



## ANDROID STATIC ANALYSIS REPORT



 TapTapSee (3.3.4.5)

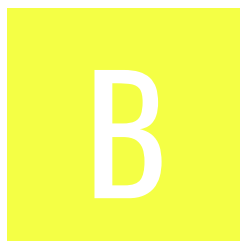
File Name: TapTapSee\_3.3.4.5\_APKPure.apk

Package Name: com.msearcher.taptapsee.android

Scan Date: Nov. 23, 2024, 4:07 p.m.






App Security Score: 52/100 (MEDIUM RISK)

Grade:



Trackers Detection: 5/432

## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	11	2	2	2

## FILE INFORMATION

**File Name:** TapTapSee\_3.3.4.5\_APKPure.apk

**Size:** 6.5MB

**MD5:** 82842902ada4396c160cc7ca0cdbfaf9

**SHA1:** 8037e0e6e92bd9475f28d77b0ded4b2111eaadac

**SHA256:** 8642a63e925c3e87c9b423baf7e8052c081e867bcad648e5871d95cae7adcaa7

## APP INFORMATION

**App Name:** TapTapSee

**Package Name:** com.msearcher.taptapsee.android

**Main Activity:** com.msearcher.taptapsee.activity.SplashActivity

**Target SDK:** 33

**Min SDK:** 19

**Max SDK:**

**Android Version Name:** 3.3.4.5

Android Version Code: 120

## APP COMPONENTS

Activities: 6

Services: 8

Receivers: 5

Providers: 3

Exported Activities: 0

Exported Services: 0

Exported Receivers: 1

Exported Providers: 0

## CERTIFICATE INFORMATION

Binary is signed

v1 signature: True

v2 signature: True

v3 signature: False

v4 signature: False

X.509 Subject: CN=taptapsee

Signature Algorithm: rsassa\_pkcs1v15

Valid From: 2014-03-01 13:50:20+00:00

Valid To: 2214-01-12 13:50:20+00:00

Issuer: CN=taptapsee

Serial Number: 0x7748b659

Hash Algorithm: sha256

md5: cbaa2fb9aa98a1889fc9187ab65b11ca

sha1: 843f31ea9ffd0b811a33a82f6bcdcb496dbbd4169

sha256: 3c9d7d1783b03d8efb1880a0c425d1fb96743f04110fd1a043966d3a656192bb

sha512: 2dac65bad04d7c0139473e5edd6932c12234d8aa909f8b026e0d881b192e5d17acc6589737953df22bac49b82d96a82fa06cf215412b98005bc5932befc83558

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 5755eeb0587acff3444a5bcbcbf91d6f635a99ba3f15f456ee55be76f9c760a3

Found 1 unique certificates

## ☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
com.google.android.marvin.talkback.PERMISSION_SEND_INTENT_BROADCAST_COMMANDS_TO_TALKBACK	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_DOWNLOAD_MANAGER	unknown	Unknown permission	Unknown permission from android reference
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.msearcher.taptapsee.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference



FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)
classes2.dex	FINDINGS	DETAILS
	Anti-VM Code	possible Build.SERIAL check network operator name check
	Compiler	r8 without marker (suspicious)

HIGH: 0 | WARNING: 1 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	warning	Base config is configured to trust system certificates.

## CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

## MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.4-4.4.4, [minSdk=19]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_configuration]	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.
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 (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.

## </> CODE ANALYSIS

HIGH: 0 | WARNING: 6 | INFO: 1 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
----	-------	----------	-----------	-------

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/common/DateConversion.java com/common/ImageUtil.java com/common/ImageUtil_old.java com/common/MyLocation.java com/msearcher/taptapsee/activity/TaptapseeActivity.java com/msearcher/taptapsee/appirater/Appirater.java com/msearcher/taptapsee/customview/AllCapsTransformationMethod.java com/msearcher/taptapsee/customview/RoundedDrawable.java com/msearcher/taptapsee/customview/UiUtil.java com/msearcher/taptapsee/fragment/CameraFragment.java com/msearcher/taptapsee/gallery/BaseImage.java com/msearcher/taptapsee/gallery/BaseImageList.java com/msearcher/taptapsee/gallery/ImageManager.java com/msearcher/taptapsee/gallery/Util.java com/msearcher/taptapsee/gallery/VideoObject.java com/msearcher/taptapsee/home/ImageManager.java com/msearcher/taptapsee/oauth/OAuth.java com/msearcher/taptapsee/oauth/signature/OAuthSignatureMethod.java crittercism/android/c.java crittercism/android/di.java crittercism/android/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	<a href="#">App can read/write to External Storage. Any App can read data written to External Storage.</a>	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/common/ImageUtil.java com/common/ImageUtil_old.java com/msearcher/taptapsee/fragment/CameraFragment.java com/msearcher/taptapsee/gallery/ImageManager.java com/msearcher/taptapsee/home/ImageManager.java com/msearcher/taptapsee/util/DownloadHelper.java crittercism/android/bo.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/msearcher/taptapsee/android/BuildConfig.java
4	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/common/SharedPrefsUtil.java com/msearcher/taptapsee/constants/Constants.java com/msearcher/taptapsee/oauth/OAuth.java com/msearcher/taptapsee/oauth/OAuthConsumer.java com/msearcher/taptapsee/oauth/signature/RSA_SHA1.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java
5	<a href="#">SHA-1 is a weak hash known to have hash collisions.</a>	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/msearcher/taptapsee/oauth/signature/RSA_SHA1.java com/msearcher/taptapsee/util/DeviceId.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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	com/msearcher/taptapsee/activity/TaptapseeActivity.java
7	<a href="#">The App uses an insecure Random Number Generator.</a>	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/msearcher/taptapsee/util/DeviceId.java
8	<a href="#">This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.</a>	secure	OWASP MASVS: MSTG-NETWORK-4	com/msearcher/taptapsee/api/TapTapSeeApi.java

## SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libkeys.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) <a href="#">info</a></p> <p>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.</p>	<p>False <a href="#">high</a></p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO <a href="#">info</a></p> <p>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.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	x86/libkeys.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) <a href="#">info</a></p> <p>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.</p>	<p>False <a href="#">high</a></p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO <a href="#">info</a></p> <p>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.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libkeys.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) <a href="#">info</a></p> <p>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.</p>	<p>False <a href="#">high</a></p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO <a href="#">info</a></p> <p>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.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86_64/libkeys.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) <a href="#">info</a></p> <p>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.</p>	<p>False <a href="#">high</a></p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO <a href="#">info</a></p> <p>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.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	armeabi-v7a/libkeys.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) <a href="#">info</a></p> <p>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.</p>	<p>False <a href="#">high</a></p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO <a href="#">info</a></p> <p>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.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86/libkeys.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) <a href="#">info</a></p> <p>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.</p>	<p>False <a href="#">high</a></p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO <a href="#">info</a></p> <p>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.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libkeys.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) <a href="#">info</a></p> <p>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.</p>	<p>False <a href="#">high</a></p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO <a href="#">info</a></p> <p>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.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/libkeys.so	<p>True <a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>Dynamic Shared Object (DSO) <a href="#">info</a></p> <p>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.</p>	<p>False <a href="#">high</a></p> <p>This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.</p>	<p>Full RELRO <a href="#">info</a></p> <p>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.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

# NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

## BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/common/ImageUtil.java com/common/ImageUtil_old.java com/crittercism/app/CrittercismNDK.java com/msearcher/taptapsee/fragment/CameraFragment.java com/msearcher/taptapsee/util/DownloadHelper.java com/msearcher/taptapsee/util/IntentHelper.java crittercism/android/bj.java crittercism/android/cp.java crittercism/android/dm.java crittercism/android/h.java
00013	Read file and put it into a stream	file	com/common/ImageUtil.java com/common/ImageUtil_old.java com/msearcher/taptapsee/oauth/signature/pem/PEMReader.java com/msearcher/taptapsee/util/Utils.java crittercism/android/bp.java crittercism/android/bq.java crittercism/android/bu.java okio/Okio__vmOkioKt.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/msearcher/taptapsee/activity/AppSettingsActivity.java com/msearcher/taptapsee/activity/TaptapseeActivity.java com/msearcher/taptapsee/appirater/Appirater.java com/msearcher/taptapsee/util/IntentHelper.java crittercism/android/ay.java
00162	Create InetAddress object and connecting to it	socket	crittercism/android/ac.java
00163	Create new Socket and connecting to it	socket	crittercism/android/aa.java crittercism/android/ac.java
00183	Get current camera parameters and change the setting.	camera	com/msearcher/taptapsee/customview/AllCapsTransformationMethod.java com/msearcher/taptapsee/customview/CameraPreview.java com/msearcher/taptapsee/fragment/CameraFragment.java com/msearcher/taptapsee/util/CameraUtil.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/msearcher/taptapsee/gallery/ImageManager.java com/msearcher/taptapsee/home/ImageManager.java
00112	Get the date of the calendar event	collection calendar	com/common/DateConversion.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/msearcher/taptapsee/appirater/Appirater.java crittercism/android/ay.java
00036	Get resource file from res/raw directory	reflection	com/msearcher/taptapsee/appirater/Appirater.java crittercism/android/ay.java
00002	Open the camera and take picture	camera	com/msearcher/taptapsee/fragment/CameraFragment.java
00195	Set the output path of the recorded file	record file	com/msearcher/taptapsee/fragment/CameraFragment.java



RULE ID	BEHAVIOUR	LABEL	FILES
00199	Stop recording and release recording resources	record	com/msearcher/taptapsee/fragment/CameraFragment.java
00198	Initialize the recorder and start recording	record	com/msearcher/taptapsee/fragment/CameraFragment.java
00007	Use absolute path of directory for the output media file path	file	com/msearcher/taptapsee/fragment/CameraFragment.java
00006	Scheduling recording task	record	com/msearcher/taptapsee/fragment/CameraFragment.java
00041	Save recorded audio/video to file	record	com/msearcher/taptapsee/fragment/CameraFragment.java
00147	Get the time of current location	collection location	com/common/MyLocation.java
00075	Get location of the device	collection location	com/common/MyLocation.java
00115	Get last known location of the device	collection location	com/common/MyLocation.java
00096	Connect to a URL and set request method	command network	crittercism/android/cu.java crittercism/android/g.java
00089	Connect to a URL and receive input stream from the server	command network	crittercism/android/cu.java
00109	Connect to a URL and get the response code	network command	crittercism/android/cu.java crittercism/android/g.java
00094	Connect to a URL and read data from it	command network	crittercism/android/cu.java
00108	Read the input stream from given URL	network command	crittercism/android/cu.java

RULE ID	BEHAVIOUR	LABEL	FILES
00192	Get messages in the SMS inbox	sms	com/msearcher/taptapsee/activity/TaptapseeActivity.java
00078	Get the network operator name	collection telephony	crittercism/android/bo.java
00033	Query the IMEI number	collection	crittercism/android/dd.java
00014	Read file into a stream and put it into a JSON object	file	crittercism/android/bu.java
00004	Get filename and put it to JSON object	file collection	crittercism/android/bu.java

## FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at <a href="https://taptapsee-cc0f3.firebaseio.com">https://taptapsee-cc0f3.firebaseio.com</a>
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for <a href="https://firebase-remoteconfig.googleapis.com/v1/projects/273754017222/namespaces/firebase:fetch?key=AlzaSyDKJfMEnf4AxO3-b9u3MOMOU0BIJBzLzU">https://firebase-remoteconfig.googleapis.com/v1/projects/273754017222/namespaces/firebase:fetch?key=AlzaSyDKJfMEnf4AxO3-b9u3MOMOU0BIJBzLzU</a> . This is indicated by the response: {'state': 'NO_TEMPLATE'}

## ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.ACCESS_WIFI_STATE, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.RECORD_AUDIO
Other Common Permissions	5/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FLASHLIGHT, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

**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
--------	--------	-------------

DOMAIN	STATUS	GEOLOCATION
www.googleapis.com	ok	<b>IP:</b> 216.58.209.170 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
api.taptapseeapp.com	ok	<b>IP:</b> 34.95.125.151 <b>Country:</b> United States of America <b>Region:</b> Missouri <b>City:</b> Kansas City <b>Latitude:</b> 39.099731 <b>Longitude:</b> -94.578568 <b>View:</b> <a href="#">Google Map</a>
www.google.com	ok	<b>IP:</b> 216.58.211.228 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
www.protocol.http.httpurlconnectionimpl	ok	No Geolocation information available.
apm.crittercism.com	ok	No Geolocation information available.
www.protocol.https.httpsurlconnectionimpl	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
market.android.com	ok	<b>IP:</b> 216.58.211.238 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
github.com	ok	<b>IP:</b> 140.82.121.3 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
www.protocol.http.httpurlconnection	ok	No Geolocation information available.
taptapsee-cc0f3.firebaseio.com	ok	<b>IP:</b> 35.201.97.85 <b>Country:</b> United States of America <b>Region:</b> Missouri <b>City:</b> Kansas City <b>Latitude:</b> 39.099731 <b>Longitude:</b> -94.578568 <b>View:</b> <a href="#">Google Map</a>
www.protocol.https.httpsurlconnection	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api.cloudsight.ai	ok	<b>IP:</b> 34.95.125.151 <b>Country:</b> United States of America <b>Region:</b> Missouri <b>City:</b> Kansas City <b>Latitude:</b> 39.099731 <b>Longitude:</b> -94.578568 <b>View:</b> <a href="#">Google Map</a>
www.amazon.com	ok	<b>IP:</b> 23.36.158.146 <b>Country:</b> Netherlands <b>Region:</b> Noord-Holland <b>City:</b> Amsterdam <b>Latitude:</b> 52.374031 <b>Longitude:</b> 4.889690 <b>View:</b> <a href="#">Google Map</a>
api.crittercism.com	ok	No Geolocation information available.
www.taptapseeapp.com	ok	<b>IP:</b> 34.120.73.174 <b>Country:</b> United States of America <b>Region:</b> Missouri <b>City:</b> Kansas City <b>Latitude:</b> 39.099731 <b>Longitude:</b> -94.578568 <b>View:</b> <a href="#">Google Map</a>



EMAIL	FILE
support@crittercism.com	crittercism/android/ay.java
support@crittercism.com	com/crittercism/app/Crittercism.java
contact@taptapseeapp.com	Android String Resource

## TRACKERS

TRACKER	CATEGORIES	URL
Aptelligent by VMWare (formerly Crittercism)		<a href="https://reports.exodus-privacy.eu.org/trackers/155">https://reports.exodus-privacy.eu.org/trackers/155</a>
Google Analytics	Analytics	<a href="https://reports.exodus-privacy.eu.org/trackers/48">https://reports.exodus-privacy.eu.org/trackers/48</a>
Google CrashLytics	Crash reporting	<a href="https://reports.exodus-privacy.eu.org/trackers/27">https://reports.exodus-privacy.eu.org/trackers/27</a>
Google Firebase Analytics	Analytics	<a href="https://reports.exodus-privacy.eu.org/trackers/49">https://reports.exodus-privacy.eu.org/trackers/49</a>
Google Tag Manager	Analytics	<a href="https://reports.exodus-privacy.eu.org/trackers/105">https://reports.exodus-privacy.eu.org/trackers/105</a>

## HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"

POSSIBLE SECRETS
"google_api_key" : "AlzaSyDKJfMEnf4AxO3-b9u3MOmOU0BIJBzLzU"
"firebase_database_url" : "https://taptapsee-cc0f3.firebaseio.com"
"google_crash_reporting_api_key" : "AlzaSyDKJfMEnf4AxO3-b9u3MOmOU0BIJBzLzU"
5410e42f83fb7914a1000007
258EAF5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcd9735803434cec591fa

## PLAYSTORE INFORMATION

**Title:** TapTapSee

**Score:** 3.75 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Tools **Play Store URL:** [com.msearcher.taptapsee.android](https://play.google.com/store/apps/details?id=com.msearcher.taptapsee.android)

**Developer Details:** CloudSight Inc., CloudSight+Inc., 5455 Wilshire Blvd. Unit #1111 Los Angeles, CA 90036, <https://taptapseeapp.com>, [contact@taptapseeapp.com](mailto:contact@taptapseeapp.com),

**Release Date:** Apr 4, 2014 **Privacy Policy:** [Privacy link](#)

### Description:

TapTapSee is designed to help the blind and visually impaired identify objects they encounter in their daily lives. Simply double tap the screen to take a photo of anything, at any angle, and hear the app speak the identification back to you (Note: Spoken identification requires Talkback to be turned on). TapTapSee helps the blind and visually impaired become more independent in their day-to-day activities. FEATURES \* Flash toggle \* Auto-focus notification \* Identify images from your Camera Roll \* Repeat last image identification \* Share identification via text, email, or social media

## SCAN LOGS



Timestamp	Event	Error
2024-11-23 16:07:06	Generating Hashes	OK
2024-11-23 16:07:06	Extracting APK	OK
2024-11-23 16:07:06	Unzipping	OK
2024-11-23 16:07:06	Getting Hardcoded Certificates/Keystores	OK
2024-11-23 16:07:07	Parsing APK with androguard	OK
2024-11-23 16:07:11	Parsing AndroidManifest.xml	OK
2024-11-23 16:07:11	Extracting Manifest Data	OK
2024-11-23 16:07:11	Manifest Analysis Started	OK
2024-11-23 16:07:11	Reading Network Security config from network_security_configuration.xml	OK
2024-11-23 16:07:11	Parsing Network Security config	OK

2024-11-23 16:07:12	Performing Static Analysis on: TapTapSee (com.msearcher.taptapsee.android)	OK
2024-11-23 16:07:12	Fetching Details from Play Store: com.msearcher.taptapsee.android	OK
2024-11-23 16:07:13	Checking for Malware Permissions	OK
2024-11-23 16:07:13	Fetching icon path	OK
2024-11-23 16:07:13	Library Binary Analysis Started	OK
2024-11-23 16:07:13	Analyzing apktool_out/lib/armeabi-v7a/libkeys.so	OK
2024-11-23 16:07:13	Analyzing apktool_out/lib/x86/libkeys.so	OK
2024-11-23 16:07:13	Analyzing apktool_out/lib/arm64-v8a/libkeys.so	OK
2024-11-23 16:07:13	Analyzing apktool_out/lib/x86_64/libkeys.so	OK
2024-11-23 16:07:13	Analyzing lib/armeabi-v7a/libkeys.so	OK
2024-11-23 16:07:13	Analyzing lib/x86/libkeys.so	OK

2024-11-23 16:07:13	Analyzing lib/arm64-v8a/libkeys.so	OK
2024-11-23 16:07:13	Analyzing lib/x86_64/libkeys.so	OK
2024-11-23 16:07:13	Reading Code Signing Certificate	OK
2024-11-23 16:07:14	Running APKiD 2.1.5	OK
2024-11-23 16:07:18	Detecting Trackers	OK
2024-11-23 16:07:22	Decompiling APK to Java with JADX	OK
2024-11-23 16:08:17	Converting DEX to Smali	OK
2024-11-23 16:08:17	Code Analysis Started on - java_source	OK
2024-11-23 16:08:55	Android SAST Completed	OK
2024-11-23 16:08:55	Android API Analysis Started	OK
2024-11-23 16:08:57	Android API Analysis Completed	OK

2024-11-23 16:08:58	Android Permission Mapping Started	OK
2024-11-23 16:09:01	Android Permission Mapping Completed	OK
2024-11-23 16:09:02	Android Behaviour Analysis Started	OK
2024-11-23 16:09:04	Android Behaviour Analysis Completed	OK
2024-11-23 16:09:04	Extracting Emails and URLs from Source Code	OK
2024-11-23 16:09:06	Email and URL Extraction Completed	OK
2024-11-23 16:09:06	Extracting String data from APK	OK
2024-11-23 16:09:06	Extracting String data from SO	OK
2024-11-23 16:09:06	Extracting String data from Code	OK
2024-11-23 16:09:06	Extracting String values and entropies from Code	OK
2024-11-23 16:09:10	Performing Malware check on extracted domains	OK

2024-11-23 16:09:12	Saving to Database	OK
---------------------	--------------------	----

---

**Report Generated by - MobSF v4.2.4**

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

© 2024 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).