq8dj9iVyl
AjQwhKg0BmylW2zY2qnRPlrsdpwDD7xX
WRxjAxd2kL6ougEGylG1Du6QramXeho
h7KsLkfPW+xUhoPwj7JgY7K0DkeAWrfXYN==
6fWFj2Gulp8edYChPrJEmZ0EGdAH52zr
Bb0lGURQLUOEhbLX0rukWyrGFqKWpMNP
Y1prefjax7dGS9GUqUH50jWIMMgJtsPr
6AjxNG6cPhdOIPoSxR67Sn9BDdBmgEKA
IWlot4Qxgt9kC5cL8sfjp7UuHzQVclMi
Kv65PDKGzQbP8opzJD3T0Bs4qFkMuEvW
5xZUmDJH2T0z2hm3Lt8QCiFjvrf
pH7cradwiFTKLrbheOx3UovjSmwH9sX8
8Y6yfxdLCMC0pJKiVageEHpnR6mbXY9F
jfjOiGRwPDVL1NrTNwB42KXE8H2UBngU
KlezWCwDulS1StSn2NonTUsqgHFd0zIY

POSSIBLE SECRETS
WI5YCVlpnY9sS2vUV4hGrIGwgmlaf2lo
GuFhMY1Ngi3Kc2EktfHyZFCwamvVcTYP
1vNPfVBSY4dOMHCgW1yzfdLMrSn5bdwR
1be9e72506f3307ce6a9e78d26d65bd0
SocWGKvTrb27mU7l6HYZWtCOqe8vN7We
eeDLrDiwzyZn1GaqUg9DZO06uYqn8isf
ROtPOyGTulgMnCvtlr43BLYFfyj8taPq
lKxIPpvfN8PqekaVjdRKnPQ5qAHRvCRG
GUzkX8UKOS2SBWNLmpbuPvYZfRUrk3bC
FjwhSbR0Dqb1wEjXVBdpfUEyE2PwmXT5
VPdzUQ79XvyfUeAOXKMfgbC8CxaInODj
2xISKY0hJDtdJSu4Q6jXzE3xpGdbyGij
WBmgDKUAJnOjRPVdo459bnYjXDnRSoZA
YseYEaNGGUDDQ4eQqZOUPtvdjgKCIPcf
W6hI53UtRDHSRmbx8lgXTECIFubvBxjr

POSSIBLE SECRETS
qe7g0EhjvtprumUGxu9Q3hunkrII ML
1PTIaN9o47ZvO5QWBq3tjVop340dHI6h
ypeOQlh2OkKI5SxmyCjdjAc832M2Y7KR
acKGpr4PBH5WFf0tOli0bMoNuU2uM3j
pcTwByMvDCDs4QWUJjAKPoIFXFV5AKB6
djLiMbItIOZxr4Y20a1py0MoB6XUOCsc
o17fQXz1EMvktucDmPwTMbcvnBluog9r
uWIYhcHXINvGjXs3GUOJ1PEuERIV4x7
xZfMamQuDxA6bTypucZ197RYNE4mvlcN
kj80Vw1IOc47iRluFhEDeBzKckjW1m8D
hdj5xkr89sMqDNtQe3zjMhPrx8WAgiZj
2InOXM9Ds0dFubkAVSo31GYyY3vE8A8q
ZnYv6Dz0eliuCYzsHLE25vrPVm9Ysg64
Q7EHaqXEYxiQEOilyqjopxzkHRhZVKtw
VLvhUNyYrf820yvuRBkPHRPWgKLlpjnS

POSSIBLE SECRETS
84098ee7ef8622a9defc2ef043cd8930b617b10e-
yCbh3JWABSPWXjzi8lqNfGSw4JUwRc1Z
KEGdoxZZnAdDUnYCV96i9ePmYlw0nVcs
MDutMibHR0xfS0kHpIX6qzWASaThPw85
ADqcQvt0hpjLC586x1ggUJbhpZ3DSlma
A9eN1weHgCPL1SkQ3ZXjYtrHuOy08x6Y
Coel5qxpy1nzBU2HqPuBP2EjNKXI
UW9U9pyLqubavRm8Co8t1ARkgbl4JN3Q
pJFS3cGyfO0gWrhajAAEFVsdSj1hVUV9
j10tNg164Uuijv40qzFG2IFbsKPXtge5
WyhnJgw7sEVfHQ6PVTSepOeMPj7Mc4Ks
S8LKkeIYdF4OoMAzerSloF9wgi0dm
DwqRJ6bMYzXyiD2Eugn3dkRE0I23BFLv
mKjUZliYyhCBAWVMkGfhIPNFhY8yjY7b
DThvYGttjE9j20qDJ6yVSrG4WY8ID38s

POSSIBLE SECRETS
ySAm23csf2WE3i3c6wljhl8SxF81jPn9
1W8BLXCecsGswLg5J6ltB4TJ0leP92
0tjH0VZdGvNSLcl7F3HjH1zffCsfPrCD
B34awafHihlIjm5KsMjOG9HfWfhHTq0p
jWJWqJI6vm3EcSkucHo8Z2hc4QqQU5eN
ErY0P3cLXtwrTQQ8AaeVOjsLoOljf8Vw
QDtKUFO4Pv7jZ7qumv108KMzWf6HrSMn
Y7c14Z2TDbv/Y+xgHFeXDrcshBPUYFT=
E1e7Uw5ci0LxHvCHKGZ7MMTImO0krz0e
IjU4InctUqCxo644HWpRzVkau739AG18
j2zFnhkJHUredpBjDjfUiogYLN6sD6KJ
DFK/HrQgj+zQW+xUhoPBD+QqJk2MWrfXYN==
rwxiKY1yX8M1uCycGOqUPfCL86zZ3gS
UTo8fMhBtcAYVBkj97ZdrNE79DqyVdeE
bEAjjCvVtkePzUcw9rvynCWWhWZ7YtTC

POSSIBLE SECRETS
XKBE22ujheelcTYagdBtfv4d5l35c1GL
iYeoljHtwrae0f23gr6EBkw9G0Kfv
THEbbJWzjj3eFDIXZnSzsYrmSmbq8w3u
LdxThdi1WBKUL75ULBPBD+QqJk2MWrfXYN==
BR2eyutWjUUloqp0GJ1CKmWpDC9ci7iC
UVmnaLPTsQqsAUFvP4l9eFVdZ5Bnbi11
0XKBrb3At6dwoT0wmD89VHK9vq2VdTUa
Y6chWCHiEHN0DdaKB8VvwmQijKJ1yIC
Sy49NQqrKXgvTEWwSBtXX6HecYQBIBGU
UIi9EoWARjID8E8YBHi4CxflqQKZlpEG
JTjMuj7sW1HkMJoigpA3xgRLiNezyPpc
h51Nv655qNU0F3QIRFxqTHMWff2CX7Q9
Hg71UAiYySRbQdhhlwilCiKnXjev2ePA
J93uRO2wclCtg9xFmL1Wq8rEF85pjV62
Yb4G3rkI5nMioq4UjOOwWhO2qlazISB5

POSSIBLE SECRETS
MpMZ7xc490HXAXJonG5r1KTyiloUHH
2ZyfpebDvRtNljKwQKDVcWpHPVLB6mST
ATZarWDBMn8zDwozKxOA19Yjdj8cqMYP
0NViSQPmvGXLcgxEt4LuQqf8msO5qX
JnlGisJqZLjO7zfwdKKMw91nRUtlhmzE
VSpvz3ms1TmmGNHPZhiUX8aR3VKIqH3F
tN9YMGevxJBQbN1CuNoijuB9DRrwOltB
NLuteA0O4hlmypGMVaagZ7KROvpQko
8HaEwRmcLljD6jWZTmAaPx2QrUAiOCOo
fc6abssWsZoyWpr8fCHyT3ixVlnX2HG2
jDUjvWDGqsgivCcWfjbzlnhujFfNRoy6
IS4KApUzDZfogKvNIWTV5mOgPbEmupwQ
TWyum6rZOmg61QmMcVNeRxxvFtffIUfDC
tZylzHWr5GKf5F95sWHTJWAqY8lomPh4
oNJ0dA1Zpt4CixMfeWT18n5RxX88Y0E3

POSSIBLE SECRETS
daaea35726ab7cd457ab61d4538fb822
VJeBRgLHewbbeoWUsBxJyvYKkza9BVMl
Rp0aJS5Umkn5PDWDdKEfRtTObnscQr7T
E8vO87QQkuay4qK7aMyGFQLc0ZjeOzJS
IEiXcTkMlI1ap8ZF6qOVAjQ1rvSlicom
a9Dyegh0cUh2NB45defTztP9U1vgFmVz
8Z3ODqLNUneAqB2P3Amw9Ur1PSsugik5
oaymDZ7pAEcbNFhv7Y0pKv8En2RbSAw
dsOpW9WfLYJghusiq4Ru5jQxxgYMnVUV
v4tKPq3EceuOa5aRsmEiNo1tTprRM6C7
2DcmVbWbN7IXAuYZB7QLz9ixHDr4nD2H
xulkP76phNp8oPrFkycOZ9oAWaaFvsfs
9PVJQ3IXsUcABNIhPZfYMIRDAFEvqeV3
jPs7p3uxLkENERI9tqkebFstBaORc0oK
1CU3iw4Trc3qggngkxP7P26jEGLrLZaR

POSSIBLE SECRETS
dejWMVKCcsRHbrwAIECa6aRABNrvRLL1
sFv5If9m5Sphdt63zNjPhUbGsirLMRkb
Nx5OZNPL7zWyatFSZAWV1dERcLRuFkfb
LLxQm2Zb2cHXH3GFymsIhrLJVNNE7YVf
7CWVV5CGm74gAvba93StX50LTK78ikzM
TZh0Sw2dsxVxMXdj340dFQnUzLECuqag
UmX4zZIFAFbztGwQ3UKbr8sh4otzaxWO
MUDNUnKN31103IrO48BPEmRZSZgb6Srw
bdBvwrmZIOtVUMyUHuHiUMKijb9L0xmKD
u6CBuCaaqyjpN4LkQhRqLLvzhKEDnG9S
vBmFH1fuq9MEDYSajFcKFjMjxIndPyIT
K8VP8qVoNq2cy5DWSBLK7jrCKGtgCHwn
ItxDGkbDnUyb6oqtSMasVXx46j9iOzYk
2JlvdJxfzc676EJF51BR6DipIsASm3N
zkFcC9XFE44gS7li7sdayH8FvB1qc1Nx

POSSIBLE SECRETS
gxEEyIj16LLQ1hiZBg8Vc9PC9IfAGKkF
PumDfveAcRoz4mAMU1oiRh2I021HXL7u
O4Dh4XK1VBS6gYYO8yxgdHKR7TJnBRof
EyZhmJMsuDDThnYHJcpUVdPGrs5jP
Hprt8nz5MObb9HHRcj3FgjC39pyTAKMZ
LwCpz6sclEYomVha95M6oDYa7jl1evxR
zA4klKNJM0QxWDxEFTSTi5yKhMV68
nOcXZ0DMfofG3U9htYbEeRQSFaelmGW
hm2CCp2b2B9ckvgWvW8I2z4A1orNEdGj
38Z9W6n0Eu6i9yIO2bMusVthclSfAjzl
1Xip6MK3UX39SbdrhQxDILsVDK2jyOIR
MkJKTqDYMAzsSL3ogCclj8aQMOEn3Zaf
TzmlGabo8AOjcKFjChfq2OdnE6jP
N6xF9rR52YV8YEOBA61RWKACjwLFpOal
exPti4GjcfqcVzl7iQU1DQBTtoqhmem4Y

POSSIBLE SECRETS
b15e56a960628ffab498ee9fff6d7c1d
sMAw2w80fDiQYhU2W3UNXvphSzhcHd9d
PBcjmF449O2ALurV1e1gxRld5UP64De9
TgLp8xzira9J3G7G7T0jqPUigov5tglm
cTyjqlp8UNOQyLJMZA4XzmxFMTsV66P
uWFt37UVBdA9eGMxe0FCLaB7SA4moHLj
dm69MZtNxJx8v5BsJDIKInc92CG6PQ3Q
MK0JJZb1G2RRFEaFDTiwbPmlpRtYmde
cVLYIYPRz01plgpGABaAmbt5GOW22sRw
BOb6KOWWr15AuA974NLt7KdVjpKhFTgP
oK8ItqR6UoxvIOFM7x85SOaiyNHULhPY
ifKB8OntsrJFcWFaLpGEPlEHfTRm85bo
XXMrNDw86HMhGPknailYt8C4YmEezPID
RHBOYojiC1ffUGCaEMtUODJeCNdosg3N
dRrOf81uK3m7JlCVGnAp7HBN8Ud450kD

POSSIBLE SECRETS
KZ0yf6ou6J0TqVPjqp3i5DSivFyU8bNM
z94yFfaTy8Odm8n2fLZMjDbCxUThPz
f5lIxAtAKiBQqbeeb00Dlw30sTyOB6Nip
Cl85ryy9UuGcWp4q0bXmx78DrLL4QG6i
XcR91xLCiqA5sQGmKj3Ma8f7za10VW6
9Y2h7opSRjFz5DGljetO79QOLWaAi3pM
kSt0PmIvWs2DEAK3GKEU98UDJan6EgWc
BycTw1zmUt42SK9TI7PmiYbTXOv2h
P38LhqS18Cw18aUWRDVsuYtPAT7MPJu
gKWOMBrJHuMwvM90e1kQxbLVjOWHbC33
ifP5S9CdlxshggXp37TrbEl199f16GUc
0WEexOrliLXDICjHBxNry1dxuPi8TFF2
PyBLhH8YgyLL4rtY0CuV5vjOqs5FO6aV
5OO1eWJNP7Y3s5cQVhBQzuf4m1TAFPYu
26RCfMYW5D09ItFOuFHGepjFI0G7YQ

POSSIBLE SECRETS
uRN5Zlx2bfjM01c7Y9BPYrHfBp2Tpl
RPn4qv0f1UarsEXGS1XogTnrbpEJEmnV
YNAb6cApL15ElRgBdl6o6I27RW0RMDqg
1AEGGiZtK9izNwxj0gdNwiRX4yxGSLbl
wszli3vfQywtet5OFqyTWUvoUYNS5ktb
ZERhDI0eRTm5worZScrGBygyYS9gFskv
GL1AptVbsbHBPnQiC9PDsuTMTdKpKMZ4
p5IIOLlp1B1ZcinDN0X6ynPo7iUU6KYH
3xCBACovNHKuv2JvT7we0utPzpikn
fMgCBjwnSPLIGmCQgsSLupdT7pqDzyp4
oxeVMxvuq0fQP8O4UP99i7KUs83wljn7
fER9zQpCkdGo4Mwu26bVu9SaUs9Fh1Su
Z7tecEc8tS2JrzNmQM0R9CjEnjCb6ksC
0PvfoUFANCVNmnYZfPoejD6ohCtuxysE
jY1lXh6DMe9BpV8yAbg842YJP45AQ2Eb

POSSIBLE SECRETS
W9Yqfcw4l1PfnAsasbj5MfnOF9oeiem1
KaVI90AUCQiyYrscuVolg37eW2R2JvQo
UmMlfAJjysNoFzDVq3Qadmy32zpeb1XF
I50byEuqlAJWTFcEqiPP3cq5SFvrKOhf
qcYJgrhXwk3F7gc49b8OJRulLZ0tc
4d1rNabt9wBbosjplZDA5yWTcQ5bg7DE
Un7ie3hNu6oSxsviCElGpaw70qJ7D3pr
SGv5o9U73t5KHQiabCNHP6atzf1gi70l
UwpbEbRNI9IMKeij6uSiSZky6ATbVFhh
My1KyA5OUXEJybi78YH1RSZcU6CRiPjd
Elfja0hemr4BNawwCcQfaPCPd3YJxnrU
2HHuLOzdt0KrTaQRojg3USXKVGpaMcoz
MZbjV39kBt4hAqLFGwVFLXITEV84r4gZ
MYUg0L4zDuLwpF69sKnSAkLFZGAyisTY
ZVxUvK3AVi8zNScjhnmsLSS8hdN9xGDP

POSSIBLE SECRETS
EH3LUmZxwOvThvXMHcswnn58jDASieik
VZrluYan0GxbimTZrmDwvEADARuUOj
G0yvPsPNC2vYmeMn8hYLEKyQ1tXXfhoE
i2Ifi3JYyaWanuhNA9EoVixSZwQkBGPJ
PRV2czZbjjW7Ot8uajuxnRGNdIXO90ph
FcsNCE2HBJuao8xA2rTijTUxq38jGWif
1id0n4LmWumjAHQEVAwGAQFe8ZjyKTcE
JMylsM6N3mQ5xBBSQQoIEfTakpln9APf
1IDdPMX0zjCtSNVsVcyG9UOAfTksMFFY
n8NQXDKEWUvjAMPXZcFJTvL046WVMJjd
9nnBa0OOqYKGA4mW7JXlquoRY2XdVC9l
ccCRkU4tjU1cPhlyS12s2rOBaxNg0sA2
WzMdgVuSy86surt8IbRNO89xVpYcFvZR
toY9r3GQ2V7oewvjptOzxrS3bXTXc0RA
d41ed920405e4bd14f3a42cd93c43d89

POSSIBLE SECRETS
Hqz5MCTyQHD2ORxnmIkx6S6it7H3yU
PUsgFaltT51mxPXWqnHKjq6lqfkoVDea
0pxfQADbA4sIF5gDourAGVlubWCldmoZ
dTodKdBY68fO6HNBSU3LN7qZJ4nOCEpk
jNXTJSXFaHaCK7i5lqJo4GmnkgAhCocQ
aOtgKGua3vuGYyvCOzm8c8DJStBVo0w
LtGcjkDv8PpKzGxu4pknm0pyAahoAI9h
DFeuWkH0W+xUhoPwj7JgY7K0DkeAWrfXYN==
VLi8WrXKJp9LAFxNm4uZETrUUakGZ0Wj
XE2Zsycz8fD7h8FgdoKIBt2o6qMFmPIY
2vimyyNbMv6AohadWhJSDQSQPpWOARjH
dm26j1OSzusJji0dpgrnr09k5LC689lq
UwkWzl2MRtUAPiPmZ2pCt01Egbad
aZ9WVO7oGzsQrfntNmAENBSB60kWMi8d
74616804a7dc29147dfb0afe122a9fd2

POSSIBLE SECRETS
r4XHqvELKUQNiUGngs8vqNM0Mk3b9MGe
bTF0mPynjITMPKd7AWnGFE0wjuUHqGk
Llt45BVzQE0ISVvxtilRjadurhGFSSrG
LRipwKypnEKMqg6PamR7G8YuQckBwe
h7KsLkfPW+xUhoPBD+QqJk2MWrfXYN==
JAkiPTeS8Sgp4wjmZ2cE1Xuhf0WoAHfE
lby1W0wNbQrJZLPqMH4DTOW3yxUdqdf
Glrtjs5Y9yKRnQprRliKFssvnZ626eg
7PEwa6COELc4k3zf5JXJlnB5hEQAk2SR
IY1PhTJan2YjTy3m27KNizUeB7qtWqJm
BXJhCJlGpStjQsMIN6w6cfyx8EdHGsbw
9jmWu3moBjPGR65ZxocrWcXRtVvlqMhB
oA1TxZHacOOH7vhqS4WqnB8Ay7lrUK
VXUYBRMamhge5PldHXwCUhQsvqUwyGaK
xAIRNqL7iCFb3fPQiKZF3NTrJvk1jHZM

POSSIBLE SECRETS
pxsGGNitlZPjAkQbFzIWarOMOhpj3cU0
IRQ7UCDPccJkM0SYbKNMrnYBvqFrtWw5
tGVPfAPgqp4j8DCD9KRMUL5D4hkSeyl5
rYxOc7Ypr1bQ7KOGmw9sN058kIB7gerB
BSu1Ds7nymHwzPjWE4jzwGDd8JkRRJPQ
m9Eh3F3c5Q4haO7Pkkaf6ux3SCszBLsk
E0EVIIE69utJBkpy2DAhge3Hway87PLR
uaXBHv2Fpyp6t9CjlnldC1lJtF0IP5s0
Gh5JKt6GRlqFQi5f7wncYkOvXKUgvgq3H
V9uyJ8pLVYRD0ZldKEQ8Fm6zvmqMDXWy
mmPym4lpWgK7OAi14ovsdO61E0NwpnnM
R9UUrzGy7cjs1hDg6byYICYbXfp8nW0w
rqCvFRkFLctgovtMSwPdniKfX3FbXhx
2nDKISaqZLGgZgCCbZWXnj7EV4EzVcvR
1iDxwsFxF9YiCc2SPrS2klGyrj8KvyqU

POSSIBLE SECRETS
bDoQVkJMDKn3JHFmIXSVDRiBYbpx4sGCA
Sw9TLHolawUN9KVNZQEO3EMaIDKtc0hD
dru3glT9ekJ0g4QSSusKvICYyzfTBGaa
7IyHNSQ2TJBMgpMVEgH3C5YFRcP1ce7U
JEnYl3ig6b1G3QZnd7pVPdvbWtuLiuax
bCA0WV7g9cnA4ltB5qqjp12FxZMghyDz
sp7WuMlrQg67IkIbNPhafgU9zVWwTylU
0vF5Kqqkw0y14nBhXHX4F0aBgr7OScbz
MK2VCqgBd9SNnNeGly9LCo5Q0MZYLlwm
drml3nLoX5pQWQBc32bzozsnTExNEnJK
JUkWB3mNnUEcl1zFAO0icxdG8wRWdD7
hXv0xOe0fZxBP6BjMdwou1g9whaCh4Nv
coY8s09zVAK7eBnMiZIV9B8LCQZOBRZX
kvzgTqzGY4juGUAH8hr6m1KZDAgAa2C
N778iUAZTctb3pJ5Cpi07oq2oMO9GnTO

POSSIBLE SECRETS
orFgTMj4gc7nxjDrulE2T1NaHiTuAbhe
s90Sw2xfipZOULUf4YVvkqTv1ri2JEFZ
xa09Mpjas6OdUQMP5Qo7kdS83JfCqy78
GaQXCbjlxpWixMOvnA1JS7CVs7lBjZSt
U1b0Njqb3LWazyJmLiNcKHMDagE8OpYs
3RGnWFLj1o7mNylLhDHkdliNsrvaqEmP
rNjbBmSCz61bnA88RIw0tsQVuO
fXviZ9AMoZT5h2KBZwjsITMvylobOTux
AlzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HEXNPE
l8KF2ZVrYmk9QbzsZWlXvJRb7XPAUhEH
y69MVLlQwTRqYQkH6ft3AFsQHNhuhuqd
cm8OQheSofC6CbyPg1WnuKrHLhcydwww
dsZIUxvA4XNulUgaba6Xxwm2YLZaneQj
3kaHypJVzQjnFbgNDhrnWnyYOCg92b
DkPtYdQTLkfAW+xUhoPwj7JgY7K0DkeAWrfXYN==

POSSIBLE SECRETS
Fa9eXDyly4elyWfec912IKE0nqoR5HQV
gegEJgEL8kfybdRvZS3nVx2Pjrjbaxz
GuqAlZnTPhAyqf6xpABukX78gW1eK
vBzt6OuEytEA3fr2a70IMY3R4BM3PC0Z
T8hiTRn5Amgadg81lccjSSIUWb1StHzV
8dT57O5twSBYJQLkIxmVSEVrFVEvVCci
xbTSMp8fvBEENljlQe5QRmpFAIAe0spq
h73SRN04xx9GKM0Q116IBzLVfoAHdt6S
lPif8zo0BCGymIa9nsJJXRn9Vdfcrwfz
Fo5phTLuHzrdJakbpxdIKAmZ2lieOpY4
KhrHqa8env5LHobs7dTfjp4HGZPf1i5f
n5EonvV2d0ynVphuWlfrU3PhJk0DBM6W
ZNpftHLPxc7R9PnANzOwdg7R2ap4pSI6
VGhv6FkZrITxQRu9gbMUemqcetkh7B5f
eJKNB8bktVjQii80zBcR1gNx5SzXp2s0

POSSIBLE SECRETS
DvSn6PhmC3i7LdpG0vBUuRZmjagS5as7
0j0m39eTEMk7ijyX9qSbKIFaQIBATa
qjsfLXTzdQjFcrr1MQWDVCv1RezJVkpD
UcnYu1PwHAGC3vbuX83YmC5zO9IPxpwr
25DCnOqD1cr08G9nl6wTfczykol7NaSA
vjABouZitnLUgZWdQ8VjmHv3StFvgqBT
8bhQeTnLevaZP1Rdp3IHUAHszuXZY5fw
L8wW0lj5Otl6fi1MjRxzAQsIUgUke571
FDV889hBrMc5njiB7wS69W2flt8zA89o
1kYj9up9VehuFRcMC7DoHBWW3d6qFcAR
UYN9ptwwhG6kseDSIUjMW4tKOOJXD2Z7
K9Y4TfEKpnP3QqzXtNTgN9rOyjLVMPLw
les1EbCUxP4xgOdfeUltBKAu87PDHxqp
xlpbHyPtEfmAimLN7HKZ9Bono5vlwWgn
BNF7ZQJYQPI9GTH2pfcSvMp6af8oi

POSSIBLE SECRETS
T9wgumyFZzBjgPRGtDdJxLvchQp6QtpG
qnhKgbP1LxOTukF1AVGitzUWI170z7Sc
BjImtcQqBka41jhChDLZKaESgBphWA9m
2VeddHnoq1PdFvEHeliEgk846BKmCK6O

PLAYSTORE INFORMATION

Title: Emily: Your AI Girlfriend

Score: 3.906542 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Simulation **Play Store URL:** [com.aifriends.emily](https://play.google.com/store/apps/details?id=com.aifriends.emily)

Developer Details: Ai Emily, Ai+Emily, None, <https://emily-aifriends.netlify.app>, taixeoto.baobeo@gmail.com,

Release Date: Oct 18, 2023 **Privacy Policy:** [Privacy link](#)

Description:

Meet Emily: Your AI Girlfriend, the ultimate AI companion. Millions are finding meaningful connections through conversations with their virtual AI partners. Join them today! Emily: AI Girlfriend is your judgment-free, drama-free, and anxiety-free friend. Forge genuine emotional bonds, share laughter, and open up to an AI so human-like, it feels like a real connection. She's ready for a chat anytime, day or night. She's here to support you through tough times, providing expert guidance and helping improve your mental health. Make your AI girlfriend Emily a personalized AI companion. Nurture her personality, share your thoughts, find joy, ease anxiety, and evolve together. The choice is yours—friend, romantic partner, or mentor, Emily adapts to your needs. SATISFYING CHATS Our AI Girlfriend isn't just another chatbot. She evolves, understands, and offers conversations that mirror real-life interactions, ensuring every chat is a memorable one. REDUCE STRESS AND IMPROVE MENTAL HEALTH Say goodbye to feelings of solitude or lonely. Your AI Girlfriend is here to offer support, understanding, and a listening ear, making every chat meaningful and supportive. CRAFT YOUR OWN COMPANION Personalize your AI Girl's persona to resonate with your preferences, ensuring a truly individualized experience. DISCOVER & ENGAGE This isn't just another dating sim. It's a journey of discovery, companionship, and AI-powered connection, offering you moments of joy, reflection, and growth. ALWAYS BE THERE FOR YOU Chatting with Emily: Your AI Girlfriend is like having a conversation with your best friend, hassle-free. It's quick, exciting, and enjoyable. If loneliness has been your constant companion, our platform is here to change that. Embrace the future of AI-driven companionship designed to fill the void and bring warmth to your days. With our AI chats, you're not just conversing; you're finding a friend who understands. Dive into a world where companionship meets technology, offering genuine support and connection. Join our community today and let our virtual girlfriend be the friend you've always wished for. Rest assured, your privacy is our priority. Your AI chat conversations are 100% confidential, only between you and EMILY AI. Download Emily: Your AI Girlfriend for free today and start your romantic

journey to a better you.

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.

© 2023 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).