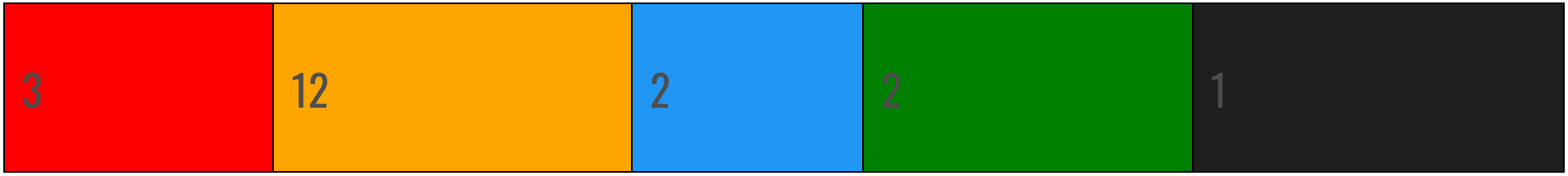
Alliance One 4.0 (1.0.0)

File Name: app-release.apk

Package Name:	com.example.alliance_one
Scan Date:	Feb. 16, 2026, 11:40 a.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT



FILE INFORMATION

File Name: app-release.apk
Size: 50.29MB
MD5: 978a8f22eb62442c2ad510347aa2a03a
SHA1: e04837dcd550913bdfee3d09998aeecfe8444e4e
SHA256: 929e959464d90723f99c6b1c52f9c9ed19e1ffa31b8133d8a09ede375e75d47c

APP INFORMATION

App Name: Alliance One 4.0
Package Name: com.example.alliance_one
Main Activity: com.example.alliance_one.MainActivity
Target SDK: 36
Min SDK: 24
Max SDK:
Android Version Name: 1.0.0
Android Version Code: 1

APP COMPONENTS

Activities: 3
Services: 6
Receivers: 4
Providers: 4
Exported Activities: 0
Exported Services: 0
Exported Receivers: 3
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: 2026-01-29 06:55:36+00:00
Valid To: 2056-01-22 06:55:36+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: 013df7becc85cb2fc7f8469989f786d1
sha1: 45467b038a45405dca24fc32cc28dfe4d3dfd607
sha256: f4f7c12074c00e3bbfbb3dfbe1629871950ac5034720288d898dd3b8a40c506a
sha512: 4f0537afddbc63679d9e1f53e3687cdbec45fa046d2f0a7a5191f8873f9505c4674d6cf8731f96506494f6dafdde43cf8f1576e09ae89bb7f470ba5b7cb00d73
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: ea6306ba00880a8ed94235baf2c38967c7d1ca302010093c682d4d155d02fcd1
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.example.alliance_one.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8

FILE	DETAILS
classes2.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: 2 | WARNING: 4 | 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.
2	Clear text traffic is Enabled For App[android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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.
4	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
5	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A0/d.java A0/h.java A0/n.java A0/o.java A1/C0004e.java A1/C0010k.java A1/CallableC0023y.java A1/G.java A1/a0.java A2/c.java A2/f.java B/B.java B/C.java B/C0032h.java B/E.java B/L.java B0/f.java D2/i.java D2/l.java D2/p.java E1/j.java E2/d.java F/d.java F0/b.java F0/d.java F0/e.java F0/f.java F0/k.java F0/l.java F0/m.java F0/n.java F0/o.java F0/p.java F0/r.java F0/s.java F2/C0075a.java F2/L.java G0/d.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	G0/e.java G0/j.java G0/k.java G0/m.java G1/l.java G2/f.java H2/C0130d.java H2/C0134h.java H2/C0135i.java H2/H.java I0/d.java I0/k.java I0/o.java I1/f.java I2/b.java J0/c.java J0/j.java J0/k.java J0/p.java J0/q.java J0/s.java J0/v.java J2/s0.java K2/a.java K2/b.java L1/b.java L1/d.java M0/a.java M1/b.java N0/d.java N1/c.java O/e.java O/j.java O/l.java P0/a.java R0/e.java R0/g.java R1/AbstractC0259e.java R1/AbstractServiceC0261g.java R1/B.java R1/C.java R1/D.java R1/F.java R1/H.java R1/i.java R1/j.java R1/p.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
			OWASP MASVS: MSTG-STORAGE-3	R1/q.java R1/w.java R1/x.java R1/y.java S/e.java S2/k.java T2/c.java X0/a.java X1/D.java a/AbstractC0317a.java a1/C0319a.java com/dexterous/flutterlocalnotifications/ActionBroadcastReceiver.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/ScheduledNotificationReceiver.java d0/f.java g0/C0507n.java h/C0516d.java h/C0517e.java i/f.java i/i.java i1/C0534g.java io/flutter/embedding/engine/FlutterJNI.java io/flutter/embedding/engine/renderer/FlutterRenderer$ImageTextureRegistryEntry.java io/flutter/embedding/engine/renderer/f.java io/flutter/plugin/editing/f.java io/flutter/plugin/editing/j.java io/flutter/plugin/platform/B.java io/flutter/plugin/platform/C0540b.java io/flutter/plugin/platform/SingleViewPresentation.java io/flutter/plugin/platform/h.java io/flutter/plugin/platform/m.java io/flutter/plugins/GeneratedPluginRegistrant.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingInitProvider.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/l.java j/AbstractC0556F.java j/AbstractC0575g0.java j/C0560J.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				j/C0587m0.java j/C0589o.java j/E0.java j/H0.java j/M0.java j/X0.java j/b1.java j0/C0621i.java k2/C0635b.java k2/c.java k2/f.java k2/g.java k2/i.java k2/k.java k2/m.java k2/r.java k2/s.java l2/C0646d.java m2/C0683b.java m2/C0691j.java n1/e.java o2/C0717e.java o2/RunnableC0714b.java r/G.java r/n.java t2/C0762a.java t2/h.java u/AbstractC0768d.java u/C0769e.java u/C0770f.java u/C0771g.java u/C0773i.java u/C0774j.java u2/C0777a.java w3/a.java x/d.java y/c.java
2	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	G1/I.java M1/b.java N1/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	A0/h.java A0/k.java A0/m.java A0/n.java A1/C0004e.java A1/a0.java A1/r.java B0/f.java B0/k.java C1/P.java C1/S.java C1/V.java
4	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 j/C0578i.java
5	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	E2/d.java m0/C0680a.java s/AbstractC0750e.java
6	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	B1/a.java D1/b.java E1/h.java G1/E.java M2/i.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/models/NotificationDetails.java x1/C0840o.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	F0/j.java L2/C0233s1.java L2/J0.java L2/W.java L2/Y.java L2/i2.java M2/l.java S/f.java S2/y.java
8	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	G1/C0099i.java
9	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	A1/a0.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	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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.

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	A1/a0.java H/O.java H/P.java J/f.java K/g.java S/a.java S/e.java S/k.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java u/C0769e.java u/C0770f.java w3/a.java
00089	Connect to a URL and receive input stream from the server	command network	H2/H.java N1/c.java
00109	Connect to a URL and get the response code	network command	H2/H.java N1/c.java
00189	Get the content of a SMS message	sms	R0/e.java
00188	Get the address of a SMS message	sms	R0/e.java
00200	Query data from the contact list	collection contact	R0/e.java
00201	Query data from the call log	collection calllog	R0/e.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	R0/e.java
00022	Open a file from given absolute path of the file	file	E2/d.java H/C0114m.java H/Q.java H/S.java H/W.java io/flutter/embedding/engine/FlutterJNI.java o2/CallableC0715c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	R1/j.java X1/D.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	A1/C0004e.java G0/e.java a/AbstractC0317a.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java
00036	Get resource file from res/raw directory	reflection	A1/C0004e.java G0/e.java a/AbstractC0317a.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java j/E0.java
00025	Monitor the general action to be performed	reflection	X1/D.java
00125	Check if the given file path exist	file	X1/D.java
00191	Get messages in the SMS inbox	sms	j/E0.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/h.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java
00014	Read file into a stream and put it into a JSON object	file	A1/a0.java
00009	Put data in cursor to JSON object	file	A1/a0.java
00004	Get filename and put it to JSON object	file collection	A1/a0.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	A1/C0004e.java G0/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00175	Get notification manager and cancel notifications	notification	com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java
00209	Get pixels from the latest rendered image	collection	k2/g.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	k2/g.java
00096	Connect to a URL and set request method	command network	H2/H.java
00023	Start another application from current application	reflection control	A1/C0004e.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/384089401859/namespaces/firebase:fetch?key=AIzaSyAWgwsBtPrvMrVa0uzgPCqqq8NHshiwi7U. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	1/44	com.google.android.c2dm.permission.RECEIVE

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
github.com	ok	**IP:** 20.207.73.82 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.205.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 142.251.223.4 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.unicode.org	ok	**IP:** 104.26.10.47 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
alliance-one-backend-production.up.railway.app	ok	**IP:** 66.33.22.212 **Country:** Canada **Region:** Ontario **City:** Etobicoke **Latitude:** 43.623768 **Longitude:** -79.559723 **View:** Google Map
fonts.gstatic.com	ok	**IP:** 172.217.24.195 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 172.217.24.14 **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:** 63.33.88.220 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
issuetracker.google.com	ok	**IP:** 172.217.24.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.mozilla.org	ok	**IP:** 151.101.209.91 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
crbug.com	ok	**IP:** 216.239.32.29 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
one.alliance.edu.in	ok	**IP:** 148.66.159.34 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **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
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
dartbug.com	ok	**IP:** 216.239.32.21 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebaseinstallations.googleapis.com	ok	**IP:** 216.239.36.223 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	G0/l.java
appro@openssl.org	lib/x86_64/libflutter.so
_imagefilter@17065589.composed _list@0150898.of _httpparser@16463476.responsepa _list@0150898._ofgrowabl _growablelist@0150898._literal5 authenticationscheme@16463476.fromstring _growablelist@0150898.withcapaci _growablelist@0150898._literal _future@5048458.immediate _compressednode@38137193.single _colorfilter@17065589.lineartosr _future@5048458.zonevalue _link@15069316.fromrawpat _nativesocket@15069316.normal _uri@0150898.directory _growablelist@0150898._literal8 _growablelist@0150898._literal3 _list@0150898._ofarray _uri@0150898.notsimple _assertionerror@0150898._create _invocationmirror@0150898._withtype	

EMAIL	FILE
_invocationmirror@0150898._withtype _directory@15069316.fromrawpat _file@15069316.fromrawpat _growablelist@0150898._literal7 _uri@0150898.file _timer@1026248.periodic _list@0150898._ofother _imagefilter@17065589.blur _timer@1026248._internal _assetmanifestbin@374287047.fromstanda _list@0150898.generate _growablelist@0150898._literal4 ngstreamsubscription@5048458.zoned _colorfilter@17065589.srgbtoline _semanticsgeometry@320266271.root _growablelist@0150898._ofother _receiveportimpl@1026248.fromrawrec _growablelist@0150898._ofarray _typeerror@0150898._create _future@5048458.immediatee _growablelist@0150898.generate _bytebuffer@8027147._new _growablelist@0150898.of _growablelist@0150898._literal1 storationinformation@234124995.fromserial _list@0150898.empty _imagefilter@17065589.fromcolorf _double@0150898.fromintege _growablelist@0150898._literal2 _growablelist@0150898._ofgrowabl _list@0150898._ofefficie _growablelist@0150898._ofefficie _hashcollisionnode@38137193.fromcollis	lib/armeabi-v7a/libapp.so
appro@openssl.org	lib/arm64-v8a/libflutter.so
appro@openssl.org	apktool_out/lib/x86_64/libflutter.so
_imagefilter@17065589.composed _list@0150898.of _httpparser@16463476.responsepa _list@0150898._ofgrowabl _growablelist@0150898._literal5 authenticationscheme@16463476.fromstring _growablelist@0150898.withcapaci _growablelist@0150898._literal	

EMAIL	FILE
_future@5048458.immediate _compressednode@38137193.single _colorfilter@17065589.lineartosr _future@5048458.zonevalue _link@15069316.fromrawpat _nativesocket@15069316.normal _uri@0150898.directory _growablelist@0150898._literal8 _growablelist@0150898._literal3 _list@0150898._ofarray _uri@0150898.notsimple _assertionerror@0150898._create _invocationmirror@0150898._withtype _directory@15069316.fromrawpat _file@15069316.fromrawpat _growablelist@0150898._literal7 _uri@0150898.file _timer@1026248.periodic _list@0150898._ofother _imagefilter@17065589.blur _timer@1026248._internal _assetmanifestbin@374287047.fromstanda _list@0150898.generate _growablelist@0150898._literal4 ngstreamsubscription@5048458.zoned _colorfilter@17065589.srgbtoline _semanticsgeometry@320266271.root _growablelist@0150898._ofother _receiveportimpl@1026248.fromrawrec _growablelist@0150898._ofarray _typeerror@0150898._create _future@5048458.immediatee _growablelist@0150898.generate _bytebuffer@8027147._new _growablelist@0150898.of _growablelist@0150898._literal1 storationinformation@234124995.fromserial _list@0150898.empty _imagefilter@17065589.fromcolorf _double@0150898.fromintege _growablelist@0150898._literal2 _growablelist@0150898._ofgrowabl _list@0150898._ofefficie _growablelist@0150898._ofefficie _hashcollisionnode@38137193.fromcollis	apktool_out/lib/armeabi-v7a/libapp.so

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

HARDCODED SECRETS

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyAWgwsBtPrvMrVa0uzgPCqqq8NHshiwi7U"
"google_api_key" : "AIzaSyAWgwsBtPrvMrVa0uzgPCqqq8NHshiwi7U"
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy

SCAN LOGS

Timestamp	Event	Error
2026-02-16 11:40:50	Generating Hashes	OK
2026-02-16 11:40:50	Extracting APK	OK
2026-02-16 11:40:50	Unzipping	OK
2026-02-16 11:40:50	Parsing APK with androguard	OK

2026-02-16 11:40:50	Extracting APK features using aapt/aapt2	OK
2026-02-16 11:40:50	Getting Hardcoded Certificates/Keystores	OK
2026-02-16 11:40:51	Parsing AndroidManifest.xml	OK
2026-02-16 11:40:51	Extracting Manifest Data	OK
2026-02-16 11:40:51	Manifest Analysis Started	OK
2026-02-16 11:40:51	Performing Static Analysis on: Alliance One 4.0 (com.example.alliance_one)	OK
2026-02-16 11:40:52	Fetching Details from Play Store: com.example.alliance_one	OK
2026-02-16 11:40:52	Checking for Malware Permissions	OK
2026-02-16 11:40:52	Fetching icon path	OK
2026-02-16 11:40:52	Library Binary Analysis Started	OK
2026-02-16 11:40:52	Analyzing lib/x86_64/libapp.so	OK
2026-02-16 11:40:52	Analyzing lib/x86_64/libdatastore_shared_counter.so	OK

2026-02-16 11:40:52	Analyzing lib/x86_64/libflutter.so	OK
2026-02-16 11:40:52	Analyzing lib/armeabi-v7a/libapp.so	OK
2026-02-16 11:40:52	Analyzing lib/armeabi-v7a/libdatastore_shared_counter.so	OK
2026-02-16 11:40:52	Analyzing lib/armeabi-v7a/libflutter.so	OK
2026-02-16 11:40:52	Analyzing lib/arm64-v8a/libapp.so	OK
2026-02-16 11:40:52	Analyzing lib/arm64-v8a/libdatastore_shared_counter.so	OK
2026-02-16 11:40:52	Analyzing lib/arm64-v8a/libflutter.so	OK
2026-02-16 11:40:52	Analyzing apktool_out/lib/x86_64/libapp.so	OK
2026-02-16 11:40:53	Analyzing apktool_out/lib/x86_64/libdatastore_shared_counter.so	OK
2026-02-16 11:40:53	Analyzing apktool_out/lib/x86_64/libflutter.so	OK
2026-02-16 11:40:53	Analyzing apktool_out/lib/armeabi-v7a/libapp.so	OK
2026-02-16 11:40:53	Analyzing apktool_out/lib/armeabi-v7a/libdatastore_shared_counter.so	OK

2026-02-16 11:40:53	Analyzing apktool_out/lib/armeabi-v7a/libflutter.so	OK
2026-02-16 11:40:53	Analyzing apktool_out/lib/arm64-v8a/libapp.so	OK
2026-02-16 11:40:53	Analyzing apktool_out/lib/arm64-v8a/libdatastore_shared_counter.so	OK
2026-02-16 11:40:53	Analyzing apktool_out/lib/arm64-v8a/libflutter.so	OK
2026-02-16 11:40:53	Reading Code Signing Certificate	OK
2026-02-16 11:40:53	Running APKiD 3.0.0	OK
2026-02-16 11:40:56	Detecting Trackers	OK
2026-02-16 11:40:57	Decompiling APK to Java with JADX	OK
2026-02-16 11:41:00	Converting DEX to Smali	OK
2026-02-16 11:41:00	Code Analysis Started on - java_source	OK
2026-02-16 11:41:00	Android SBOM Analysis Completed	OK
2026-02-16 11:41:01	Android SAST Completed	OK

2026-02-16 11:41:01	Android API Analysis Started	OK
2026-02-16 11:41:07	Android API Analysis Completed	OK
2026-02-16 11:41:07	Android Permission Mapping Started	OK
2026-02-16 11:41:08	Android Permission Mapping Completed	OK
2026-02-16 11:41:08	Android Behaviour Analysis Started	OK
2026-02-16 11:41:09	Android Behaviour Analysis Completed	OK
2026-02-16 11:41:09	Extracting Emails and URLs from Source Code	OK
2026-02-16 11:41:10	Email and URL Extraction Completed	OK
2026-02-16 11:41:10	Extracting String data from APK	OK
2026-02-16 11:41:10	Extracting String data from SO	OK
2026-02-16 11:41:11	Extracting String data from Code	OK
2026-02-16 11:41:11	Extracting String values and entropies from Code	OK

2026-02-16 11:41:11	Performing Malware check on extracted domains	OK
2026-02-16 11:41:14	Saving to Database	OK