MobSF

ANDROID STATIC ANALYSIS REPORT

Complete (18.3)

File Name:	com.abbvie.patientapp_115.apk
Package Name:	com.abbvie.patientapp
Scan Date:	Aug. 29, 2025, 6:53 p.m.

App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	8/432

FINDINGS SEVERITY

🐞 HIGH	⚠ MEDIUM	ℹ INFO	✓ SECURE	🔍 HOTSPOT
3	13	5	2	2

FILE INFORMATION

File Name: com.abbvie.patientapp_115.apk
Size: 75.76MB
MD5: 6096d13804bfcf90d19c548d91defa4b
SHA1: 3cee98f21b81819be8dd5cc4cf6262c850677b5a
SHA256: 77a698a59c0a6c2100e7d25bb841cc5f3120fc3dbfe162f39f217500b293fdaa

APP INFORMATION

App Name: Complete
Package Name: com.abbvie.patientapp
Main Activity: com.abbvie.risa.ui.activity.OneAppSplashActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 18.3
Android Version Code: 115

APP COMPONENTS

Activities: 48
Services: 14
Receivers: 16
Providers: 7
Exported Activities: 1
Exported Services: 1
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=Illinois, L=Chicago, O=AbbVie Inc, OU=MCOP, CN=Mathias Ringhof
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-04-11 04:52:13+00:00
Valid To: 2041-08-27 04:52:13+00:00
Issuer: C=US, ST=Illinois, L=Chicago, O=AbbVie Inc, OU=MCOP, CN=Mathias Ringhof
Serial Number: 0x38457c6d
Hash Algorithm: sha256
md5: a48ad03161d39883adba541d6493c123
sha1: 904cd838885c99241f512c6b4c42399c5c464eb3
```

sha256: 51928663bf9f5a9436d0755e970e420cbc2c249b2102323f9df1380801102831

sha512: 886237643954bac100be759f163232257ff5cad620b2f39f25d625071d9b1ae04301d1381aba32722c8c5310c8dcdb45012f47799447355db262af29f42e2045

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: a681b7b518f9613c5ed3151acd737efdcbcf22b9633cf7af122a39dbdbae2b4d

Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
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.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.FOREGROUND_SERVICE_REMOTE_MESSAGING	normal	allows foreground services for remote messaging.	Allows a regular application to use Service.startForeground with the type "remoteMessaging".
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.abbvie.patientapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

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.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes3.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes4.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
SIM operator check
network operator name check
ro.kernel.qemu check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
<tr><td>classes5.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.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.abbvie.risa.ui.activity.OneAppSplashActivity	Schemes: https://, completeapp://, Hosts: abbviebrandconsumer.com, welcome, abbvie.onelink.me,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.abbvie.patientapp,

NETWORK SECURITY

HIGH: **0** | WARNING: **0** | INFO: **2** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	qa.abbviebrandconsumer.com q.abbviebrandconsumer.com int.abbviebrandconsumer.com staging.abbviebrandconsumer.com abbviebrandconsumer.com	info	Domain config is configured to trust bundled certs @raw/brand_api_ssl_new.
2	qa.abbviebrandconsumer.com q.abbviebrandconsumer.com int.abbviebrandconsumer.com staging.abbviebrandconsumer.com abbviebrandconsumer.com	info	Domain config is configured to trust bundled certs @raw/brand_api_ssl_old.

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: **2** | WARNING: **5** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	App Link assetlinks.json file not found [android:name=com.abbvie.risa.ui.activity.OneAppSplashActivity] [android:host=https://abbviebrandconsumer.com]	high	App Link asset verification URL (https://abbviebrandconsumer.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 404). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
4	Activity (com.abbvie.upadac.ui.activity.UpadacNotificationHandlerActivity) is Protected by a permission. Permission: com.abbvie.patientapp.COMPLETE_APP protectionLevel: signature [android:exported=true]	info	An Activity is found to be exported, but is protected by permission.
5	Activity (com.abbvie.patientapp.ui.activity.TransparentActivity) is Protected by a permission. Permission: com.abbvie.patientapp.COMPLETE_APP protectionLevel: signature [android:exported=true]	info	An Activity is found to be exported, but is protected by permission.
6	Broadcast Receiver (com.abbvie.patientapp.receiver.AlarmReceiver) is Protected by a permission. Permission: com.abbvie.patientapp.COMPLETE_APP protectionLevel: signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Broadcast Receiver (com.abbvie.patientapp.receiver.OnBootReceiver) is Protected by a permission. Permission: com.abbvie.patientapp.COMPLETE_APP protectionLevel: signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.
8	Broadcast Receiver (com.abbvie.patientapp.receiver.NetworkChangeReceiver) is Protected by a permission. Permission: com.abbvie.patientapp.COMPLETE_APP protectionLevel: signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.
9	Activity (com.abbvie.risa.ui.activity.TransparentRisaActivity) is Protected by a permission. Permission: com.abbvie.patientapp.COMPLETE_APP protectionLevel: signature [android:exported=true]	info	An Activity is found to be exported, but is protected by permission.
10	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
11	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
12	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	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.

NO	ISSUE	SEVERITY	DESCRIPTION
14	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: **3** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/adobe/marketing/mobile/internal/eventhub/history/b.java com/adobe/marketing/mobile/internal/util/g.java com/adobe/marketing/mobile/media/internal/C11810j0.java com/microsoft/appcenter/persistence/a.java com/microsoft/appcenter/utils/storage/a.java com/microsoft/appcenter/utils/storage/c.java l1/e.java net/sqlcipher/database/SQLiteDatabase.java
				D4/c.java E0/a.java F4/a.java H4/c.java N4/a.java Q/i.java Q/y.java c0/C10819a.java c0/d.java com/abbvie/patientapp/customview/SymptomReportAvatarView.java com/abbvie/patientapp/ui/fragments/appsetup/l.java com/abbvie/patientapp/ui/fragments/appsetup/S.java com/abbvie/patientapp/ui/fragments/appsetup/ViewOnClickListenerC11293f.java com/abbvie/risa/customview/RisaHomeCardLayoutManager.java com/abbvie/risa/presenter/registration/d.java com/abbvie/risa/ui/common/a.java com/abbvie/upadac/ui/fragments/registration/B.java com/abbvie/upadac/ui/fragments/registration/ViewOnClickListenerC11748f.java com/adobe/marketing/mobile/services/C11834a.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/i0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	com/airbnb/lottie/utils/e.java com/appsflyer/AFLogger.java com/appsflyer/adobeextension/AppsFlyerAdobeExtension.java com/appsflyer/adobeextension/AppsFlyerEventListener.java com/appsflyer/adobeextension/AppsFlyerSharedStateListener.java com/appsflyer/internal/AFa1dSDK.java com/appsflyer/internal/AFa1tSDK.java com/appsflyer/internal/AFc1pSDK.java com/appsflyer/internal/AFd1aSDK.java com/appsflyer/internal/AFd1eSDK.java com/appsflyer/internal/AFd1iSDK.java com/appsflyer/internal/AFd1kSDK.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFd1pSDK.java com/appsflyer/internal/AFd1qSDK.java com/appsflyer/internal/AFe1lSDK.java com/appsflyer/internal/AFe1wSDK.java com/appsflyer/internal/AFe1zSDK.java com/appsflyer/share/LinkGenerator.java com/jakewharton/disklrucache/a.java com/jjoe64/graphview/GraphView.java com/jjoe64/graphview/helper/b.java com/jjoe64/graphview/l.java com/microsoft/appcenter/utils/a.java com/salesforce/android/cases/core/internal/http/a.java com/salesforce/android/service/common/utilities/logging/c.java com/wdullaer/materialdatetimepicker/date/j.java com/wdullaer/materialdatetimepicker/time/RadialPickerLayout.java com/wdullaer/materialdatetimepicker/time/a.java com/wdullaer/materialdatetimepicker/time/b.java com/wdullaer/materialdatetimepicker/time/h.java com/wdullaer/materialdatetimepicker/time/i.java com/wdullaer/materialdatetimepicker/time/q.java f8/b.java l1/f.java m1/C17595a.java net/sqlcipher/AbstractCursor.java net/sqlcipher/BulkCursorToCursorAdaptor.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/DefaultDatabaseErrorHandler.java net/sqlcipher/database/SQLiteCompiledSql.java net/sqlcipher/database/SQLiteContentHelper.java net/sqlcipher/database/SQLiteDatabase.java net/sqlcipher/database/SQLiteDebug.java net/sqlcipher/database/SQLiteOpenHelper.java net/sqlcipher/database/SQLiteProgram.java net/sqlcipher/database/SQLiteQuery.java net/sqlcipher/database/SQLiteQueryBuilder.java net/sqlcipher/database/SqliteWrapper.java org/joda/time/tz/b.java org/joda/time/tz/h.java r4/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				r4/g.java r4/C17829a.java z0/d.java
3	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	com/abbvie/patientapp/access/D.java com/abbvie/patientapp/app/AppController.java com/abbvie/patientapp/manager/l.java com/abbvie/patientapp/receiver/AlarmReceiver.java com/salesforce/android/database/e.java net/sqlcipher/database/SupportHelper.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/abbvie/patientapp/app/AppController.java
5	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	I1/g.java N2/d.java com/abbvie/patientapp/data/e0.java com/adobe/marketing/mobile/launch/rulesengine/json/e.java com/microsoft/appcenter/channel/c.java g2/C17128b.java j3/C17189b.java v3/i.java y2/C17879a.java
6	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	Z7/a.java com/adobe/marketing/mobile/services/ui/d.java com/appsflyer/internal/AFa1vSDK.java com/appsflyer/internal/AFb1kSDK.java com/microsoft/appcenter/http/h.java org/jsoup/helper/b.java
7	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/adobe/marketing/mobile/assurance/E.java
8	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	H4/a.java
9	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/salesforce/android/chat/ui/internal/filetransfer/h.java
10	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	v4/C17842b.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
2	arm64-v8a/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__strlen_chk', '__vsprintf_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.
3	arm64-v8a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86_64/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
5	x86_64/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__strlen_chk', '__vsprintf_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.
6	x86_64/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi-v7a/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
8	armeabi-v7a/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
9	armeabi-v7a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
11	x86/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
12	x86/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	arm64-v8a/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
14	arm64-v8a/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__strlen_chk', '__vsprintf_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.
15	arm64-v8a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	x86_64/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
17	x86_64/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk', '__strlen_chk', '__vsprintf_chk', '__vsnprintf_chk', '__memmove_chk']	True info Symbols are stripped.
18	x86_64/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	armeabi-v7a/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
20	armeabi-v7a/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
21	armeabi-v7a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	x86/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
23	x86/libsqlcipher.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
24	x86/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/adobe/marketing/mobile/assurance/C11769a.java com/airbnb/lottie/network/b.java com/appsflyer/internal/AFa1rSDK.java com/appsflyer/internal/AFc1gSDK.java com/appsflyer/internal/AFc1jSDK.java org/jsoup/helper/c.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/b.java com/appsflyer/internal/AFa1rSDK.java org/jsoup/helper/c.java
00109	Connect to a URL and get the response code	network command	com/adobe/marketing/mobile/assurance/C11769a.java com/appsflyer/internal/AFa1rSDK.java com/appsflyer/internal/AFc1gSDK.java com/appsflyer/internal/AFc1jSDK.java com/appsflyer/internal/AFd1fSDK.java org/jsoup/helper/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00112	Get the date of the calendar event	collection calendar	V3/a.java com/abbvie/patientapp/customview/LoadingDoseView.java com/abbvie/patientapp/presenter/appnotification/h.java com/abbvie/patientapp/presenter/calendar/g.java com/abbvie/patientapp/presenter/injections/g.java com/abbvie/patientapp/presenter/medicationreminders/b.java com/abbvie/patientapp/presenter/profileupdate/k.java com/abbvie/patientapp/presenter/registration/j.java com/abbvie/patientapp/presenter/registration/q.java com/abbvie/patientapp/presenter/symptomlog/B.java com/abbvie/patientapp/receiver/AlarmReceiver.java com/abbvie/patientapp/ui/fragments/appsetup/ViewOnClickListenerC11293f.java com/abbvie/patientapp/ui/fragments/appsetup/x.java com/abbvie/patientapp/ui/fragments/basefragment/g.java com/abbvie/patientapp/ui/fragments/login/H.java com/abbvie/patientapp/ui/fragments/registration/n.java com/abbvie/patientapp/ui/fragments/updatemedication/f.java com/abbvie/patientapp/utils/M.java com/abbvie/risa/access/c.java com/abbvie/risa/adapters/C11372d.java com/abbvie/risa/customview/RisaStartingDoseView.java com/abbvie/risa/presenter/activity/B.java com/abbvie/risa/presenter/activity/C11397c0.java com/abbvie/risa/presenter/activity/C11424q.java com/abbvie/risa/presenter/activity/I0.java com/abbvie/risa/presenter/activity/N.java com/abbvie/risa/presenter/activity/W0.java com/abbvie/risa/presenter/activity/x0.java com/abbvie/risa/presenter/cards/C11527w0.java com/abbvie/risa/presenter/cards/G1.java com/abbvie/risa/presenter/cards/M2.java com/abbvie/risa/presenter/profile/k.java com/abbvie/risa/presenter/registration/p.java com/abbvie/risa/ui/fragments/more/C.java com/abbvie/risa/ui/fragments/more/M.java com/abbvie/risa/ui/fragments/registration/L.java com/abbvie/risa/ui/fragments/registration/ViewOnClickListenerC11584i.java com/abbvie/risa/ui/fragments/reminders/d.java com/abbvie/risa/utils/s.java com/abbvie/upadac/adapters/activity/C11628w.java com/abbvie/upadac/presenter/registration/h.java com/abbvie/upadac/ui/fragments/activity/ViewOnClickListenerC11706q.java com/abbvie/upadac/ui/fragments/activity/w.java com/abbvie/upadac/ui/fragments/login/D.java com/abbvie/upadac/ui/fragments/more/personalgoal/e.java com/abbvie/upadac/ui/fragments/more/personalgoal/t.java com/abbvie/upadac/ui/fragments/more/r.java com/abbvie/upadac/ui/fragments/registration/O.java com/abbvie/upadac/ui/fragments/registration/ViewOnClickListenerC11757o.java com/abbvie/upadac/utils/o.java

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	com/adobe/marketing/mobile/assurance/C11771c.java com/adobe/marketing/mobile/services/C11842i.java com/appsflyer/internal/AFa1hSDK.java com/microsoft/appcenter/utils/d.java
00004	Get filename and put it to JSON object	file collection	B4/c.java E4/a.java com/airbnb/lottie/D.java com/appsflyer/internal/AFb1xSDK.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	M1/h.java com/abbvie/patientapp/customview/C10895z.java com/abbvie/patientapp/customview/S0.java com/abbvie/patientapp/receiver/TimerNotificationService.java com/abbvie/patientapp/ui/activity/HumiraISIActivity.java com/abbvie/patientapp/ui/activity/HumiraISILinkActivity.java com/abbvie/patientapp/ui/fragments/basefragment/g.java com/abbvie/patientapp/ui/fragments/d.java com/abbvie/patientapp/ui/fragments/menu/n.java com/abbvie/patientapp/ui/fragments/resourceandsaving/e.java com/abbvie/patientapp/utils/M.java com/abbvie/risa/adapters/H.java com/abbvie/risa/presenter/cards/C11447b2.java com/abbvie/risa/presenter/cards/O1.java com/abbvie/risa/ui/activity/RisaISIActivity.java com/abbvie/risa/ui/activity/RisaISILinkActivity.java com/abbvie/risa/ui/fragments/g.java com/abbvie/risa/ui/fragments/more/O.java com/abbvie/risa/ui/fragments/v.java com/abbvie/risa/ui/fragments/x.java com/abbvie/risa/utils/s.java com/abbvie/upadac/adapters/w.java com/abbvie/upadac/ui/activity/UpadacISIActivity.java com/abbvie/upadac/ui/activity/UpadacISILinkActivity.java com/abbvie/upadac/ui/fragments/b.java com/abbvie/upadac/ui/fragments/base/h.java com/abbvie/upadac/ui/fragments/more/w.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/assurance/AssuranceExtension.java com/adobe/marketing/mobile/services/ui/g.java com/appsflyer/internal/AFa1tSDK.java com/appsflyer/internal/AFb1xSDK.java com/appsflyer/internal/AFd1jSDK.java com/jjoe64/graphview/GraphView.java com/salesforce/android/chat/ui/internal/chatfeed/viewholder/o.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/abbvie/patientapp/ui/activity/HomeActivity.java com/abbvie/patientapp/ui/activity/HumiraISIActivity.java com/abbvie/patientapp/ui/activity/baseactivity/a.java com/abbvie/risa/ui/activity/OneAppSplashActivity.java com/abbvie/risa/ui/activity/RisaISIActivity.java com/abbvie/risa/ui/activity/RisaLoginActivity.java com/abbvie/risa/ui/activity/RisaMainActivity.java com/abbvie/risa/ui/activity/RisaRegistrationActivity.java com/abbvie/risa/ui/activity/baseactivity/a.java com/abbvie/upadac/ui/activity/UpadacHomeActivity.java com/abbvie/upadac/ui/activity/UpadacISIActivity.java com/abbvie/upadac/ui/activity/UpadacLoginActivity.java com/abbvie/upadac/ui/activity/UpadacRegistrationActivity.java com/abbvie/upadac/ui/activity/base/a.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/appsflyer/internal/AFa1tSDK.java com/appsflyer/internal/AFb1xSDK.java com/salesforce/android/cases/ui/internal/features/shared/h.java
00013	Read file and put it into a stream	file	B4/k.java com/abbvie/patientapp/utils/C11361s.java com/adobe/marketing/mobile/internal/util/c.java com/adobe/marketing/mobile/launch/rulesengine/download/d.java com/adobe/marketing/mobile/services/internal/caching/b.java com/airbnb/lottie/compose/t.java com/airbnb/lottie/network/g.java com/airbnb/lottie/network/h.java com/jakewharton/disklrucache/a.java com/microsoft/appcenter/utils/storage/b.java okio/D.java org/joda/time/tz/h.java org/joda/time/tz/j.java org/jsoup/helper/b.java v4/C17841a.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFf1iSDK.java com/appsflyer/internal/AFf1lSDK.java
00036	Get resource file from res/raw directory	reflection	M1/h.java com/abbvie/patientapp/receiver/TimerNotificationService.java com/abbvie/patientapp/utils/M.java com/abbvie/risa/presenter/cards/C11447b2.java com/abbvie/risa/presenter/cards/O1.java com/appsflyer/internal/AFb1qSDK.java com/appsflyer/internal/AFb1xSDK.java com/appsflyer/internal/AFf1lSDK.java com/appsflyer/internal/AFf1nSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/abbvie/patientapp/utils/C11361s.java com/adobe/marketing/mobile/internal/util/c.java com/airbnb/lottie/D.java com/airbnb/lottie/network/g.java com/airbnb/lottie/network/h.java com/appsflyer/internal/AFb1xSDK.java com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/utils/a.java com/microsoft/appcenter/utils/storage/b.java r8/c.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/D.java com/appsflyer/internal/AFb1xSDK.java
00024	Write file after Base64 decoding	reflection file	com/abbvie/patientapp/ui/fragments/resourceandsaving/prescriptionrebate/n.java com/abbvie/risa/ui/fragments/resources/prescriptionrebate/p.java com/abbvie/upadac/ui/fragments/resources/prescriptionrebate/n.java com/airbnb/lottie/D.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	M1/h.java com/abbvie/patientapp/ui/fragments/basefragment/g.java com/abbvie/patientapp/ui/fragments/menu/n.java com/abbvie/patientapp/utils/M.java com/abbvie/risa/adapters/H.java com/abbvie/risa/presenter/cards/C11447b2.java com/abbvie/risa/presenter/cards/O1.java com/abbvie/risa/ui/fragments/g.java com/abbvie/risa/ui/fragments/more/O.java com/abbvie/risa/utils/s.java com/abbvie/upadac/adapters/w.java com/abbvie/upadac/ui/fragments/base/h.java com/abbvie/upadac/ui/fragments/more/w.java com/adobe/marketing/mobile/LocalNotificationHandler.java com/adobe/marketing/mobile/services/ui/g.java
00132	Query The ISO country code	telephony collection	com/microsoft/appcenter/utils/d.java
00100	Check the network capabilities	collection network	com/appsflyer/internal/AFb1xSDK.java
00125	Check if the given file path exist	file	com/appsflyer/internal/AFb1xSDK.java
00089	Connect to a URL and receive input stream from the server	command network	H4/c.java com/adobe/marketing/mobile/assurance/C11769a.java com/appsflyer/internal/AFc1gSDK.java com/appsflyer/internal/AFc1jSDK.java
00153	Send binary data over HTTP	http	com/adobe/marketing/mobile/assurance/C11769a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00003	Put the compressed bitmap data into JSON object	camera	r4/g.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFf1iSDK.java com/salesforce/android/chat/ui/internal/filetransfer/a.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFf1iSDK.java com/salesforce/android/chat/ui/internal/filetransfer/a.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFf1iSDK.java com/salesforce/android/chat/ui/internal/filetransfer/a.java
00187	Query a URI and check the result	collection sms calllog calendar	com/salesforce/android/chat/ui/internal/filetransfer/a.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFf1iSDK.java com/salesforce/android/chat/ui/internal/filetransfer/a.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFf1iSDK.java com/appsflyer/internal/AFf1nSDK.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFf1iSDK.java com/appsflyer/internal/AFf1nSDK.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFa1aSDK.java
00163	Create new Socket and connecting to it	socket	com/adobe/marketing/mobile/services/q.java
00014	Read file into a stream and put it into a JSON object	file	B4/k.java v4/C17841a.java
00028	Read file from assets directory	file	com/abbvie/patientapp/utils/C11361s.java
00012	Read data and put it into a buffer stream	file	com/abbvie/patientapp/utils/C11361s.java
00202	Make a phone call	control	com/abbvie/patientapp/utils/M.java
00203	Put a phone number into an intent	control	com/abbvie/patientapp/utils/M.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/129718811736/namespaces/firebase:fetch?key=AIzaSyDZl32CkrU5jz3pRuyWvrcPVWDjBbKgxKQ. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE
Other Common Permissions	6/44	android.permission.CALL_PHONE, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
api.abbvie.com	ok	**IP:** 159.180.132.240 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.849998 **Longitude:** -87.650002 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sinapps.s	ok	No Geolocation information available.
abbviemetadata.my.site.com	ok	**IP:** 23.62.226.162 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
privacy.abbvie	ok	**IP:** 172.64.146.17 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
pay.google.com	ok	**IP:** 172.253.124.92 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.rxabbvie.com	ok	**IP:** 18.238.109.42 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
mobile.events.data.microsoft.com	ok	**IP:** 52.182.143.208 **Country:** United States of America **Region:** Iowa **City:** Des Moines **Latitude:** 41.600540 **Longitude:** -93.609108 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.zetetic.net	ok	**IP:** 18.238.96.105 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
blobs.griffon.adobe.com	ok	No Geolocation information available.
www.humira.com	ok	**IP:** 18.238.109.70 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
device.griffon.adobe.com	ok	**IP:** 13.224.53.13 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
firebase.google.com	ok	**IP:** 74.125.136.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sconversions.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
simpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
developer.android.com	ok	**IP:** 142.250.72.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
federation.abbvie.com	ok	**IP:** 159.180.132.75 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.849998 **Longitude:** -87.650002 **View:** Google Map
sgcdsdk.s	ok	No Geolocation information available.
www.abbviebrandconsumer.com	ok	**IP:** 159.180.133.178 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.849998 **Longitude:** -87.650002 **View:** Google Map
docs.google.com	ok	**IP:** 173.194.219.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
qa-enroll.humiracompletepro.com	ok	**IP:** 23.253.24.210 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.850029 **Longitude:** -87.650047 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
www.abbvie.com	ok	**IP:** 172.64.152.49 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
sars.s	ok	No Geolocation information available.
skyrizicomplete.com	ok	**IP:** 159.180.132.176 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.849998 **Longitude:** -87.650002 **View:** Google Map
sregister.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
abbv.ie	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
www.rinvoq.com	ok	**IP:** 18.238.109.15 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sstats.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
cloud.crm.abbvie.com	ok	**IP:** 13.111.176.41 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.788464 **Longitude:** -122.394608 **View:** Google Map
in.appcenter.ms	ok	**IP:** 4.153.25.42 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.skyrizi.com	ok	**IP:** 18.238.109.28 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
sapp.s	ok	No Geolocation information available.
abbviebrandconsumer.com	ok	**IP:** 159.180.133.178 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.849998 **Longitude:** -87.650002 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
provisioningapi.paynuver.com	ok	**IP:** 52.167.82.65 **Country:** United States of America **Region:** Virginia **City:** Boydton **Latitude:** 36.667641 **Longitude:** -78.387497 **View:** Google Map
sviap.s	ok	No Geolocation information available.
www.skyrizicompletecdrebate.com	ok	**IP:** 159.180.132.181 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.849998 **Longitude:** -87.650002 **View:** Google Map
assets.adobedtm.com	ok	**IP:** 23.3.85.32 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
svalidate.s	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
completeappsupport@abbvie.com	b3/C10807a.java

EMAIL	FILE
completeappsupport@abbvie.com info@speaknetwork.net	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Adobe Experience Cloud		https://reports.exodus-privacy.eu.org/trackers/229
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
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
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238

HARDCODED SECRETS

POSSIBLE SECRETS
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b>□□□□□□□□□□□□□□□□□□□□□□□□"
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b>□□□□□□□□□□□□"
"facebook_client_token_prod" : "0abd6ac267fd663476ad81699216e677"
"chat_dialog_end_session_positive" : "□□□□□□□"
"chat_minimized_post_session" : "□□□□□□"

POSSIBLE SECRETS
"chat_minimized_post_session" : "□□□□□□□□"
"chat_session_ended_by_agent" : "□□□□□□□□□□□□□□□□□□□□□□"
"google_crash_reporting_api_key" : "AIzaSyDZl32CkrU5jz3pRuyWvrcPVWDjBbKgxKQ"
"chat_session_button_transfer_initiated" : "□□□□□□□□□□"
"chat_minimized_post_session" : "■■■■■■■■■■■■■■■■■■■"
"google_api_key" : "AIzaSyDZl32CkrU5jz3pRuyWvrcPVWDjBbKgxKQ"
"chat_session_ended_by_agent" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"chat_dialog_end_session_title" : "Αποχωρείτε;"
"chat_end_session_content_description" : "■■■■■■■■■■■■■■■■■■■■■"
"chat_dialog_end_session_positive" : "□□□□□"
"chat_session_ended_by_agent" : "□□□□□□□□□□□□"
"chat_session_button_transfer_initiated" : "■■■■■■■■■■■■■■■■■■■■■■■■"
"chat_minimized_post_session" : "□□□□□□□□□□□□□"
"chat_dialog_end_session_positive" : "□□□□□□□□□"
"chat_dialog_end_session_title" : "Elköszön?"
"chat_dialog_end_session_title" : "□□□□□□□?"
"chat_session_button_transfer_initiated" : "□□□□□□□□□□□□□□□□"
"chat_dialog_end_session_title" : "□□□□□□□□□?"
"chat_dialog_end_session_title" : "Închideți?"
"chat_end_session_content_description" : "□□□□□□□□□"
"chat_dialog_end_session_title" : "الوداع؟"

POSSIBLE SECRETS
"chat_dialog_end_session_title" : "□□□"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
"chat_end_session_content_description" : "□□□□□□□□□□□□"
"facebook_client_token_test" : "0c4e57b1a45e41d37c68c975c9f078c5"
"chat_dialog_end_session_title" : "■■■■■■■■■■■■■■■■■■■■?"
"chat_dialog_end_session_title" : "□□□"
"chat_session_button_transfer_initiated" : "□□□□□□□□□"
"mdtp_deleted_key" : "%1$s□□□□□□□"
"chat_end_session_content_description" : "□□□□□□"
"chat_session_ended_by_agent" : "□□□□□□□□□"
"chat_dialog_end_session_positive" : "■■■■■■■■■■■■■"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
vpqgk7W2OO4+emKKnTSxckIsP1c64LGVSWcdsnDvr3w=
9rXsTdb/WXYONX554dN5CJ2eqpcy9gFPMPi8uAjaHTA=
796aa514-1278-4187-9b8b-c8829ad35278
1VeJuVnEfsh9S8+TnOEDCfIzscTATtniwvJaQ7/W6I8=
o5W1eROpLyVNcsDGW3Y0lGc2x/V+mDPvMXouv3gbW6M=
joxZSCFIfSio2J1Z0g3HMtlcDGNvogfMyrj1e2b+qPNv6DXnDVXfwkgCXW9zFWFC
c56fb7d591ba6704df047fd98f535372fea00211
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
9a04f079-9840-4286-ab92-e65be0885f95

POSSIBLE SECRETS
hhtrMjcGMTQSGdrv1+l2gakNTe0Pfchc8VT5kRHtsehlafuJ8JEE4iewNV4y5I/U
9b8f518b086098de3d77736f9458a3d2f6f95a37
e2719d58-a985-b3c9-781a-b030af78d30e
4ccb3abe1b5b12844ef24f35da2efa8e
AZwRbSS9Tjg/vY6NNyDfd3mU35mZBbQduzRpliDRt3qUNjlKylmreq0JkiCiO6dF
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
C6OPKdOx6rUdfDdOmaUimt8yM1FrOv7bKCITdJ0Uo74WwXDfvXouJ4oz4kHBjTSk
01360240043788015936020505
115792089210356248762697446949407573530086143415290314195533631308867097853951
w1mRpvC09hSNbQ10UvFXagm2P4TWR/T2KztJ+buPFQZnRnjxpdFVScAm9trUP6jM
7d73d21f1bd82c9e5268b6dcf9fde2cb
Cv/m6MvBjdOit7tT7cC+xPCpFEqovwYj4XIOcXUxCMs=
k8GEQUoJxJPI/0jAlfeUix8QD7WaaXAfMcSQAzrpgrU=
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
hwvIMOeohSBrCWT4pVkQok22g/l0cZbbqOTmNbjObWwcwhLlaFMNibQmd2cIB1Vb
SfaCE2ReDSQ3+KDKcvA6SSrX7nuWYsM/FN3ZFmlH0dA=
115792089210356248762697446949407573529996955224135760342422259061068512044369
fd321157e963b1e842e425135b5c562f
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

POSSIBLE SECRETS
z3i9M2k4RJ/f7GArNBcGbUcpUFpuRmLev6S20UO7Vqs=
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
WWJPV1FUOTlpMDA5RTBma2xVbzBnWW9ZSWZ3M0hWWU8=
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
Qzg4V09lQUFoa2duZ05ZR0hWZ1dUTE1CSEdEem5qbzY6cFpUQUFUU3ZKSkV2MElQVg==
cZ2qwY2ZIJRch325gepGJtH7dQ9IcqmfWvaHdfiFi6Y=
JLulXGPEHVwHK+0FG96HP9my+NvwpTQbwIaIZrjn9OU=
nVNp1WYfnkUt4CgZM9ftj8WNocg8ldySiFlqCJaJia4=
Cv0JAL9ptzpRvgIi9AFTFGn0l5MhpPgpRN4VfZybymKMuiqBn9AG0bgJaX/QotAk
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
RKC3mFMqGi7xOgQ7s39JMoZe9bnzGCFipcdUUf0vlgHDkBg7SvMkVmBGpwLs06ia
uJ6tafbdnitpIiJcEDt3zh4lzBZEYeFsW45S60suhbKyZNy2K2MuNEbuksualim4
cc2751449a350f668590264ed76692694a80308a
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
3LpdW89cIASEFv5WvS5ZDEWsiVGQitP33SL3WZgJ6zE=
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
1tXSieficgPhud4YihA+CzunTIb+yA05iyb1BkAzMoc=
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
iJiFXDBrMwFOGpG8WmWNKc3sGwXbWv8N6fPQac0mMm0=
lsjUo68NMWNsPUz4dBIEYtWAZHRXaEljQLBgt48XQs4=

POSSIBLE SECRETS
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
6vt+8E5GP5AwoxquDM0Y7lVJzS23/VCjNo5D8xB8rgAaaF6IhToGZhlIAUkgigHl
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
tVSI3GZQAGRITfe/VNiB0JAqJe5Pfq0lPruET3IJQ2F3N6dl8hPg+ZOAK3nXD45u
1yJaDnXEM3em29nHb3kYjIOvpW6Mkce5Fji3syGd7T0=
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748494A4B4C4D4E4F505152535455565758595A5B5C5D5E5F606162636465666768696A6B6C6D6E6F707172737475767778797A7B7C7D7E7F808182838485868788898A8B8C8D8E8F909192939495969798999A9B9C9D9E9FA0A1A2A3A4A5A6A7A8A9AAABACADAEAFB0B1B2B3B4B5B6B7B8B9BABBBCBDBEBFC0C1C2C3C4C5C6C7C8C9CACBCCCDCECFD0D1D2D3D4D5D6D7D8D9DADBDCDDDEDFE0E1E2E3E4E5E6E7E8E9EAEBECEDEEEFF0F1F2F3F4F5F6F7F8F9FAFBFCFDFEFF
r0MNv9zqwvoUwASL1pBJjOA1OkDa8Kcs5NaA6VOkJEI=
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
5BhEc19mhLCb3gixLpO/usqpdcrz8iDHUvKRNr8tUAX9rUzF0wog6vEOJrftvcpW
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
6CWPidOWJZFxRWI8V7yi3OiMbOhIWZX/jTayTGRwqCM0W8dtKHQOPe60TuQicfhG
3071c8717539de5d5353f4c8cd59a032
8Xr1ilYJHo+oWZQAYAG91DIHBuqEmXK8yHtxL6KkyfU=
sjYkfzJTuYKxh1jvZaP9n5dx9JGmzJotOUC/vdvgi4M=
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
uxIInGM9FQ+1gujg5A7z9IJxIqStl6tvqqzSbuEi494=
Ls+ZUCEdSGy+47NpfWc5WNy2WCTB2lhysvWY8PCvkdyqiw8HkO3XVSxwPIsY4tvv

POSSIBLE SECRETS
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
WWJPV1FUOTlpMDA5RTBma2xVbzBnWW9ZSWZ3M0hWWU8
X9PgbTHLX0FFxbl3gdPDuVwcglfXy5CDrzo8siaVNaH+OIJ6JI34Wu3QK5rLega4
23456789abcdefghjkmnpqrstvwxyz
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150571 51
HeBkX9XaSpC6sV82I6X2HUgm82vH8VhIWt26LGkrI3A=
sdX902x/AS9226TxUXaqji9wP1uHqRQA8nkg2YMN1TcruTTaw008l9z5V3jZGjLO
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504 0a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d33363031303732333133 33345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504 0a130b476f6f676c6520496e632e3110300e06035504 0b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773114301206035504 0a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d01010405000382010100 6dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
XFxH1z0dBuMDP7aWA+P/3WKwW9qr8sC2ASjEfciaKHfSLryjCNl4cmJgfsh2Tylb
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
B3EEABB8EE11C2BE770B684D95219ECB
tPxcLkiesd8JzrYIyuRbLGxWAQfsX+C1jrJaS2rsRu6lU/ve1b9hEzSSzo6VwqXx
gYPijpNio6OwLgbzbH6IuWSNtvp7bCV5UMbKZJCVNdg=
ysEnh8zkgcN8WwINs5FP7vGybZW2TtVSX36HO6emvdUrcCkVbC9hrF5Pe5ZSZx3i

POSSIBLE SECRETS
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d010104050003820101001 9d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
24f7+wNdQe8HQwz0gPH2QIzxUp8iQNA20yBU7Dg74Sc=
xcWDoPM3ZfO4P10VSUmZKRTMvsXPXnglJL31bwAJBgJGdSUy2IQG17s4MILOncV2
CkzLLxV5zSb+jeaEDnt9Q3eBrpVMtqnw6wBKNocN2YzoApdHEqHkRi4x0VOMDtd4
mkunJHFc5vhTAVOcsaNSYx7OvFB6slgbORGrA/joIDO0IYq5rQvDcAbp2AI6CPUh

PLAYSTORE INFORMATION

Title: Complete – Medication Tracker

Score: 4.539604 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.abbvie.patientapp

Developer Details: AbbVie, AbbVie, None, http://www.abbvie.com, customerservice@abbvie.com,

Release Date: Sep 9, 2015 **Privacy Policy:** Privacy link

Description:

Please see Uses and Important Safety Information including BOXED WARNING for HUMIRA (adalimumab) at www.humira.com/important-safety-information. Please see Uses and Important Safety Information including BOXED WARNING for RINVOQ (upadacitinib) at www.rinvoq.com/important-safety-information. Please see Uses and Important Safety Information for SKYRIZI (risankizumab) at www.skyrizi.com/important-safety-information. Please see the Full Prescribing Information for HUMIRA at www.rxabbvie.com/pdf/humira.pdf, RINVOQ at www.rxabbvie.com/pdf/rinvoq_pi.pdf, and SKYRIZI at www.rxabbvie.com/pdf/skyrizi_pi.pdf. Please see the Savings Card Terms & Conditions for HUMIRA at www.humira.com/humira-complete/cost-and-copay#hcsctac, RINVOQ at www.rinvoq.com/resources/save-on-rinvoq-costs#saving-cards-t-m, and SKYRIZI at https://www.skyrizi.com/skyrizi-complete/save-on-skyrizi-costs#tandcs. The Complete App features personalized injection and symptom logging, medication reminders, and goal setting to support and encourage you throughout treatment. Your Complete App keeps you in the know of what HUMIRA, RINVOQ, and SKYRIZI can do for you. CUSTOMIZED INJECTION LOGGING & TRAINING • Keep track of when and where you inject either HUMIRA or SKYRIZI on your body. • View your injection history by date with details. Tap on a specific date to see injection times, sites, and notes. • Personalize how you rotate injection sites in a chronological order. • Use in-app videos, training kits, and more to review injection training from your doctor. DOSE TRACKING FOR RINVOQ PATIENTS • Make it easier to stick to your treatment plan and track monthly progress with the RINVOQ dose tracker. DOSE REMINDERS & MEDICATION TRACKERS • Tools to help manage your medication through this free app. Set reminders and enable push notifications so you never miss a dose. CALENDAR & ACTIVITY LOG • View your injection or medication schedule, symptom history, and a body diagram of injection locations. SYMPTOM TRACKING • Keep a log of your symptoms to discuss at your next doctor visit. This may help you have more productive discussions about your treatment. ACCESS MORE COMPLETE RESOURCES • Request resources to support you throughout treatment, like a Savings Card that may help eligible patients lower prescription cost. • Connect with a dedicated Nurse Ambassador*, there to provide support and help answer questions. • Submit receipts for reimbursement on eligible out-of-pocket expenses through the Complete Prescription Rebate. *Nurse Ambassadors are provided by AbbVie and do not work under the direction of your health care professional (HCP) or give medical advice. They are trained to direct patients to their HCP for treatment-related advice, including further referrals. CUSTOMIZED GOAL TRACKING FOR RINVOQ PATIENTS • Set personal goals to focus on something personally meaningful to work toward. Personal goals may help motivate and keep you on track with your prescribed treatment plan. Additional Information If you're taking HUMIRA, SKYRIZI, or RINVOQ, you may want help starting and staying on track with your treatment plan. The Complete App can help by providing resources that allow you to set reminders, track symptoms, and create personal goals that can support and encourage you throughout your treatment journey. If you have any questions or concerns with the Complete App, or you need to report medication side effects or adverse events, call 1.800.4HUMIRA (1.800.448.6472) for HUMIRA, 1.866.SKYRIZI (1.866.759.7494) for SKYRIZI, and 1-800-2RINVOQ (1-800-274-6867) for RINVOQ. This app is intended for the exclusive use of U.S. residents 18 years of age and older. The Complete App is not intended to provide treatment decisions or replace the care and advice of a licensed healthcare provider. All medical analysis and treatment plans should be performed by a licensed healthcare provider. US-MULT-250196

SCAN LOGS

Timestamp	Event	Error
2025-08-29 18:53:16	Generating Hashes	OK
2025-08-29 18:53:17	Extracting APK	OK
2025-08-29 18:53:17	Unzipping	OK
2025-08-29 18:53:18	Parsing APK with androguard	OK
2025-08-29 18:53:19	Extracting APK features using aapt/aapt2	OK
2025-08-29 18:53:19	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 18:53:24	Parsing AndroidManifest.xml	OK
2025-08-29 18:53:24	Extracting Manifest Data	OK
2025-08-29 18:53:24	Manifest Analysis Started	OK
2025-08-29 18:53:27	Reading Network Security config from network_security_config.xml	OK
2025-08-29 18:53:27	Parsing Network Security config	OK
2025-08-29 18:53:27	Performing Static Analysis on: Complete (com.abbvie.patientapp)	OK

2025-08-29 18:53:28	Fetching Details from Play Store: com.abbvie.patientapp	OK
2025-08-29 18:53:28	Checking for Malware Permissions	OK
2025-08-29 18:53:28	Fetching icon path	OK
2025-08-29 18:53:28	Library Binary Analysis Started	OK
2025-08-29 18:53:28	Analyzing lib/arm64-v8a/libandroidx.graphics.path.so	OK
2025-08-29 18:53:28	Analyzing lib/arm64-v8a/libsqlcipher.so	OK
2025-08-29 18:53:28	Analyzing lib/arm64-v8a/libimage_processing_util_jni.so	OK
2025-08-29 18:53:28	Analyzing lib/x86_64/libandroidx.graphics.path.so	OK
2025-08-29 18:53:28	Analyzing lib/x86_64/libsqlcipher.so	OK
2025-08-29 18:53:28	Analyzing lib/x86_64/libimage_processing_util_jni.so	OK
2025-08-29 18:53:28	Analyzing lib/armeabi-v7a/libandroidx.graphics.path.so	OK
2025-08-29 18:53:28	Analyzing lib/armeabi-v7a/libsqlcipher.so	OK
2025-08-29 18:53:28	Analyzing lib/armeabi-v7a/libimage_processing_util_jni.so	OK
2025-08-29 18:53:28	Analyzing lib/x86/libandroidx.graphics.path.so	OK
2025-08-29 18:53:28	Analyzing lib/x86/libsqlcipher.so	OK

2025-08-29 18:53:28	Analyzing lib/x86/libimage_processing_util_jni.so	OK
2025-08-29 18:53:28	Analyzing apktool_out/lib/arm64-v8a/libandroidx.graphics.path.so	OK
2025-08-29 18:53:28	Analyzing apktool_out/lib/arm64-v8a/libsqlcipher.so	OK
2025-08-29 18:53:28	Analyzing apktool_out/lib/arm64-v8a/libimage_processing_util_jni.so	OK
2025-08-29 18:53:28	Analyzing apktool_out/lib/x86_64/libandroidx.graphics.path.so	OK
2025-08-29 18:53:28	Analyzing apktool_out/lib/x86_64/libsqlcipher.so	OK
2025-08-29 18:53:29	Analyzing apktool_out/lib/x86_64/libimage_processing_util_jni.so	OK
2025-08-29 18:53:29	Analyzing apktool_out/lib/armeabi-v7a/libandroidx.graphics.path.so	OK
2025-08-29 18:53:29	Analyzing apktool_out/lib/armeabi-v7a/libsqlcipher.so	OK
2025-08-29 18:53:29	Analyzing apktool_out/lib/armeabi-v7a/libimage_processing_util_jni.so	OK
2025-08-29 18:53:29	Analyzing apktool_out/lib/x86/libandroidx.graphics.path.so	OK
2025-08-29 18:53:29	Analyzing apktool_out/lib/x86/libsqlcipher.so	OK
2025-08-29 18:53:29	Analyzing apktool_out/lib/x86/libimage_processing_util_jni.so	OK
2025-08-29 18:53:29	Reading Code Signing Certificate	OK
2025-08-29 18:53:30	Running APKiD 2.1.5	OK

2025-08-29 18:53:39	Detecting Trackers	OK
2025-08-29 18:53:46	Decompiling APK to Java with JADX	OK
2025-08-29 18:54:21	Converting DEX to Smali	OK
2025-08-29 18:54:21	Code Analysis Started on - java_source	OK
2025-08-29 18:54:31	Android SBOM Analysis Completed	OK
2025-08-29 18:54:49	Android SAST Completed	OK
2025-08-29 18:54:49	Android API Analysis Started	OK
2025-08-29 18:55:04	Android API Analysis Completed	OK
2025-08-29 18:55:04	Android Permission Mapping Started	OK
2025-08-29 18:55:19	Android Permission Mapping Completed	OK
2025-08-29 18:55:20	Android Behaviour Analysis Started	OK
2025-08-29 18:55:40	Android Behaviour Analysis Completed	OK
2025-08-29 18:55:40	Extracting Emails and URLs from Source Code	OK
2025-08-29 18:55:50	Email and URL Extraction Completed	OK
2025-08-29 18:55:50	Extracting String data from APK	OK

2025-08-29 18:55:51	Extracting String data from SO	OK
2025-08-29 18:55:51	Extracting String data from Code	OK
2025-08-29 18:55:51	Extracting String values and entropies from Code	OK
2025-08-29 18:55:59	Performing Malware check on extracted domains	OK
2025-08-29 18:56:04	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.