APP SCORES

Security Score **37/100**

Trackers Detection **6/432**

FILE INFORMATION

File Name MT_v25.11.28_r4546-release.apk

Size 15.74MB

MD5 493e552f3de7a3372b8fd6b5a6421776

SHA1 09bed2857175f009da0172f590e605adf971c786

SHA256 3c9f76d593c2bd3dab95a09084d5d885a84724cc52ba1f7daf30528d4d26b69f

APP INFORMATION

App Name MonTransit

Package Name org.mtransit.android

Main Activity org.mtransit.android.ui.SplashScreenActivity

Target SDK 35 Min SDK 24 Max SDK

Android Version Name 25.11.28r4546

Android Version Code 4546

PLAYSTORE INFORMATION

Title MonTransit

Score 4.2 Installs 1,000,000+ Price 0 Android Version Support Category Maps & Navigation Play Store URL org.mtransit.android

Developer MTransit Apps, Developer ID 4695172782869639778

Developer Address None

Developer Website https://mtransitapps.github.io/

Developer Email mtransit.apps@gmail.com

Release Date Feb 2, 2015 Privacy Policy Privacy link

Description

MonTransit effortlessly brings the most relevant transit information to you, including:
- buses, ferries, subways, streetcars & trains schedules (offline & real-time),
- bike stations availability,
- service alerts & the latest news from agencies web sites, blogs, Twitter, YouTube…

On the home screen, you can see all nearby route trips next departures as well as nearby bike stations availability in a predictable user interface.
You can access the information any way you want by using the sliding menu (click on the ☰ icon in the upper left corner of the screen or swipe from the left edge of any screen).
For example, you can use the Map screen to discover new bus stops, subway stations, train stations or bike stations or you can search for a place by clicking on the 🔍 icon in the upper right corner of any screen.

No Internet? GPS turned off? WiFi disabled? No problem, MonTransit offers multiple ways to find the information you're looking for:
- you can access your ★ favorites or browse all transit information by using the sliding menu (click on the ☰ icon in the upper left corner of the screen or swipe from the left edge of any screen)
- you can enter a route number # or name, stop code # or name, street names... by clicking on the search 🔍 icon in the upper right corner of any screen
- all buses, ferries, subways, streetcars & trains schedule are available offline

MonTransit lets you install the transit agencies that you want (you don't have to switch between cities & you can access all the information any time, anywhere).
The buses, ferries, subways, streetcars & trains information are kept up-to-date through Google Play Store auto-updates without using your device's battery or mobile Internet data plan (3G/4G/LTE).

MonTransit is currently available in Canada:
- AB: Calgary, ETS, Red Deer…
- BC: BC Transit, TransLink, West Coast Express…
- MB: Winnipeg, Brandon…
- NB: Codiac, Fredericton…
- NL: Metrobus…
- NS: Halifax…
- ON: GO Transit, GRT, HSR, MiWay, OC Transpo, TTC, YRT Viva, Niagara Region, St Catharines…

- QC: exo, BIXI, RTC, RTL, STM, STL, STO, STS…
- SK: Regina, Saskatoon…
- YK: Whitehorse…

MonTransit is currently available in the northern United States:
- AK: People Mover…

All the features are available for free (no paywall) but you can support the project (and hide ads) by paying a Google Play subscription (1 month free, cancel any time).

You are our customers & only source of revenues.
Thank You.

Social:
- Facebook: https://facebook.com/MonTransit
- Twitter: https://twitter.com/montransit

This app is free & open-source:
https://github.com/mtransitapps/mtransit-for-android

More information: https://bit.ly/MonTransitStats

Made with ♥ in Montreal, Canada in North America.

Permissions:
- In-app purchases: required for donations (hide ads & support MonTransit)
- Location: required to show nearby transit information & show distance & compass
- Photo/Media/Files: required by Google Maps
- Other: required by Google Analytics & Google Mobile Ads (AdMob) & Google Maps & Facebook Audience Network

2 / 40	1 / 11
EXPORTED ACTIVITIES	EXPORTED SERVICES
View All	View All
3 / 8	1 / 10
EXPORTED RECEIVERS	EXPORTED PROVIDERS
View All	View All

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: O=MonTransit Apps, CN=Mathieu Méa
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-09-30 14:48:16+00:00
Valid To: 2113-09-06 14:48:16+00:00
Issuer: O=MonTransit Apps, CN=Mathieu Méa
Serial Number: 0x61dec709
Hash Algorithm: sha256
md5: 6c73735ee5133a96d32d740584f0f0d9
sha1: ee6bb0756a02113fd46f2c434a06ebd5d04ff639
sha256: f8ea1dec24743662ef0243cdeb55f4a5085823e2a34ae0b140ac63012895da7a
sha512:
23a2e06b851fc95ba50e6eb95fedc89be22b404cb9545764078c67c143bc95dad373fa9db27b553b6c317a698ee1bf0dd1c035288c1331a6cad
3905e9698d248
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c301dbb39ee28390cb01c12c2e1f11cdca7e95415c885d9bbeca4917ec2c35fb
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CO MA
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.	
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.	

PERMISSION	STATUS	INFO	DESCRIPTION	CO MA
android.permission.ACCESS_ADSERVICES_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.	
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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CO MA
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.	
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.	

PERMISSION	STATUS	INFO	DESCRIPTION	CO MA
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.	

Showing 1 to 10 of 19 entries

Previous 1 2 Next

ANDROID API

Search:

API	FILES
Base64 Decode	
Base64 Encode	
Certificate Handling	
Content Provider	

API	FILES
Crypto	
Get Android Advertising ID	
Get Installed Applications	
Get Network Interface information	
Get Running App Processes	
Get System Service	

Showing 1 to 10 of 31 entries

Previous 1 2 3 4 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

NETWORK SECURITY

HIGH	WARNING	INFO	SECURE
1	0	2	0

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	octranspo.com	info	Domain config is configured to trust bundled certs @raw/com_octranspo_pem.
3	stm.info	info	Domain config is configured to trust bundled certs @raw/info_stm_pem.

Showing 1 to 3 of 3 entries

Previous 1 Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
0	0	1

Search:

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 1 of 1 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
1	8	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable unpatched Android version Android 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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
3	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.	
4	**Broadcast Receiver** (org.mtransit.android.receiver.ModulesReceiver) is not Protected. [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.	
5	**Broadcast Receiver** (org.mtransit.android.receiver.ModuleDataChangeReceiver) is Protected by a permission. **Permission:** org.mtransit.android.receiver.permission.BROADCAST_RECEIVER **protectionLevel:** signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
6	**Content Provider** (org.mtransit.android.commons.provider.RSSNewsProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	
7	**Activity** (org.mtransit.android.commons.ui.AppUpdateActivity) 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.	
8	**Activity** (org.mtransit.android.commons.ui.InvisibleActivity) 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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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.	

Showing 1 to 10 of 11 entries

Previous 1 2 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
4	6	1	1	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
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		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
2	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		
3	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		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
4	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	org/mtransit/android/commons/PreferenceUtils.java org/mtransit/android/datasource/DataSourcesReader.java	
5	The App uses an insecure Random Number Generator.	warning	**CWE:** CWE-330: Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
6	SHA-1 is a weak hash known to have hash collisions.	warning	**CWE:** CWE-327: Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	com/applovin/impl/sdk/utils/StringUtils.java com/applovin/impl/u4.java	
7	Remote WebView debugging is enabled.	high	**CWE:** CWE-919: Weaknesses in Mobile Applications **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-RESILIENCE-2	com/applovin/impl/adview/AppLovinWebViewBase.java com/applovin/impl/adview/l.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
8	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	**CWE:** CWE-295: Improper Certificate Validation **OWASP Top 10:** M3: Insecure Communication **OWASP MASVS:** MSTG-NETWORK-3	org/mtransit/android/ui/fragment/WebBrowserFragment.java	
9	The file or SharedPreference is World Readable. Any App can read from the file	high	**CWE:** CWE-276: Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	com/instagram/common/viewpoint/core/C0734Sn.java com/instagram/common/viewpoint/core/WR.java org/mtransit/android/ui/view/MapViewController.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
10	App can read/write to External Storage. Any App can read data written to External Storage.	warning	**CWE:** CWE-276: Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	com/vungle/ads/internal/platform/AndroidPlatform.java	

Showing 1 to 10 of 12 entries

Previous 1 2 Next

SHARED LIBRARY BINARY ANALYSIS

Search:

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNP/

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPA
1	arm64-v8a/libapplovin-native-crash-reporter.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 bi does n have RUNPA set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNP/

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPA
2	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 bi does n have RUNPA set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNP/

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPA
3	armeabi-v7a/libapplovin-native-crash-reporter.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 bi does n have RUNPA set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNP/

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPA
4	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 bi does n have RUNPA set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNP/

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPA
5	x86/libapplovin-native-crash-reporter.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 bi does n have RUNPA set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNP/

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPA
6	x86/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 bi does n have RUNPA set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNP/

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPA
7	x86_64/libapplovin-native-crash-reporter.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 bi does n have RUNPA set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNP/

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPA
8	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 bi does n have RUNPA set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNP/

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPA
9	arm64-v8a/libapplovin-native-crash-reporter.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 bi does n have RUNPA set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNP/

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPA
10	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 bi does n have RUNPA set.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNP/

Showing 1 to 10 of 16 entries

Previous 1 2 Next

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

FIREBASE DATABASE ANALYSIS

Search:

TITLE	SEVERITY	DESCRIPTION
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

MALWARE LOOKUP

VirusTotal Report | Triage Report | MetaDefender Report | Hybrid Analysis Report

APKiD ANALYSIS

Search:

DEX	DETECTIONS
assets/audience_network/classes.dex	Search:

FINDINGS	DETAILS
Compiler	unknown (please file detection issue!)

Showing 1 to 1 of 1 entries

Previous 1 Next

DEX	DETECTIONS
assets/audience_network/classes2.dex	Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Compiler	unknown (please file detection issue!)

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes.dex	

Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check possible VM check
Compiler	r8

Showing 1 to 3 of 3 entries

Previous 1 Next

DEX	DETECTIONS
classes2.dex	Search:

FINDINGS	DETAILS
Compiler	r8

Showing 1 to 1 of 1 entries

Previous 1 Next

DEX	DETECTIONS
classes3.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.HARDWARE check Build.TAGS check
Compiler	r8

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes4.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.PRODUCT check Build.BOARD check possible VM check
Compiler	r8

Showing 1 to 2 of 2 entries

Previous 1 Next

Showing 1 to 6 of 6 entries

Previous 1 Next

BEHAVIOUR ANALYSIS

Search:

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/instagram/common/viewpoint/core/C0745Sy.java
00003	Put the compressed bitmap data into JSON object	camera	com/instagram/common/viewpoint/core/C1509jj.java
00004	Get filename and put it to JSON object	file collection	com/applovin/impl/n7.java com/applovin/impl/sdk/l.java com/instagram/common/viewpoint/core/C0752Tf.java
00005	Get absolute path of file and put it to JSON object	file	com/applovin/impl/sdk/NativeCrashReporter.java
00009	Put data in cursor to JSON object	file	
00012	Read data and put it into a buffer stream	file	com/vungle/ads/internal/ui/VungleWebClient.java
00013	Read file and put it into a stream	file	
00014	Read file into a stream and put it into a JSON object	file	com/applovin/impl/n7.java com/instagram/common/viewpoint/core/C0752Tf.java com/instagram/common/viewpoint/core/C1132dM.java
00022	Open a file from given absolute path of the file	file	

RULE ID	BEHAVIOUR	LABEL	FILES
00023	Start another application from current application	reflection control	com/applovin/impl/k7.java org/mtransit/android/commons/PackageManagerUtils.java

Showing 1 to 10 of 31 entries

Previous 1 2 3 4 Next

ABUSED PERMISSIONS

Top Malware Permissions **7**/25

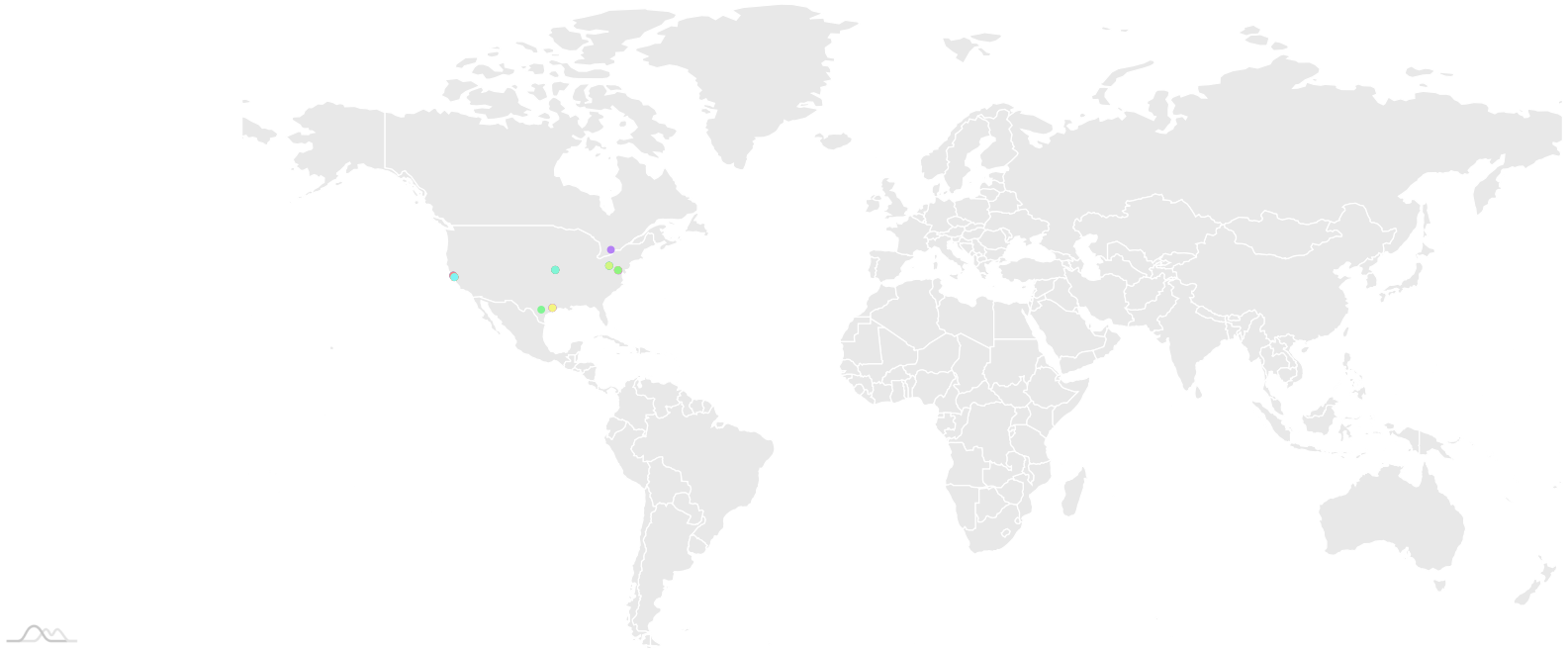
android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE

Other Common Permissions **3**/44

com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions are the top permissions that are widely abused by known malware.
Other Common Permissions are permissions that are commonly abused by known malware.

SERVER LOCATIONS



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

Search:

DOMAIN	COUNTRY/REGION
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

DOMAIN MALWARE CHECK

Search:

DOMAIN	STATUS	GEOLOCATION
a.applovin.com	ok	**IP:** 34.117.147.68 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
a.applvn.com	ok	**IP:** 34.117.147.68 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
adx.ads.vungle.com	ok	**IP:** 44.219.165.180 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
applovin.com	ok	**IP:** 34.54.184.105 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
assets.applovin.com	ok	**IP:** 34.120.175.182 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
b.applovin.com	ok	**IP:** 35.241.1.16 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
compliance.iabtechnologylab.com	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
config.ads.vungle.com	ok	**IP:** 34.231.53.90 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
d.applovin.com	ok	**IP:** 34.110.179.88 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
d.applvn.com	ok	**IP:** 34.110.179.88 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

Showing 1 to 10 of 45 entries

Previous 1 2 3 4 5 Next

URLS

Search:

URL	FILE
data:,	com/applovin/impl/l8.java
data:image	com/bumptech/glide/load/model/DataUrlLoader.java
http://developer.android.com/google/play-services/setup.html.	com/applovin/impl/v.java

URL	FILE
http://ipwho.is/	org/mtransit/android/ui/DaggerMTApplication_HiltComponents_SingletonC
http://schemas.android.com/apk/res/android	com/applovin/mediation/ads/MaxAdView.java
http://schemas.applovin.com/android/1.0	com/applovin/adview/AppLovinAdView.java
http://www.w3.org/tr/svg11/feature# http://www.w3.org/1999/xlink http://www.w3.org/2000/svg http://xmlpull.org/v1/doc/features.html#process-docdecl http://xml.org/sax/properties/lexical-handler http://xmlpull.org/v1/doc/features.html#process-namespaces http://xml.org/sax/features/external-parameter-entities http://xml.org/sax/features/external-general-entities	com/caverock/androidsvg/SVGParser.java
https://adx.ads.vungle.com/api/ads https://logs.ads.vungle.com/sdk/metrics https://logs.ads.vungle.com/sdk/error_logs	com/vungle/ads/internal/Constants.java
https://applovin.com.	com/applovin/impl/m3.java
https://compliance.iabtechnologylab.com/compliance-js/omid-validation-verification-script-v1-applovin-01102024.js	com/applovin/impl/k4.java

Showing 1 to 10 of 46 entries

Previous 1 2 3 4 5 Next

EMAILS

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
AppLovin (MAX and SparkLabs)	Advertisement, Identification, Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/72
Facebook Ads	Advertisement	https://reports.exodus-privacy.eu.org/trackers/65
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

TRACKER NAME	CATEGORIES	URL
IAB Open Measurement	Advertisement, Identification	https://reports.exodus-privacy.eu.org/trackers/328

Showing 1 to 6 of 6 entries

Previous 1 Next

POSSIBLE HARDCODED SECRETS

▶ Show all **4339** secrets

STRINGS

From APK Resource

From Code

▶ Show all **43113** strings

From Shared Objects

lib/arm64-v8a/libapplovin-native-crash-reporter.so

▶ Show all **546** strings

lib/arm64-v8a/libdatastore_shared_counter.so

▼ Showing all **3** strings
ro.arch
exynos9810
java/io/IOException

lib/armeabi-v7a/libapplovin-native-crash-reporter.so

▶ Show all **542** strings

lib/armeabi-v7a/libdatastore_shared_counter.so

▼ Showing all **1** strings
java/io/IOException

lib/x86/libapplovin-native-crash-reporter.so

▶ Show all **551** strings

lib/x86/libdatastore_shared_counter.so

▼ Showing all **1** strings
java/io/IOException

lib/x86_64/libapplovin-native-crash-reporter.so

▶ Show all **550** strings

lib/x86_64/libdatastore_shared_counter.so

▼ Showing all **1** strings

java/io/IOException

apktool_out/lib/arm64-v8a/libapplovin-native-crash-reporter.so

▶ Show all **546** strings

apktool_out/lib/arm64-v8a/libdatastore_shared_counter.so

▼ Showing all **3** strings
ro.arch
exynos9810
java/io/IOException

apktool_out/lib/armeabi-v7a/libapplovin-native-crash-reporter.so

▶ Show all **542** strings

apktool_out/lib/armeabi-v7a/libdatastore_shared_counter.so

▼ Showing all **1** strings
java/io/IOException

apktool_out/lib/x86/libapplovin-native-crash-reporter.so

▶ Show all **551** strings

apktool_out/lib/x86/libdatastore_shared_counter.so

▼ Showing all **1** strings
java/io/IOException

apktool_out/lib/x86_64/libapplovin-native-crash-reporter.so

▶ Show all **550** strings

apktool_out/lib/x86_64/libdatastore_shared_counter.so

▼ Showing all **1** strings

java/io/IOException

ACTIVITIES

▼ Showing all **40** activities

org.mtransit.android.ui.SplashScreenActivity
org.mtransit.android.ui.MainActivity
org.mtransit.android.ui.main.NextMainActivity
org.mtransit.android.ui.pref.PreferencesActivity
org.mtransit.android.ui.purchase.PurchaseActivity
org.mtransit.android.ui.modules.ModulesActivity
org.mtransit.android.commons.ui.AppUpdateActivity
org.mtransit.android.commons.ui.InvisibleActivity
com.google.android.libraries.places.widget.AutocompleteActivity
com.google.android.libraries.places.widget.BasicPlaceAutocompleteActivity
com.google.android.libraries.places.widget.PlaceAutocompleteActivity
com.google.android.libraries.places.widget.internal.photoviewer.PlacesLightboxActivity
com.google.android.gms.ads.AdActivity
com.google.android.gms.ads.OutOfContextTestingActivity
com.google.android.gms.ads.NotificationHandlerActivity
com.android.billingclient.api.ProxyBillingActivity
com.android.billingclient.api.ProxyBillingActivityV2
com.applovin.adview.AppLovinFullscreenActivity
com.applovin.adview.AppLovinFullscreenImmersiveActivity

com.applovin.sdk.AppLovinWebViewActivity
com.applovin.mediation.MaxDebuggerActivity
com.applovin.mediation.MaxDebuggerDetailActivity
com.applovin.mediation.MaxDebuggerMultiAdActivity
com.applovin.mediation.MaxDebuggerAdUnitsListActivity
com.applovin.mediation.MaxDebuggerAdUnitWaterfallsListActivity
com.applovin.mediation.MaxDebuggerAdUnitDetailActivity
com.applovin.mediation.MaxDebuggerCmpNetworksListActivity
com.applovin.mediation.MaxDebuggerTcfConsentStatusesListActivity
com.applovin.mediation.MaxDebuggerTcfInfoListActivity
com.applovin.mediation.MaxDebuggerTcfStringActivity
com.applovin.mediation.MaxDebuggerTestLiveNetworkActivity
com.applovin.mediation.MaxDebuggerTestModeNetworkActivity
com.applovin.mediation.MaxDebuggerUnifiedFlowActivity
com.applovin.mediation.MaxDebuggerWaterfallSegmentsActivity
com.applovin.creative.MaxCreativeDebuggerActivity
com.applovin.creative.MaxCreativeDebuggerDisplayedAdActivity
com.google.android.gms.common.api.GoogleApiActivity
com.facebook.ads.AudienceNetworkActivity
com.vungle.ads.internal.ui.VungleActivity
com.google.android.play.core.common.PlayCoreDialogWrapperActivity

SERVICES

▼ Showing all **11** services
androidx.appcompat.app.AppLocalesMetadataHolderService
com.google.android.gms.ads.AdService
androidx.work.impl.background.systemjob.SystemJobService

androidx.work.impl.foreground.SystemForegroundService
androidx.room.MultiInstanceInvalidationService
com.google.firebase.components.ComponentDiscoveryService
com.applovin.impl.adview.activity.FullscreenAdService
com.google.android.gms.measurement.AppMeasurementService
com.google.android.gms.measurement.AppMeasurementJobService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService

RECEIVERS

▼ Showing all **8** receivers
org.mtransit.android.receiver.ModulesReceiver
org.mtransit.android.receiver.ModuleDataChangeReceiver
androidx.work.impl.utils.ForceStopRunnable$BroadcastReceiver
androidx.work.impl.background.systemalarm.RescheduleReceiver
androidx.work.impl.diagnostics.DiagnosticsReceiver
com.google.android.gms.measurement.AppMeasurementReceiver
androidx.profileinstaller.ProfileInstallReceiver
com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver

PROVIDERS

▼ Showing all **10** providers
org.mtransit.android.provider.FavoriteProvider
org.mtransit.android.provider.ModuleProvider

org.mtransit.android.provider.PlaceProvider
org.mtransit.android.commons.provider.RSSNewsProvider
com.google.android.gms.ads.MobileAdsInitProvider
androidx.startup.InitializationProvider
com.applovin.sdk.AppLovinInitProvider
com.facebook.ads.AudienceNetworkContentProvider
com.google.firebase.provider.FirebaseInitProvider
com.vungle.ads.VungleProvider

LIBRARIES

▼ Showing all **4** libraries
org.apache.http.legacy
android.ext.adservices
androidx.window.extensions
androidx.window.sidecar

SBOM

▼ Showing all **87** Versioned Packages
androidx.activity:activity-ktx@1.12.0
androidx.activity:activity@1.12.0
androidx.annotation:annotation-experimental@1.5.0
androidx.appcompat:appcompat-resources@1.7.1
androidx.appcompat:appcompat@1.7.1
androidx.arch.core:core-runtime@dynamic
androidx.browser:browser@1.9.0
androidx.cardview:cardview@1.0.0

androidx.compose.runtime:runtime-annotation@1.9.0
androidx.constraintlayout:constraintlayout@2.2.1
androidx.coordinatorlayout:coordinatorlayout@1.3.0
androidx.core:core-ktx@1.17.0
androidx.core:core-splashscreen@1.2.0
androidx.core:core-viewtree@1.0.0
androidx.core:core@1.17.0
androidx.cursoradapter:cursoradapter@1.0.0
androidx.customview:customview-poolingcontainer@1.0.0
androidx.customview:customview@1.1.0
androidx.databinding:viewbinding@8.13.1
androidx.datastore:datastore-core@1.1.7
androidx.datastore:datastore-preferences-core@1.1.7
androidx.datastore:datastore-preferences@1.1.7
androidx.datastore:datastore@1.1.7
androidx.documentfile:documentfile@1.0.0
androidx.drawerlayout:drawerlayout@1.1.1
androidx.dynamicanimation:dynamicanimation@1.1.0
androidx.emoji2:emoji2-views-helper@1.3.0
androidx.emoji2:emoji2@1.3.0
androidx.exifinterface:exifinterface@1.3.6
androidx.fragment:fragment-ktx@1.8.9
androidx.fragment:fragment@1.8.9
androidx.graphics:graphics-shapes@1.0.1
androidx.interpolator:interpolator@1.0.0
androidx.legacy:legacy-support-core-utils@1.0.0
androidx.lifecycle:lifecycle-livedata-core-ktx@2.10.0
androidx.lifecycle:lifecycle-livedata-core@2.10.0
androidx.lifecycle:lifecycle-livedata@2.10.0
androidx.lifecycle:lifecycle-process@2.10.0

androidx.lifecycle:lifecycle-runtime-ktx@2.10.0
androidx.lifecycle:lifecycle-runtime@2.10.0
androidx.lifecycle:lifecycle-service@2.10.0
androidx.lifecycle:lifecycle-viewmodel-ktx@2.10.0
androidx.lifecycle:lifecycle-viewmodel-savedstate@2.10.0
androidx.lifecycle:lifecycle-viewmodel@2.10.0
androidx.loader:loader@1.0.0
androidx.localbroadcastmanager:localbroadcastmanager@1.0.0
androidx.navigation:navigation-common@2.9.6
androidx.navigation:navigation-fragment@2.9.6
androidx.navigation:navigation-runtime@2.9.6
androidx.navigation:navigation-ui@2.9.6
androidx.navigationevent:navigationevent@1.0.0
androidx.preference:preference-ktx@1.2.1
androidx.preference:preference@1.2.1
androidx.print:print@1.0.0
androidx.privacysandbox.ads:ads-adservices-java@1.1.0-beta11
androidx.privacysandbox.ads:ads-adservices@1.1.0-beta11
androidx.profileinstaller:profileinstaller@1.4.0
androidx.recyclerview:recyclerview@1.4.0
androidx.room:room-ktx@2.8.4
androidx.room:room-runtime@2.8.4
androidx.savedstate:savedstate-ktx@1.4.0
androidx.savedstate:savedstate@1.4.0
androidx.slidingpanelayout:slidingpanelayout@1.2.0
androidx.sqlite:sqlite-framework@2.6.2
androidx.sqlite:sqlite-ktx@2.6.2
androidx.sqlite:sqlite@2.6.2
androidx.startup:startup-runtime@1.2.0
androidx.swiperefreshlayout:swiperefreshlayout@1.1.0

androidx.tracing:tracing-ktx@1.2.0
androidx.tracing:tracing@1.2.0
androidx.transition:transition@1.5.0
androidx.vectordrawable:vectordrawable-animated@1.1.0
androidx.vectordrawable:vectordrawable@1.2.0
androidx.versionedparcelable:versionedparcelable@1.1.1
androidx.viewpager2:viewpager2@1.1.0
androidx.viewpager:viewpager@1.0.0
androidx.webkit:webkit@1.14.0
androidx.window:window@1.0.0
androidx.work:work-runtime@2.11.0
com.google.android.material:material@1.13.0
com.google.dagger:dagger-lint-aar@2.57.2
com.google.dagger:dagger@2.57.2
com.google.dagger:hilt-android@2.57.2
com.google.dagger:hilt-core@2.57.2
org.jetbrains.kotlinx:kotlinx-coroutines-android@1.10.2
org.jetbrains.kotlinx:kotlinx-coroutines-core@1.10.2
org.jetbrains.kotlinx:kotlinx-coroutines-play-services@1.10.2

▼ Showing all **37** Packages

android.app
android.content.pm
android.graphics
android.media
android.os
android.telephony
android.view
android.webkit
android.window
com.applovin.adview

com.applovin.communicator
com.applovin.creative
com.applovin.impl
com.applovin.mediation
com.applovin.sdk
com.applovin.shadow.okio
com.bumptech.glide
com.caverock.androidsvg
com.chuckerteam.chucker.api
com.iab.omid.library.applovin
com.iab.omid.library.vungle
com.instagram.common.viewpoint.core
com.vungle.ads
com.vungle.mediation
dagger.hilt
dagger.internal
javax.annotation
javax.inject
okio
org.checkerframework.checker.nullness.qual
org.checkerframework.dataflow.qual
org.checkerframework.framework.qual
org.jacoco.core.data
org.mtransit.android
org.mtransit.commons
org.objectweb.asm
retrofit2

FILES

▶ Show all **1566** files

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity. **Version** v4.4.3