MOBSF

ANDROID STATIC ANALYSIS REPORT

Drugs.com (2.14.15)

File Name: com.drugscom.app_139.apk

Package Name:	com.drugscom.app
Scan Date:	Aug. 29, 2025, 9:55 p.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	6/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	15	4	1	1

FILE INFORMATION

File Name: com.drugscom.app_139.apk
Size: 23.46MB
MD5: b3af6e4b24c7d1125ffca21f4230ab4c
SHA1: 8bb06eced6169e7ed03241b4f19206d63bb16bab
SHA256: 25b8ca9fde6392c4c91bd01081df4486f1b755249e0e8de1e68ca51f74cb7b61

APP INFORMATION

App Name: Drugs.com
Package Name: com.drugscom.app
Main Activity: com.drugscom.app.SplashActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 2.14.15
Android Version Code: 139

APP COMPONENTS

Activities: 14
Services: 13
Receivers: 14
Providers: 5
Exported Activities: 2
Exported Services: 3
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=NZ, ST=Auckland, L=Auckland, O=drugs.com, OU=Infrastructure, CN=Paul Wager
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-02-05 22:31:37+00:00
Valid To: 2073-01-21 22:31:37+00:00
Issuer: C=NZ, ST=Auckland, L=Auckland, O=drugs.com, OU=Infrastructure, CN=Paul Wager
Serial Number: 0x51118849
Hash Algorithm: sha1
md5: d05347d9786edbe4bd0548e5ddc7ee72
sha1: 14384d69d8ce71688cb544f2e3a76a8c1386f10a
sha256: 96e5471000c8d78875f99780db2471a5f84d532394cf6af06cfc7d4f7e4d126a
sha512: a5e17e978f71faf8a67db879eee2faaf545881ef775af4279f59c0e68f7f5cf4f48f82307258e8f0b203864495b7368d68f60b2392db5da80e858dd72abc5f7b
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 3404f17ca0d1c61df6168e4202012b82f7f18e5ca8cb9c5b94b32357557b6504
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.drugscom.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
network operator name check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
crc644136901249a4bd38.MainActivity	Schemes: ddcuber://, Hosts: *,

ACTIVITY	INTENT
crc644136901249a4bd38.WebAuthenticationCallbackActivity	Schemes: dcuber://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | 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.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 9 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	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.
4	Activity (crc644136901249a4bd38.MainActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (crc644136901249a4bd38.WebAuthenticationCallbackActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Service (crc646fc37d57d2d6b57c.DdcGcmListenerService) is not Protected. [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.
7	Service (crc646fc37d57d2d6b57c.DdcInstanceIDListenerService) is not Protected. [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.
8	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.

NO	ISSUE	SEVERITY	DESCRIPTION
9	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.
10	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **0** | WARNING: **3** | INFO: **3** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/microsoft/appcenter/AbstractAppCenterService.java com/microsoft/appcenter/AppCenter.java com/microsoft/appcenter/Constants.java com/microsoft/appcenter/Flags.java com/microsoft/appcenter/ServiceInstrumentationUtils.java com/microsoft/appcenter/UncaughtExceptionHandler.java com/microsoft/appcenter/analytics/Analytics.java com/microsoft/appcenter/analytics/AnalyticsTransmissionTarget.java com/microsoft/appcenter/analytics/AuthenticationProvider.java com/microsoft/appcenter/analytics/EventProperties.java com/microsoft/appcenter/analytics/channel/AnalyticsValidator.java com/microsoft/appcenter/analytics/channel/Session

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	Tracker.java com/microsoft/appcenter/analytics/ingestion/models/EventLog.java com/microsoft/appcenter/analytics/ingestion/models/json/EventLogFactory.java com/microsoft/appcenter/channel/DefaultChannel.java com/microsoft/appcenter/channel/OneCollectorChannelListener.java com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/WrapperSdkExceptionManager.java com/microsoft/appcenter/crashes/ingestion/models/AbstractErrorLog.java com/microsoft/appcenter/crashes/ingestion/models/ErrorAttachmentLog.java com/microsoft/appcenter/crashes/ingestion/models/HandledErrorLog.java com/microsoft/appcenter/crashes/ingestion/models/ManagedErrorLog.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/http/AbstractAppCallTemplate.java com/microsoft/appcenter/http/DefaultHttpClient.java com/microsoft/appcenter/http/DefaultHttpClientCallTask.java com/microsoft/appcenter/http/HttpClientNetworkStateHandler.java com/microsoft/appcenter/http/HttpClientRetryer.java com/microsoft/appcenter/ingestion/OneCollectorIngestion.java com/microsoft/appcenter/ingestion/models/AbstractLog.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaDataUtils.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaLog.java com/microsoft/appcenter/ingestion/models/one/PartAUtils.java com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/AppCenterLog.java com/microsoft/appcenter/utils/AsyncTaskUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/microsoft/appcenter/utils/DeviceInfoHelper.java com/microsoft/appcenter/utils/IdHelper.java com/microsoft/appcenter/utils/NetworkStateHelper.java com/microsoft/appcenter/utils/context/SessionContext.java com/microsoft/appcenter/utils/context/UserIdContext.java com/microsoft/appcenter/utils/crypto/CryptoUtils.java com/microsoft/appcenter/utils/storage/DatabaseManager.java com/microsoft/appcenter/utils/storage/FileManager.java mono/android/incrementaldeployment/IncrementalClassLoader.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/microsoft/appcenter/AppCenter.java com/microsoft/appcenter/Constants.java com/microsoft/appcenter/channel/DefaultChannel.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/http/DefaultHttpClient.java com/microsoft/appcenter/ingestion/OneCollectorIngestion.java com/microsoft/appcenter/ingestion/models/WrapperSdk.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaLog.java com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/context/SessionContext.java com/microsoft/appcenter/utils/storage/DatabaseManager.java
3	This App uses SQL Cipher. Ensure that secrets are not hardcoded in code.	info	OWASP MASVS: MSTG-CRYPTO-1	com/microsoft/appcenter/utils/storage/DatabaseManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/storage/DatabaseManager.java
5	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	mono/android/content/ClipboardManager_OnPrimaryClipChangedListenerImplementor.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	com/microsoft/appcenter/http/HttpClientRetryer.java

SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libmonodroid.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: ['__umask_chk', '__read_chk', '__memcpy_chk', '__umask_chk', '__read_chk', '__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libe_sqlite3.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: ['__strlen_chk', '__memcpy_chk', '__memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libxamarin-app.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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
4	arm64-v8a/libesqlite3.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
5	arm64-v8a/libmono-native.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	arm64-v8a/libmonosgen-2.0.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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: ['__FD_ISSET_chk', '__FD_SET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libxa-internal-api.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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libmono-btls-shared.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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	armeabi-v7a/libmonodroid.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: ['__umask_chk', '__memcpy_chk', '__ThumbV7PILongThunk___umask_chk', '__umask_chk', '__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi-v7a/libe_sqlite3.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
11	armeabi-v7a/libxamarin-app.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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
12	armeabi-v7a/libesqlite3.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	armeabi-v7a/libmono-native.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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	armeabi-v7a/libmonosgen-2.0.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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	armeabi-v7a/libxa-internal-api.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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	armeabi-v7a/libmono-btls-shared.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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	arm64-v8a/libmonodroid.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: ['__umask_chk', '__read_chk', '__memcpy_chk', '__umask_chk', '__read_chk', '__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	arm64-v8a/libe_sqlite3.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: ['__strlen_chk', '__memcpy_chk', '__memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	arm64-v8a/libxamarin-app.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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
20	arm64-v8a/libesqlite3.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
21	arm64-v8a/libmono-native.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	arm64-v8a/libmonosgen-2.0.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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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: ['__FD_ISSET_chk', '__FD_SET_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	arm64-v8a/libxa-internal-api.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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	arm64-v8a/libmono-btls-shared.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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	armeabi-v7a/libmonodroid.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: ['__umask_chk', '__memcpy_chk', '__ThumbV7PILongThunk___umask_chk', '__umask_chk', '__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	armeabi-v7a/libe_sqlite3.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
27	armeabi-v7a/libxamarin-app.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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
28	armeabi-v7a/libesqlite3.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
29	armeabi-v7a/libmono-native.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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	armeabi-v7a/libmonosgen-2.0.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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	armeabi-v7a/libxa-internal-api.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.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	armeabi-v7a/libmono-btls-shared.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.	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00078	Get the network operator name	collection telephony	com/microsoft/appcenter/utils/DeviceInfoHelper.java
00132	Query The ISO country code	telephony collection	com/microsoft/appcenter/utils/DeviceInfoHelper.java
00022	Open a file from given absolute path of the file	file	com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/utils/storage/FileManager.java
00013	Read file and put it into a stream	file	com/microsoft/appcenter/utils/storage/FileManager.java okio/Okio__JvmOkioKt.java
00005	Get absolute path of file and put it to JSON object	file	com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java
00004	Get filename and put it to JSON object	file collection	com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://drugscomnotifications.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/888507478658/namespaces/firebase:fetch?key=AIzaSyDqeOTA0-7VuLflA9h-nJ7IZLmLSaTyiCg. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION
Other Common Permissions	3/44	com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
in.appcenter.ms	ok	**IP:** 4.152.45.255 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
android.googlesource.com	ok	**IP:** 142.251.15.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
docs.microsoft.com	ok	**IP:** 23.53.144.75 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map
mobile.events.data.microsoft.com	ok	**IP:** 52.168.117.171 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
drugscomnotifications.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	Analytics	https://reports.exodus-privacy.eu.org/trackers/105
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
"firebase_database_url" : "https://drugscomnotifications.firebaseio.com"
"google_crash_reporting_api_key" : "AIzaSyDqeOTA0-7VuLflA9h-nJ7IZLmLSaTyiCg"
"google_api_key" : "AIzaSyDqeOTA0-7VuLflA9h-nJ7IZLmLSaTyiCg"
15gLcM46Z4orUYIpbooVfBRJ135AlZRFOmzWaSvqSHg=
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
AEKrzIydHngo8q7U2b8x25JI4cfZS+4qAP315Zd3WikH6poIulxYQwD/LrG8ezMS
GZmNPeawNfdnWxeYT+Jkvj7Vlk5JycUitv3JUjomoDekPAkUoGh0m7MOHceNe5l+
CNH0HFMOMU1Nrmid580u5GwyoVtbweFPAsHIvna6oGuy7GvzbjYQOB8wix+zhJ0t

POSSIBLE SECRETS
Bh5pClYU50tw4hiHvABH1pMF0C7RYCQSvKvFr+ZMSOJwQxEU/7HcV4ByjdhbUI8z
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
Tw8s+i46jU7h4eAAIyqjRm6Qx2s08AiuQFiQiAnvTc/m6i7qS69Zqr0xce6FwG0s
fyLPA28mp7uPyBOReRADDijv3FZ1tUGnt5ZGr7JsU06e7RVIoG/wHKNRMf3WJSQe
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
faUXYiGUMq7bQIeIkZZxqavg/5i6OivEyj0LKDXCfso=
sGX187VmldVivMx8d2G9ijy8IexWLJjVBriaGlzwhpHKAK1AG3if6ICXfcjwXboZ
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
Tgl2ye65VdPWpGRA4PcAavXIUkvdg+RB2j/Kpy7fLYc=
EBqSzSIe3Rjv1o1jIB+xCBngdhv60cOxeintd9wp68g=
mckfj+6L7YQAG+Kc7UoytYIs9AbnOm5Xq8IrT+DQQ5M=
dBvoahw90QxEayGvM7wPL8uyGyjAlcLulgarkCbJ360=
i/S3Ms1xTrAJGHFn1omMI5XPFfDzyhz5oaagmOhDNQg=
hunjs8A/5DNYOOAMFaIGgcT5i4IxfyPvlvtXNFOaD034Wz4GSxVvrwBSs7k+Xuhr
FZw69K6puYJxxRxEPnIcPhNWMb6KJOCrIG9Jmt7OCzqsABzt6hhEAApiISZy7jIX
7E6XPHHgJYFzxm7py5uavXz1wvEMAaDOWzYZ4RGmH8Q=
ae2044fb577e65ee8bb576ca48a2f06e

POSSIBLE SECRETS
apLnpmRDpCfdu10ORTmQ+sdRCmiB4EA8hGSHUeA9nD0=
2aR451s+WavC28PZAI1OicYdxdf9H8e1m2qQ6Vd7HNY=
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
bNQyCiIh4bApN5OPBGky2u9xZmVV2JI0QXAUD4Niu0E=
PuuRKBgJ4ot1aOnWjIUdGlqyRoZ6ZOMOeX7ZmvGezGg=
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e69613116 30140603550407130d4d6f756e7461696e2056696577311430120603550 40a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e0603550403130 7416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603 550407130d4d6f756e7461696e2056696577311430120603550 40a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e0603550403130 7416e64726f6964308 20120300d06092a864886f70d0101010500038201 0d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656 a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf78576 9bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5 db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc22 11756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603 5 50408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e2056696577311430120603550 40a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69 643110300e0603550403130 7416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d0101040500038201 01006dd252ceef85302c360aaace939 bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d 9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41ed da0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff6214 10c069308a
ehe3LQxKXFrt/NNsQSZhaLiz0oEhy5ctQpqWTqSg+00=
SWC7heB+iJvjMtyDTDnMRbHSVyBQ/kwwuxCjVwpzEBg=
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
HiRHV0+7iHel8ouy3rC3Vh6JmfAaV6+B5y9bcOz6v6RtgCUkDJJ1u0Sc7x4KnqIM

POSSIBLE SECRETS
1Bl17hQq0WWTvmWWEgdcU2HCh9GQdFF/nionC9ho0WU=
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
B3EEABB8EE11C2BE770B684D95219ECB
Jdw9xFuo4OHuL+Waf9VEkBs6M7XtRhuX3PknFoicWEjQXQ4CENXY5MXEEK1WPoR/
0IMe0hZjzvPOj0FU8vVpI60XmFXXOxBk0ZbCWvkG8dU=
mC2vnvn09mABIg+Z3lW4jT9JiWpty1Pg+VYrat/OBbcFnzi+qVKsaQnZ8pNi1wxq
9Ibp0iX8frxcDol5LCDOary7OEblvzOEr0WtPn69zRxHnh2qqHn8v0kanoAZtnND
2wtcCTLoT7a0RzNv8L+mVKR+6NVfukO9BpKgsaOGTiHGeYqcI7vlZYOTUtiUYK5a
vKrEk100dPKKqaxICALjJbVlJ7Gg4dfwKwDEqSKZDKo=
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
gRiEqMdygJbXVwKGpJJS0XfYaGpCoNDcsHcIyHSZIcdpg+a2r1SI+bnO9R0NWRI0
NVotBewebesTf3yaQqbfIHsAQGGO5mYV6zcO8zQG+1Te4y/3fFN6rm5Uo4mLM7YY
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
nFFCV0RNg4jne34kh3cuJ7Rctyd77rnT1UYT4k6WJUQ=
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
5kaSofNlVXtCUNlGdVeQWvaOP7NTlA28WhQGVqYMr2+1W5DIZ4rAeif/Ixnxac6c

POSSIBLE SECRETS
IowIKykYnY6WZolnjAhl1KeEVDwldWZiaxuj9ry3exU=
5181942b9ebc31ce68dacb56c16fd79f
kwtXYBCvBLfWcikGQlC0YCCiAi3jf0v8mKFP3Rqx70Jf0cytKZO4qWHMAffIVrkU
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
Nh+w10G1n7Da4ABjUIxN+bi57DvusNUcn9VqpF1GXimOuh+Booa8zjDH+Fzh+CdP
8G9c9fsfPvjJxInHRs9Zm9vZr56UYrRb8WMC1rhyiOA=
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d01010405003081943 10b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d303830343135323333635365a170d333530393031323333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d01010405003820101001 9d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
soiTax1jBnD3649O45Tb84AswyowGJo3bnB66jWq5Kw=
gqK1fJWMt2lYn7O2X7ompi2Bw14HxMMjzTnJdiQom2Q=
xg6GNdV7fYR9czDPsYCpiIl0/69vO40WnrUnsYSb5exMDfWVVhFT+7O8xMnCz7QV
XIDT/tdnEZKwO9t3IF1TXzt4lSi3aThE4MpcZzXzgu8=

POSSIBLE SECRETS
6DjMpZpwaW5op66Lef2rZgfmub82/L76U+lowNvybUI=
z6qQV45Nmnz8yfEHycE7xvBh5frOehaJSTK9o+9gqcg=
3U0cjCPkA8fmy+qqbK7WJ2AhtyNFccQtIqqvzcvTqob91cu5tr66zNiNrkLc8aJb
115792089210356248762697446949407573529996955224135760342422259061068512044369
afOCxwiNZt1pFw/pjRCeFiRYbGwWcjibO33q64LhR0M=
icVSPKCsokOqk/nN9ldgEGzs48x1unFAjrOT1dBDO7k=

PLAYSTORE INFORMATION

Title: Drugs.com Medication Guide

Score: 4.748418 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.drugscom.app

Developer Details: Drugs.com, Drugs.com, None, https://www.drugs.com, apps@drugs.com,

Release Date: Feb 24, 2013 **Privacy Policy:** Privacy link

Description:

Manage meds, identify pills, check interactions, compare prices and more. Discover detailed, peer-reviewed info on over 24,000 prescription drugs, OTC meds, and natural products all in one place. WHAT'S NEW - Customizable home screen: Show, hide, and reorder app sections to suit your needs. - Light & dark support: Switch between themes in Settings > Appearance. Key Features - My Med List: Create your health profile and track drug interactions, reminders and alerts, with offline access. - Price Guide: Find the lowest prices for medications and search pharmacies near you. - Pill Identifier: Identify pills by imprint, color and shape to confirm medications with confidence. - Interactions Checker: Check potential interactions between prescription medications, OTC drugs, and supplements. - Q & A: Find answers to thousands of medication-related questions, join support groups or ask a question. - Compare Tool: Compare any medication side-by-side. - Side Effects Checker: Access detailed side effect information for thousands of prescription and OTC medications, from common mild reactions to rare severe effects. - Dosage Information: Reliable dose guidance. - FDA Alerts: Stay up to date with product recalls, safety alerts, and FDA-related news. - Health Professionals: Tailored tools and information for medical professionals, including FDA monographs. Permissions We request limited permissions to improve your experience: - Network access: Required to connect to our database. - Media/Storage: For installation on your SD card only, we never access your personal files. - Your location: Used when you choose to find nearby pharmacies when using the drug discount card. About Drugs.com With over 25 million U.S. monthly visitors, Drugs.com is a Webby-nominated health information platform offering peer-reviewed data on more than 24,000 medications. Whether you're a patient, caregiver, or healthcare professional, the app provides reliable tools to manage and understand medication use. Note: Drugs.com does not provide medical advice, diagnosis or treatment. Do not rely on this app to replace medical advice, diagnosis or treatment. Always consult with your healthcare professional. Support & Subscriptions Please visit: https://www.drugs.com/apps/support/ for support and feedback, if its subscription related, our team will prioritize your request.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 21:55:27	Generating Hashes	OK
2025-08-29 21:55:27	Extracting APK	OK
2025-08-29 21:55:27	Unzipping	OK
2025-08-29 21:55:28	Parsing APK with androguard	OK
2025-08-29 21:55:28	Extracting APK features using aapt/aapt2	OK
2025-08-29 21:55:28	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 21:55:31	Parsing AndroidManifest.xml	OK
2025-08-29 21:55:31	Extracting Manifest Data	OK
2025-08-29 21:55:31	Manifest Analysis Started	OK
2025-08-29 21:55:31	Performing Static Analysis on: Drugs.com (com.drugscom.app)	OK

2025-08-29 21:55:32	Fetching Details from Play Store: com.drugscom.app	OK
2025-08-29 21:55:32	Checking for Malware Permissions	OK
2025-08-29 21:55:32	Fetching icon path	OK
2025-08-29 21:55:32	Library Binary Analysis Started	OK
2025-08-29 21:55:32	Analyzing lib/arm64-v8a/libmonodroid.so	OK
2025-08-29 21:55:32	Analyzing lib/arm64-v8a/libe_sqlite3.so	OK
2025-08-29 21:55:32	Analyzing lib/arm64-v8a/libxamarin-app.so	OK
2025-08-29 21:55:32	Analyzing lib/arm64-v8a/libesqlite3.so	OK
2025-08-29 21:55:32	Analyzing lib/arm64-v8a/libmono-native.so	OK
2025-08-29 21:55:32	Analyzing lib/arm64-v8a/libmonosgen-2.0.so	OK
2025-08-29 21:55:32	Analyzing lib/arm64-v8a/libxa-internal-api.so	OK
2025-08-29 21:55:32	Analyzing lib/arm64-v8a/libmono-btls-shared.so	OK

2025-08-29 21:55:32	Analyzing lib/armeabi-v7a/libmonodroid.so	OK
2025-08-29 21:55:32	Analyzing lib/armeabi-v7a/libe_sqlite3.so	OK
2025-08-29 21:55:32	Analyzing lib/armeabi-v7a/libxamarin-app.so	OK
2025-08-29 21:55:32	Analyzing lib/armeabi-v7a/libesqlite3.so	OK
2025-08-29 21:55:32	Analyzing lib/armeabi-v7a/libmono-native.so	OK
2025-08-29 21:55:32	Analyzing lib/armeabi-v7a/libmonosgen-2.0.so	OK
2025-08-29 21:55:33	Analyzing lib/armeabi-v7a/libxa-internal-api.so	OK
2025-08-29 21:55:33	Analyzing lib/armeabi-v7a/libmono-btls-shared.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/arm64-v8a/libmonodroid.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/arm64-v8a/libe_sqlite3.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/arm64-v8a/libxamarin-app.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/arm64-v8a/libesqlite3.so	OK

2025-08-29 21:55:33	Analyzing apktool_out/lib/arm64-v8a/libmono-native.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/arm64-v8a/libmonosgen-2.0.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/arm64-v8a/libxa-internal-api.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/arm64-v8a/libmono-btls-shared.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/armeabi-v7a/libmonodroid.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/armeabi-v7a/libe_sqlite3.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/armeabi-v7a/libxamarin-app.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/armeabi-v7a/libesqlite3.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/armeabi-v7a/libmono-native.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/armeabi-v7a/libmonosgen-2.0.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/armeabi-v7a/libxa-internal-api.so	OK
2025-08-29 21:55:33	Analyzing apktool_out/lib/armeabi-v7a/libmono-btls-shared.so	OK

2025-08-29 21:55:33	Reading Code Signing Certificate	OK
2025-08-29 21:55:34	Running APKiD 2.1.5	OK
2025-08-29 21:55:38	Detecting Trackers	OK
2025-08-29 21:55:40	Decompiling APK to Java with JADX	OK
2025-08-29 21:55:54	Converting DEX to Smali	OK
2025-08-29 21:55:54	Code Analysis Started on - java_source	OK
2025-08-29 21:55:55	Android SBOM Analysis Completed	OK
2025-08-29 21:56:00	Android SAST Completed	OK
2025-08-29 21:56:00	Android API Analysis Started	OK
2025-08-29 21:56:04	Android API Analysis Completed	OK
2025-08-29 21:56:05	Android Permission Mapping Started	OK
2025-08-29 21:56:08	Android Permission Mapping Completed	OK

2025-08-29 21:56:09	Android Behaviour Analysis Started	OK
2025-08-29 21:56:13	Android Behaviour Analysis Completed	OK
2025-08-29 21:56:13	Extracting Emails and URLs from Source Code	OK
2025-08-29 21:56:13	Email and URL Extraction Completed	OK
2025-08-29 21:56:13	Extracting String data from APK	OK
2025-08-29 21:56:14	Extracting String data from SO	OK
2025-08-29 21:56:14	Extracting String data from Code	OK
2025-08-29 21:56:14	Extracting String values and entropies from Code	OK
2025-08-29 21:56:16	Performing Malware check on extracted domains	OK
2025-08-29 21:56:17	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.