



ANDROID STATIC ANALYSIS REPORT



 Open Camera (1.49.2)

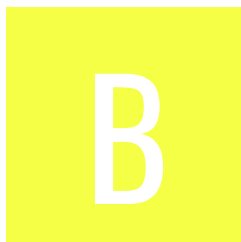
File Name: OpenCamera.apk

Package Name: net.sourceforge.opencamera





Scan Date: March 2, 2022, 1:14 p.m.

App Security Score: **56/100 (MEDIUM RISK)**

Grade:



FINDINGS SEVERITY

 HIGH	 WARNING	 INFO	 SECURE
0	10	2	1

FILE INFORMATION

File Name: OpenCamera.apk

Size: 3.67MB

MD5: 0def71b2f07912b9a71026b84005a311

SHA1: 1ec16466c3f076a5c3d0d13f32c6fc3ef7ebd88c

SHA256: 429121640e16491eef1f939a0013c10e762c2d4ccb40804a9d3bca1ab6979291

APP INFORMATION

App Name: Open Camera

Package Name: net.sourceforge.opencamera

Main Activity: net.sourceforge.opencamera.MainActivity

Target SDK: 30

Min SDK: 15

Max SDK:

Android Version Name: 1.49.2

Android Version Code: 83

APP COMPONENTS

Activities: 3

Services: 4

Receivers: 2

Providers: 1

Exported Activities: 0

Exported Services: 3

Exported Receivers: 2

Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed

v1 signature: True

v2 signature: True

v3 signature: False

Found 1 unique certificates

Subject: C=UK, ST=Cambridgeshire, L=Cambridge, O=Mark Harman, OU=Mark Harman, CN=Mark Harman

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2012-04-01 18:21:23+00:00

Valid To: 2039-08-18 18:21:23+00:00

Issuer: C=UK, ST=Cambridgeshire, L=Cambridge, O=Mark Harman, OU=Mark Harman, CN=Mark Harman

Serial Number: 0x60f79e2a

Hash Algorithm: sha256

md5: fd016318030f9b5c852b9ee988a1dbeb

sha1: fc5d0093f21a8fa91ef702526de0b39cc50ae59e

sha256: ff4b85f5037ab16f535ae5a1272697abcf96f0faa0e0c7ac37b2ed5c894e588

sha512: 76b3227b96f6006c9f6508110e13d5589d43a1b3d79acbea9ce5def3814363248fea06e7e601237525e62f6fd70baca0f84502ee296da77a1f4ef3b879b17fe5

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: ae3f39d5768bc828b160eb6575652ec4ad073a29ebcee1a068ec7897b716a8a4

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.

≡ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to 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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.

APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check
	Compiler	r8 without marker (suspicious)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Broadcast Receiver (net.sourceforge.opencamera.MyWidgetProvider) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
3	Broadcast Receiver (net.sourceforge.opencamera.MyWidgetProviderTakePhoto) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
4	Service (net.sourceforge.opencamera.MyTileService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_QUICK_SETTINGS_TILE [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.
5	Service (net.sourceforge.opencamera.MyTileServiceVideo) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_QUICK_SETTINGS_TILE [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
6	<p>Service (net.sourceforge.opencamera.MyTileServiceFrontCamera) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: android.permission.BIND_QUICK_SETTINGS_TILE [android:exported=true]</p>	warning	<p>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.</p>

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	net/sourceforge/opencamera/cameracontroller/CameraController1.java net/sourceforge/opencamera/MyApplicationInterface.java net/sourceforge/opencamera/MainActivity.java net/sourceforge/opencamera/preview/VideoQualityHandler.java net/sourceforge/opencamera/LocationSupplier.java net/sourceforge/opencamera/cameracontroller/CameraControllerManager1.java net/sourceforge/opencamera/ui/DrawPreview.java net/sourceforge/opencamera/SpeechControl.java net/sourceforge/opencamera/ui/MainUI.java net/sourceforge/opencamera/remotecomotecontrol/BluetoothLeService.java net/sourceforge/opencamera/ImageSaver.java net/sourceforge/opencamera/MyPreferenceFragment.java net/sourceforge/opencamera/HDRProcessor.java net/sourceforge/opencamera/SettingsManager.java net/sourceforge/opencamera/preview/Preview.java net/sourceforge/opencamera/remotecomotecontrol/BluetoothRemoteControl.java net/sourceforge/opencamera/ui/PopupView.java net/sourceforge/opencamera/PanoramaProcessor.java net/sourceforge/opencamera/StorageUtils.java net/sourceforge/opencamera/cameracontroller/CameraControllerManager2.java net/sourceforge/opencamera/OpenCameraApplication.java net/sourceforge/opencamera/cameracontroller/CameraController2.java net/sourceforge/opencamera/AudioListener.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	net/sourceforge/opencamera/cameracontroller/CameraController1.java net/sourceforge/opencamera/PreferenceKeys.java
3	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	net/sourceforge/opencamera/MyApplicationInterface.java net/sourceforge/opencamera/ImageSaver.java net/sourceforge/opencamera/MyPreferenceFragment.java net/sourceforge/opencamera/ui/FolderChooserDialog.java net/sourceforge/opencamera/PanoramaProcessor.java net/sourceforge/opencamera/StorageUtils.java
4	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	net/sourceforge/opencamera/MyPreferenceFragment.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application use no DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['microphone', 'bluetooth', 'location', 'camera'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has no network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
--------	--------	-------------

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	IP: 74.50.61.58 Country: United States of America Region: Texas City: Dallas Latitude: 32.814899 Longitude: -96.879204 View: Google Map
google.github.io	ok	IP: 185.199.110.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
opencamera.org.uk	ok	IP: 216.105.38.11 Country: United States of America Region: California City: San Diego Latitude: 32.894405 Longitude: -117.200951 View: Google Map
schemas.android.com	ok	No Geolocation information available.
design.google.com	ok	IP: 142.250.192.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	IP: 142.250.182.206 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
github.com	ok	IP: 20.205.243.166 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
privacy.google.com	ok	IP: 142.250.183.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

EMAILS

EMAIL	FILE
mark.harman.apps@gmail.com	Android String Resource

POSSIBLE SECRETS
"preference_camera_api" : "API"
"preference_camera_api" : "Camera-API"
"preference_camera_api_camera2" : "Camera2-API"

PLAYSTORE INFORMATION

Title: Open Camera

Score: 4.1749363 **Installs:** 50,000,000+ **Price:** 0 **Android Version Support:** 4.0.3 and up **Category:** Photography **Play Store URL:** [net.sourceforge.opencamera](https://play.google.com/store/apps/details?id=net.sourceforge.opencamera)

Developer Details: Mark Harman, Mark+Harman, 28 Charles Street, Cambridge, CB1 3LZ, <https://opencamera.org.uk/>, mark.harman.apps@gmail.com,

Release Date: Oct 17, 2013 **Privacy Policy:** [Privacy link](#)

Description:

Open Camera is a completely free Camera app. Features: * Option to auto-level so your pictures are perfectly level no matter what. * Expose your camera's functionality: support for scene modes, color effects, white balance, ISO, exposure compensation/lock, selfie with "screen flash", HD video and more. * Handy remote controls: timer (with optional voice countdown), auto-repeat mode (with configurable delay). * Option to take photo remotely by making a noise, or by voice command "cheese". * Configurable volume keys and user interface. * Upside-down preview option for use with attachable lenses. * Overlay a choice of grids and crop guides. * Optional GPS location tagging (geotagging) of photos and videos; for photos this includes compass direction (GPSTagDirection, GPSTagDirectionRef). * Apply date and timestamp, location coordinates, and custom text to photos; store date/time and location as video subtitles (.SRT). * Panorama, including for front camera. * Support for HDR (with auto-alignment and ghost removal) and Exposure Bracketing. * Support for Camera2 API: manual controls (with optional focus assist); burst mode; RAW (DNG) files; slow motion video; log profile video. * Noise reduction (including low light night mode) and Dynamic range optimisation modes. * Options for on-screen histogram, zebra stripes, focus peaking. * Focus bracketing mode. * Completely free, and no third party ads in the app (I only run third party ads on the website). Open Source. (Some features may not be available on all devices, as they may depend on hardware or camera features, the Android version, etc.) Website (and links to source code): <http://opencamera.org.uk/> Note that it's not possible for me to test Open Camera on every Android device out there, so please test before using Open Camera to photo/video your wedding etc :) App icon by Adam Lapinski. Open Camera also uses content under third party licences, see <https://opencamera.org.uk/#licence>

Report Generated by - MobSF v3.5.1 Beta

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.

© 2022 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).