MOBSF

ANDROID STATIC ANALYSIS REPORT

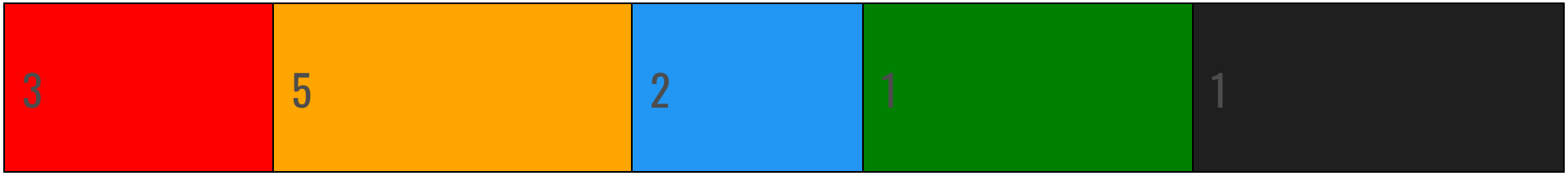
carto (1.0.0)

File Name: app-release.apk

Package Name:	com.example.carto
Scan Date:	Jan. 29, 2026, 12:04 a.m.
App Security Score:	41/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT



FILE INFORMATION

File Name: app-release.apk
Size: 46.77MB
MD5: 7cbe1d3eb215f4e479e7cc7d44c897d6
SHA1: b1f9d6187d990e4f40852915c313d3f3d31d4564
SHA256: 633fbbe2263b29c16e1b594ce38e7d4da51a08cc92f22997e7ff3eaad38726a6

APP INFORMATION

App Name: carto
Package Name: com.example.carto
Main Activity: com.example.carto.MainActivity
Target SDK: 36
Min SDK: 24
Max SDK:
Android Version Name: 1.0.0
Android Version Code: 1

APP COMPONENTS

Activities: 1
Services: 1
Receivers: 1
Providers: 2
Exported Activities: 0
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2025-11-20 23:14:07+00:00
Valid To: 2055-11-13 23:14:07+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: c1ef71ee0c4b17905ab1ebe9ff57e082
sha1: a71a7c9d97867ac5635613ff776721e19f444f4e
sha256: ff65160d887c08c360879547c3458a622ab91c507eb75dc868e07a842f438b4b
sha512: 6adb7bb9b63bc71a766424b7dfde74c9cd59720735f79653d9aa6683a9966567b34a1f9499ab62bba719baa93e2d557226accd0c116871a1220987a51b884c44
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 38a9b9d0479fcc416d7eeeab194629cb90c3a86ecfd5d64255b8f582b950bd6b
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.
com.example.carto.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.

MANIFEST ANALYSIS

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

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

NO	ISSUE	SEVERITY	DESCRIPTION
2	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	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: **1** | WARNING: **3** | INFO: **2** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A/n.java F/d.java I/a.java L/b.java L/d.java L/h.java N/e.java P/C0026b.java P/Q.java V/f.java Y/n.java a/AbstractC0069a.java b0/j.java c/b.java e0/C0110a.java e0/d.java h/C0117c.java h/C0118d.java h0/AbstractActivityC0123d.java h0/C0122c.java h0/C0127h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	h0/i.java h0/k.java h0/m.java h0/o.java h0/u.java i/g.java i/j.java i0/d.java io/flutter/embedding/engine/FlutterJNI.java io/flutter/embedding/engine/renderer/FlutterRenderer$ImageTextureRegistryEntry.java io/flutter/embedding/engine/renderer/e.java io/flutter/plugin/editing/f.java io/flutter/plugin/editing/l.java io/flutter/plugin/platform/p.java io/flutter/plugins/GeneratedPluginRegistrant.java io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/l.java j/AbstractC0130A.java j/C0156p.java j/C0162w.java j/L.java j/O.java j/g0.java j/t0.java j/x0.java j0/b.java j0/j.java l0/C0178e.java q0/d.java q0/k.java r0/C0202a.java s/d.java s/e.java s/f.java s/g.java v/AbstractC0216b.java w/b.java x0/C0219a.java y0/C0243d.java z/AbstractC0260p.java z/B.java z/C0251g.java z/D.java z/E.java z/I.java z0/C0266b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				z0/K.java
2	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	N0/a.java N0/b.java N0/c.java O0/a.java
3	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	x0/C0228j.java
4	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	q/e.java y0/C0243d.java
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	I/a.java x0/C0226h.java
6	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/editing/c.java q0/d.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	armeabi-v7a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk', '__vsprintf_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	armeabi-v7a/libdatastore_shared_counter.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
4	arm64-v8a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	arm64-v8a/libdatastore_shared_counter.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
7	x86_64/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86_64/libdatastore_shared_counter.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	armeabi-v7a/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk', '__vsprintf_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	armeabi-v7a/libdatastore_shared_counter.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/libflutter.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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	arm64-v8a/libdatastore_shared_counter.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
16	x86_64/libflutter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	Not Applicable info RELRO checks are not applicable for Flutter/Dart binaries	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__read_chk', '__memcpy_chk', '__strcpy_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	x86_64/libdatastore_shared_counter.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
00013	Read file and put it into a stream	file	H/S.java H/T.java I/a.java J/f.java K/g.java L/h.java N/a.java N/e.java N/i.java c/b.java s/e.java s/f.java
00022	Open a file from given absolute path of the file	file	H/C0014o.java H/U.java H/V.java H/Z.java I/a.java io/flutter/embedding/engine/FlutterJNI.java l0/CallableC0176c.java x0/C0226h.java y0/C0243d.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/h.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	P/Q.java e0/d.java x0/C0226h.java
00202	Make a phone call	control	P/Q.java
00203	Put a phone number into an intent	control	P/Q.java
00033	Query the IMEI number	collection	P/Q.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	P/Q.java e0/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00083	Query the IMEI number	collection telephony	P/Q.java
00036	Get resource file from res/raw directory	reflection	P/Q.java e0/d.java j/g0.java
00014	Read file into a stream and put it into a JSON object	file	c/b.java
00024	Write file after Base64 decoding	reflection file	c/b.java
00004	Get filename and put it to JSON object	file collection	c/b.java
00046	Method reflection	reflection	c/b.java
00191	Get messages in the SMS inbox	sms	j/g0.java
00209	Get pixels from the latest rendered image	collection	h0/i.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	h0/i.java
00012	Read data and put it into a buffer stream	file	I/a.java L/h.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	1/25	android.permission.READ_EXTERNAL_STORAGE

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	0/44	

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
www.unicode.org	ok	**IP:** 172.67.74.23 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
issuetracker.google.com	ok	**IP:** 216.58.210.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
fonts.gstatic.com	ok	**IP:** 216.58.210.131 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
images.unsplash.com	ok	**IP:** 199.232.174.208 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ns.adobe.com	ok	No Geolocation information available.
dartbug.com	ok	**IP:** 216.239.34.21 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
youtrack.jetbrains.com	ok	**IP:** 63.35.30.167 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
developer.android.com	ok	**IP:** 142.251.38.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

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

EMAILS

EMAIL	FILE
_hashcollisionnode@34137193.fromcollis authenticationscheme@16463476.fromstring _imagefilter@17065589.fromcolorf _growablelist@0150898._literal2 _list@0150898._ofefficie _growablelist@0150898._literal3 _file@15069316.fromrawpat _assetmanifestbin@43287047.fromstanda _growablelist@0150898._ofarray _list@0150898.generate _nativesocket@15069316.normal _invocationmirror@0150898._withtype _timer@1026248._internal _list@0150898.of _colorfilter@17065589.lineartosr _imagefilter@17065589.composed _receiveportimpl@1026248.fromrawrec _growablelist@0150898.generate _semanticsgeometry@371266271.root _growablelist@0150898._ofother _growablelist@0150898._literal7 _link@15069316.fromrawpat _compressednode@34137193.single _bytebuffer@8027147._new _httpparser@16463476.responsepa _double@0150898.fromintege	

EMAIL	FILE
_future@5048458.immediatee _growablelist@0150898._literal5 storationinformation@287124995.fromserial	lib/armeabi-v7a/libapp.so
_colorfilter@17065589.srgbtoline usuario@email.com _assertionerror@0150898._create _growablelist@0150898._ofgrowabl _uri@0150898.directory _uri@0150898.file _growablelist@0150898._literal _future@5048458.immediate _directory@15069316.fromrawpat _growablelist@0150898.withcapaci _growablelist@0150898._literal4 _imagefilter@17065589.blur _growablelist@0150898._ofefficie _growablelist@0150898._literal1 _list@0150898._ofother _list@0150898._ofgrowabl _list@0150898._ofarray _uri@0150898.notsimple ngstreamsubscription@5048458.zoned _timer@1026248.periodic _typeerror@0150898._create _growablelist@0150898.of _list@0150898.empty _growablelist@0150898._literal8	
appro@openssl.org	lib/arm64-v8a/libflutter.so
appro@openssl.org	lib/x86_64/libflutter.so
_hashcollisionnode@34137193.fromcollis authenticationscheme@16463476.fromstring _imagefilter@17065589.fromcolorf _growablelist@0150898._literal2 _list@0150898._ofefficie _growablelist@0150898._literal3 _file@15069316.fromrawpat _assetmanifestbin@43287047.fromstanda _growablelist@0150898._ofarray _list@0150898.generate _nativesocket@15069316.normal _invocationmirror@0150898._withtype _timer@1026248._internal _list@0150898.of	

EMAIL	FILE
_list@0150898.of _colorfilter@17065589.lineartosr _imagefilter@17065589.composed _receiveportimpl@1026248.fromrawrec _growablelist@0150898.generate _semanticsgeometry@371266271.root _growablelist@0150898._ofother _growablelist@0150898._literal7 _link@15069316.fromrawpat _compressednode@34137193.single _bytebuffer@8027147._new _httpparser@16463476.responsepa _double@0150898.fromintege _future@5048458.immediatee _growablelist@0150898._literal5 storationinformation@287124995.fromserial _colorfilter@17065589.srgbtoline usuario@email.com _assertionerror@0150898._create _growablelist@0150898._ofgrowabl _uri@0150898.directory _uri@0150898.file _growablelist@0150898._literal _future@5048458.immediate _directory@15069316.fromrawpat _growablelist@0150898.withcapaci _growablelist@0150898._literal4 _imagefilter@17065589.blur _growablelist@0150898._ofefficie _growablelist@0150898._literal1 _list@0150898._ofother _list@0150898._ofgrowabl _list@0150898._ofarray _uri@0150898.notsimple ngstreamsubscription@5048458.zoned _timer@1026248.periodic _typeerror@0150898._create _growablelist@0150898.of _list@0150898.empty _growablelist@0150898._literal8	apktool_out/lib/armeabi-v7a/libapp.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libflutter.so
appro@openssl.org	apktool_out/lib/x86_64/libflutter.so

HARDCODED SECRETS

POSSIBLE SECRETS
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy

SCAN LOGS

Timestamp	Event	Error
2026-01-29 00:04:59	Generating Hashes	OK
2026-01-29 00:04:59	Extracting APK	OK
2026-01-29 00:04:59	Unzipping	OK
2026-01-29 00:04:59	Parsing APK with androguard	OK
2026-01-29 00:04:59	Extracting APK features using aapt/aapt2	OK
2026-01-29 00:05:00	Getting Hardcoded Certificates/Keystores	OK
2026-01-29 00:05:03	Parsing AndroidManifest.xml	OK
2026-01-29 00:05:03	Extracting Manifest Data	OK

2026-01-29 00:05:03	Manifest Analysis Started	OK
2026-01-29 00:05:03	Performing Static Analysis on: carto (com.example.carto)	OK
2026-01-29 00:05:04	Fetching Details from Play Store: com.example.carto	OK
2026-01-29 00:05:04	Checking for Malware Permissions	OK
2026-01-29 00:05:04	Fetching icon path	OK
2026-01-29 00:05:04	Library Binary Analysis Started	OK
2026-01-29 00:05:04	Analyzing lib/armeabi-v7a/libflutter.so	OK
2026-01-29 00:05:04	Analyzing lib/armeabi-v7a/libapp.so	OK
2026-01-29 00:05:04	Analyzing lib/armeabi-v7a/libdatastore_shared_counter.so	OK
2026-01-29 00:05:04	Analyzing lib/arm64-v8a/libflutter.so	OK
2026-01-29 00:05:04	Analyzing lib/arm64-v8a/libapp.so	OK

2026-01-29 00:05:04	Analyzing lib/arm64-v8a/libdatastore_shared_counter.so	OK
2026-01-29 00:05:04	Analyzing lib/x86_64/libflutter.so	OK
2026-01-29 00:05:05	Analyzing lib/x86_64/libapp.so	OK
2026-01-29 00:05:05	Analyzing lib/x86_64/libdatastore_shared_counter.so	OK
2026-01-29 00:05:05	Analyzing apktool_out/lib/armeabi-v7a/libflutter.so	OK
2026-01-29 00:05:05	Analyzing apktool_out/lib/armeabi-v7a/libapp.so	OK
2026-01-29 00:05:05	Analyzing apktool_out/lib/armeabi-v7a/libdatastore_shared_counter.so	OK
2026-01-29 00:05:05	Analyzing apktool_out/lib/arm64-v8a/libflutter.so	OK
2026-01-29 00:05:05	Analyzing apktool_out/lib/arm64-v8a/libapp.so	OK
2026-01-29 00:05:05	Analyzing apktool_out/lib/arm64-v8a/libdatastore_shared_counter.so	OK
2026-01-29 00:05:05	Analyzing apktool_out/lib/x86_64/libflutter.so	OK
2026-01-29 00:05:05	Analyzing apktool_out/lib/x86_64/libapp.so	OK

2026-01-29 00:05:06	Analyzing apktool_out/lib/x86_64/libdatastore_shared_counter.so	OK
2026-01-29 00:05:06	Reading Code Signing Certificate	OK
2026-01-29 00:05:06	Running APKiD 3.0.0	OK
2026-01-29 00:05:10	Detecting Trackers	OK
2026-01-29 00:05:10	Decompiling APK to Java with JADX	OK
2026-01-29 00:05:23	Converting DEX to Smali	OK
2026-01-29 00:05:23	Code Analysis Started on - java_source	OK
2026-01-29 00:05:23	Android SBOM Analysis Completed	OK
2026-01-29 00:05:57	Android SAST Completed	OK
2026-01-29 00:05:57	Android API Analysis Started	OK
2026-01-29 00:05:59	Android API Analysis Completed	OK
2026-01-29 00:05:59	Android Permission Mapping Started	OK

2026-01-29 00:06:01	Android Permission Mapping Completed	OK
2026-01-29 00:06:01	Android Behaviour Analysis Started	OK
2026-01-29 00:06:03	Android Behaviour Analysis Completed	OK
2026-01-29 00:06:03	Extracting Emails and URLs from Source Code	OK
2026-01-29 00:06:05	Email and URL Extraction Completed	OK
2026-01-29 00:06:05	Extracting String data from APK	OK
2026-01-29 00:06:05	Extracting String data from SO	OK
2026-01-29 00:06:06	Extracting String data from Code	OK
2026-01-29 00:06:06	Extracting String values and entropies from Code	OK
2026-01-29 00:06:07	Performing Malware check on extracted domains	OK
2026-01-29 00:06:09	Saving to Database	OK