APP SCORES

No icon

Security Score **46/100**

Trackers Detection **0/432**

FILE INFORMATION

File Name app-debug-androidTest.apk

Size 0.53MB

MD5 3b74f98f50e764cc138e7bb98cd92cc7

SHA1 189ad8835e6b7a0d1104b4a3773fde616a62875c

SHA256 503f53dfac61cf296127919fa5a7f22a5f524d9e0c1aee5a45d9e44ceb4e3c25

APP INFORMATION

App Name

Package Name com.example.gpsmaps.test

Main Activity androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity

Target SDK 34 Min SDK 27 Max SDK

Android Version Name Android Version Code

3	0	0	0
ACTIVITIES	SERVICES	RECEIVERS	PROVIDERS
View	View	View	View

Exported Activities	Exported Services	Exported Receivers	Exported Providers
2	0	0	0

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
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: 2024-09-12 01:38:41+00:00
Valid To: 2054-09-05 01:38:41+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: 1da3a7bb8ecedaf048f5c6729004c771
sha1: a36611411df0ec7cfe74b5b1d5a67d8779c497c1
sha256: 5e4208ef04c9f67d368c9f8fb794f352c30b9e4bbeebfe709f22c089a1284fe3
sha512:
5454b58eb08f87dd0a332bd459d062b60351ec5ac404446035c9dac33c55500719dd1d3627b6a2c392f3e4f14a2e8abd7b4a951180fe1c8ba213f217c5e
c7f1f
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 716f2c618fb79cea6be9abead700fffaa01fe03948c581f1ef34d73d6ed13a40
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.	

Showing 1 to 1 of 1 entries

Previous 1 Next

ANDROID API

Search:

API	FILES
Java Reflection	
Local File I/O Operations	

Showing 1 to 2 of 2 entries

Previous 1 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

NETWORK SECURITY

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
No data available in table			

Showing 0 to 0 of 0 entries

Previous Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
1	0	1

Search:

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

Showing 1 to 2 of 2 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
1	4	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable Android version Android 8.1, minSdk=27]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.	
2	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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	**Activity** (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) 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
5	**Activity** (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) 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.	

Showing 1 to 5 of 5 entries

Previous 1 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
0	2	1	0	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	junit/runner/BaseTestRunner.java junit/runner/Version.java junit/textui/TestRunner.java	
2	The App uses an insecure Random Number Generator.	warning	**CWE:** CWE-330: Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6	org/junit/runner/manipulation/Ordering.java	
3	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	org/junit/rules/TemporaryFolder.java	

Showing 1 to 3 of 3 entries

SHARED LIBRARY BINARY ANALYSIS

No Shared Objects found.

Search:

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
No data available in table								

Showing 0 to 0 of 0 entries

Previous 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

APKiD ANALYSIS

Search:

DEX	DETECTIONS
classes.dex	Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.HARDWARE check
Compiler	r8 without marker (suspicious)

Showing 1 to 3 of 3 entries

Previous 1 Next

classes2.dex

Search:

FINDINGS	DETAILS
Compiler	dx

Showing 1 to 1 of 1 entries

Previous 1 Next

DEX	DETECTIONS
classes3.dex	Search:

FINDINGS	DETAILS
Compiler	unknown (please file detection issue!)

Showing 1 to 1 of 1 entries

Previous 1 Next

Showing 1 to 3 of 3 entries

Previous 1 Next

QUARK ANALYSIS

Search:

POTENTIAL MALICIOUS BEHAVIOUR	EVIDENCE
No data available in table	

Showing 0 to 0 of 0 entries

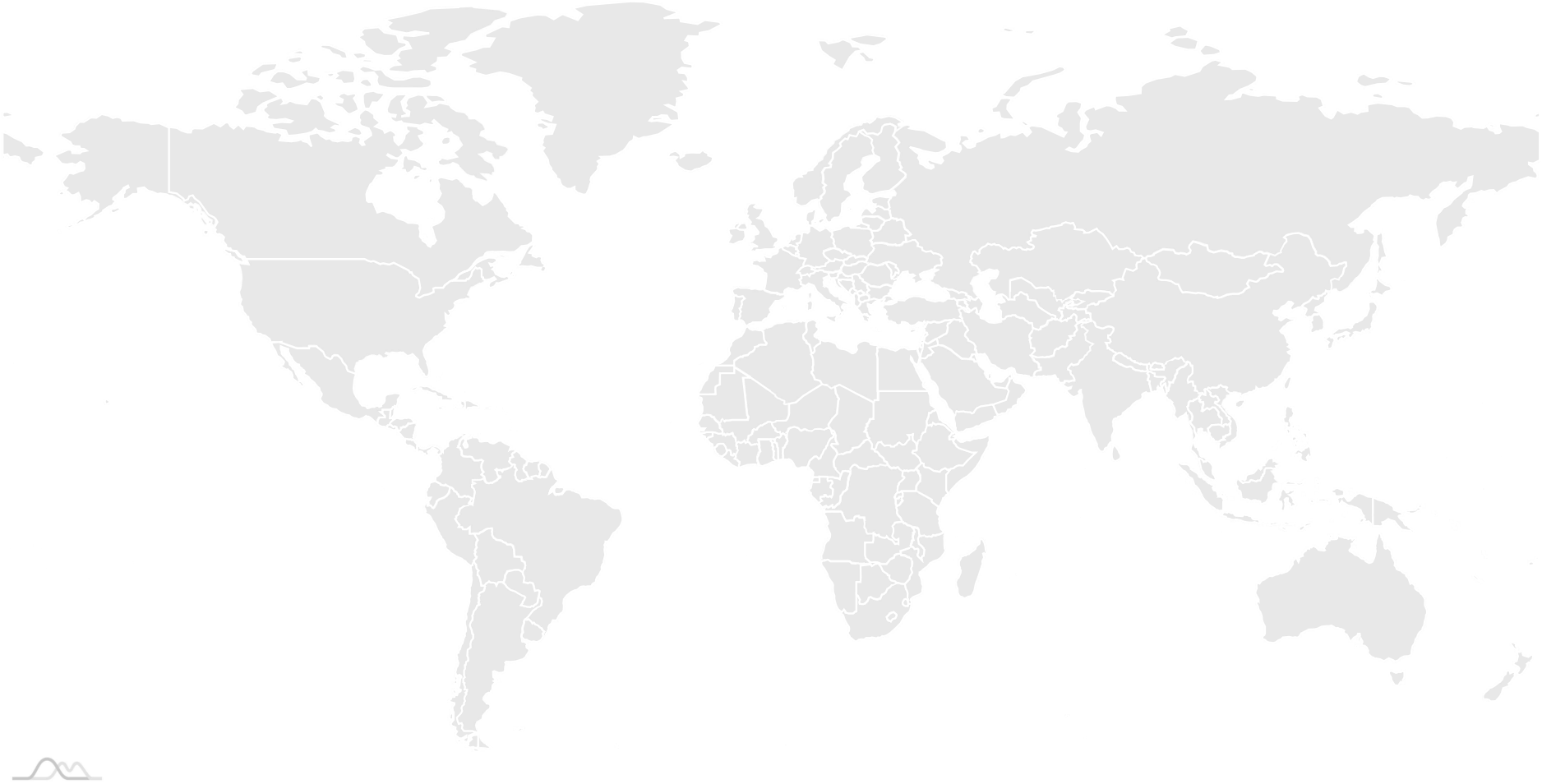
Previous Next

ABUSED PERMISSIONS

Top Malware Permissions	0/24	Other Common Permissions	0/4

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



DOMAIN MALWARE CHECK

URLS

FIREBASE DATABASE

EMAILS

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

POSSIBLE HARDCODED SECRETS

STRINGS

From APK Resource

From Code

▶ Show all **1592** strings

From Shared Objects

ACTIVITIES

▼ Showing all **3** activities
androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity
androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity
androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity

SERVICES

RECEIVERS

PROVIDERS

LIBRARIES

▼ Showing all **1** libraries
android.test.runner

FILES

▼ Showing all **8** files
AndroidManifest.xml
resources.arsc
classes3.dex
classes2.dex
LICENSE-junit.txt
junit/runner/logo.gif
junit/runner/smalllogo.gif
classes.dex

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.

Version v4.0.7