APP SCORES

Security Score **47/100**

Trackers Detection **0/432**

FILE INFORMATION

File Name openmrs-client-debug.apk

Size 14.51MB

MD5 cf93727cbf7408c3f3d1318f85ce7e39

SHA1 15304228dc1bc9e2a259b5067a10563b5f380791

SHA256 e17897d0fbfcc25b1383468ee65c98f65d2f031903505a3a0664c1a210497a17

APP INFORMATION

App Name OpenMRS Android Client

Package Name org.openmrs.mobile

Main Activity org.openmrs.mobile.activities.introduction.SplashActivity

Target SDK 29 Min SDK 19 Max SDK

Android Version Name 3.1.1-debug.1 Android Version Code 1

4 / 33

EXPORTED ACTIVITIES

View All

1 / 13

EXPORTED SERVICES

View All

0 / 10

EXPORTED RECEIVERS

View All

0 / 6

EXPORTED PROVIDERS

View All

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
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: 2023-08-05 15:26:08+00:00
Valid To: 2053-07-28 15:26:08+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha1
md5: 0e57622f2daf1091246039a3fbd7c6ec
sha1: bdf493569215f8c87769fd2c6ef6b58e105604f3
sha256: 6a6fc45d9ae2ce6c729c7905f005b7c13e2cca37340b0f1797b44d7c974ae28a
sha512: 51c7df7cfa9f599ac960e13e5edd2f33d23d024c057d8ae0daa6c47ec61d1829ccd247312a3beec5c8050ff6ccce0714b16069f45ba850246a6775dcf0c0cbad
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 6e52f4c209a271d56908eeda4cb4b89f7dcd3c004270deaea6504c942209b342
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.	
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.	
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.	
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.	
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.	

Showing 1 to 10 of 10 entries

Previous 1 Next

ANDROID API

Search:

API	FILES
Android Notifications	
Base64 Encode	
Content Provider	
Crypto	
Execute OS Command	
Get Installed Applications	
Get System Service	
Get WiFi Details	
Inter Process Communication	
Java Reflection	

Showing 1 to 10 of 19 entries

Previous 1 2 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	2	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.

TITLE	SEVERITY	DESCRIPTION
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.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 4 of 4 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
2	11	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
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	OPTIONS
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.	
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	**Activity** (org.openmrs.mobile.activities.syncedpatients.SyncedPatientsActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.	
5	**Activity** (org.openmrs.mobile.activities.activevisits.ActiveVisitsActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.	
6	**Activity** (org.openmrs.mobile.activities.lastviewedpatients.LastViewedPatientsActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
7	TaskAffinity is set for activity (com.chuckerteam.chucker.internal.ui.MainActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.	
8	Launch Mode of activity (com.chuckerteam.chucker.internal.ui.MainActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.	
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	TaskAffinity is set for activity (leakcanary.internal.activity.LeakActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.	

Showing 1 to 10 of 13 entries

Previous 1 2 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
1	5	2	1	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
1	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		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
2	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		
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	**CWE:** CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') **OWASP Top 10:** M7: Client Code Quality		
4	Debug configuration enabled. Production builds must not be debuggable.	high	**CWE:** CWE-919: Weaknesses in Mobile Applications **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-RESILIENCE-2	com/openmrs/android_sdk/BuildConfig.java org/openmrs/mobile/BuildConfig.java	
5	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	leakcanary/internal/activity/LeakViewsKt.java org/openmrs/mobile/activities/logs/LogsFragment.java	

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
6	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	**CWE:** CWE-312: Cleartext Storage of Sensitive Information **OWASP Top 10:** M9: Reverse Engineering **OWASP MASVS:** MSTG-STORAGE-14		
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	**OWASP MASVS:** MSTG-NETWORK-4	com/openmrs/android_sdk/library/api/RestServiceBuilder.java	
8	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/jacoco/agent/rt/internal_8ff85ea/core/runtime/AbstractRuntime.java permissions/dispatcher/ktx/PermissionRequestFragment.java	
9	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/openmrs/android_sdk/library/security/SecretKeyGenerator.java	

Showing 1 to 9 of 9 entries

Previous 1 Next

SHARED LIBRARY BINARY ANALYSIS

No Shared Objects found.

Search:

NO	SHARED OBJECT	NX	PIE	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

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
classes.dex	Search:

FINDINGS	DETAILS
Compiler	r8

Showing 1 to 1 of 1 entries

Previous 1 Next

DEX	DETECTIONS
classes2.dex	Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check
Compiler	r8 without marker (suspicious)

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes3.dex	Search:

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

Showing 1 to 3 of 3 entries

Previous 1 Next

classes4.dex

Search:

FINDINGS	DETAILS
Compiler	r8 without marker (suspicious)

Showing 1 to 1 of 1 entries

Previous 1 Next

Showing 1 to 4 of 4 entries

Previous 1 Next

BEHAVIOUR ANALYSIS

Search:

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	
00022	Open a file from given absolute path of the file	file	
00028	Read file from assets directory	file	com/amitshekhar/utils/Utils.java
00031	Check the list of currently running applications	reflection collection	org/openmrs/mobile/services/AuthenticateCheckService.java
00036	Get resource file from res/raw directory	reflection	org/openmrs/mobile/activities/settings/SettingsViewModel.java permissions/dispatcher/ktx/PermissionRequestFragment.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	org/openmrs/mobile/activities/community/contact/ContactUsActivity.java org/openmrs/mobile/activities/login/LoginFragment.java org/openmrs/mobile/activities/settings/SettingsFragment.java
00054	Install other APKs from file	reflection	org/openmrs/mobile/activities/addeditpatient/AddEditPatientFragment.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	
00065	Get the country code of the SIM card provider	collection	com/hbb20/CountryCodePicker.java
00079	Hide the current app's icon	evasion	leakcanary/internal/InternalLeakCanary.java

Showing 1 to 10 of 14 entries

Previous 1 2 Next

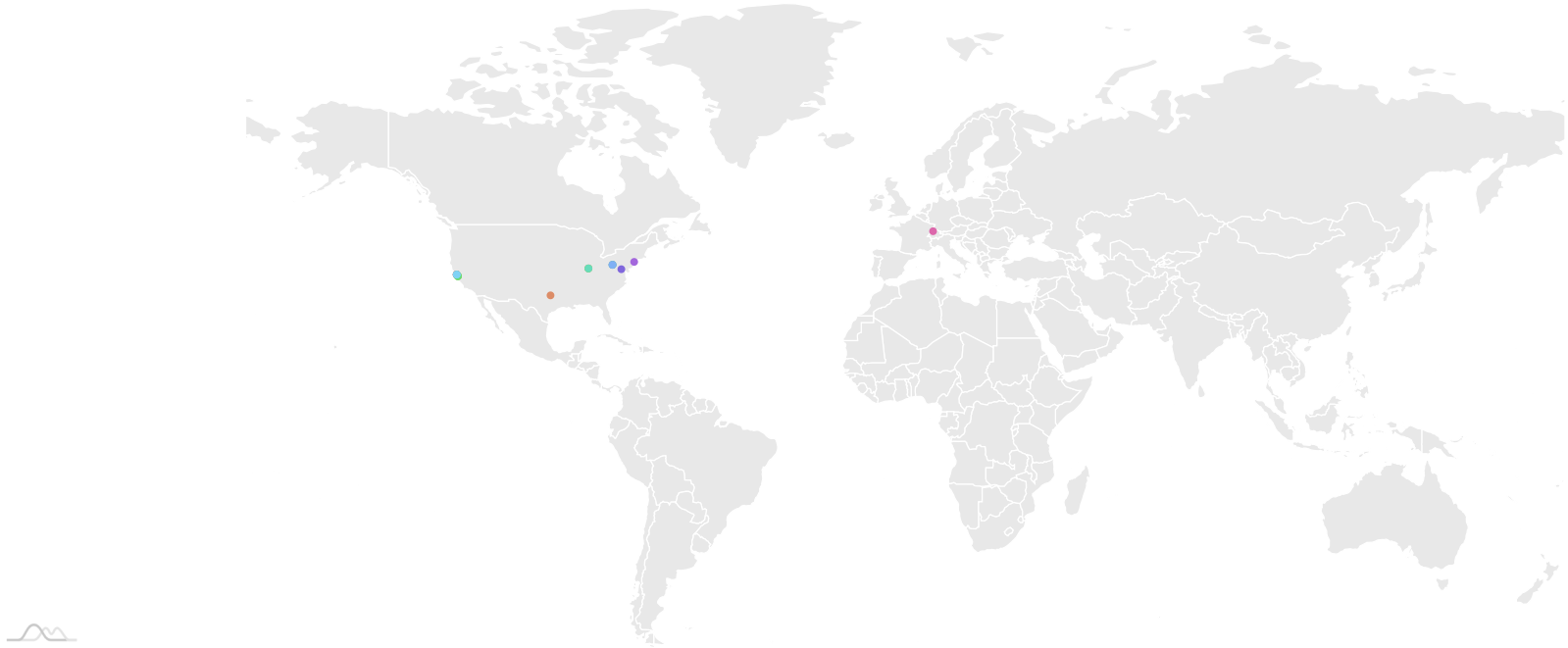
ABUSED PERMISSIONS

Top Malware Permissions	9/25	Other Common Permissions	1/44
android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE,		android.permission.FOREGROUND_SERVICE	

android.permission.ACCESS_NETWORK_STATE,
android.permission.CAMERA,
android.permission.ACCESS_FINE_LOCATION,
android.permission.ACCESS_WIFI_STATE,
android.permission.WAKE_LOCK,
android.permission.RECEIVE_BOOT_COMPLETED,
android.permission.READ_EXTERNAL_STORAGE

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
android.googlesource.com	ok	**IP:** 74.125.21.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
code.google.com	ok	**IP:** 142.250.189.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
demo.openmrs.org	ok	**IP:** 149.165.155.6 **Country:** United States of America **Region:** Indiana **City:** Bloomington **Latitude:** 39.220310 **Longitude:** -86.458237 **View:** Google Map
gist.github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.217.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
openmrs.github.io	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
openmrs.org	ok	**IP:** 149.165.155.251 **Country:** United States of America **Region:** Indiana **City:** Bloomington **Latitude:** 39.220310 **Longitude:** -86.458237 **View:** Google Map
play.g	ok	No Geolocation information available.

Showing 1 to 10 of 25 entries

Previous 1 2 3 Next

URLS

Search:

URL	FILE
http://javax.xml.xmlconstants/feature/secure-processing http://xml.apache.org/xslt}indent-amount	com/chuckerteam/chucker/internal/support/FormatUtils.java
http://localhost/	retrofit2/Response.java

URL	FILE
http://play.g http://play.google.com/store/apps/details?id=org.openmrs.mobile	org/openmrs/mobile/activities/settings/SettingsViewModel.java
http://schemas.android.com/apk/res/android	com/hbb20/CountryCodePicker.java
http://www. https://www.	org/kxml2/wap/wml/Wml.java
http://www.slf4j.org/codes.html http://www.slf4j.org/codes.html#replay http://www.slf4j.org/codes.html#staticloggerbinder http://www.slf4j.org/codes.html#null_lf http://www.slf4j.org/codes.html#multiple_bindings http://www.slf4j.org/codes.html#loggernamemismatch http://www.slf4j.org/codes.html#unsuccessfulinit http://www.slf4j.org/codes.html#substitutelogger http://www.slf4j.org/codes.html#version_mismatch	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#no_static_mdc_binder http://www.slf4j.org/codes.html#null_mdca	org/slf4j/MDC.java
http://www.w3.org/xml/1998/namespace http://www.w3.org/2000/xmlns/	org/kxml2/wap/WbxmlParser.java
http://www.w3.org/xml/1998/namespace http://www.w3.org/2000/xmlns/ http://xmlpull.org/v1/doc/	org/kxml2/io/KXmlParser.java
http://www.w3.org/xml/1998/namespace http://xmlpull.org/v1/doc/features.html#indent-output	org/kxml2/io/KXmlSerializer.java

Showing 1 to 10 of 30 entries

Previous 1 2 3 Next

EMAILS

Search:

EMAIL	FILE
helpdesk@openmrs.com	Android String Resource
this@with.postalcode	org/openmrs/mobile/activities/addeditpatient/AddEditPatientFragment.java

Showing 1 to 2 of 2 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

POSSIBLE HARDCODED SECRETS

▼ Showing all **15** secrets

91c4fb1455470d803a602838dfcd5774
ff9d4b6aab15b17c7fd7e9a0ef9f18c7
67a71486-1a54-468f-ac3e-7091a9a79584
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
cf029002fffdcadf079e8d0a1c9a70ac

86b326012813f09d8f1de7d6d26c986a909d
56a9a59402a83549fd1001ccb124935e
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
a210460b814c04d500eb12025902d60d
4df64341cc978a7de414
013602400437880159360205O5
8aff2efc47fafe870c738f727dfcfc6e
3ad896fa3ec863e554b9890fab536763
8c67d026b8ba5bd5773068edf1b200f9
7b0f5697-27e3-40c4-8bae-f4049abfb4ed

A STRINGS

From APK Resource

▶ Show all **8347** strings

From Code

▶ Show all **24548** strings

From Shared Objects

ACTIVITIES

▼ Showing all **33** activities
org.openmrs.mobile.activities.community.contact.AboutActivity
org.openmrs.mobile.activities.introduction.SplashActivity
org.openmrs.mobile.activities.dashboard.DashboardActivity
org.openmrs.mobile.activities.introduction.IntroActivity
org.openmrs.mobile.activities.syncedpatients.SyncedPatientsActivity
org.openmrs.mobile.activities.login.LoginActivity
org.openmrs.mobile.activities.settings.SettingsActivity
org.openmrs.mobile.activities.patientdashboard.PatientDashboardActivity
org.openmrs.mobile.activities.activevisits.ActiveVisitsActivity
org.openmrs.mobile.activities.visitdashboard.VisitDashboardActivity

org.openmrs.mobile.activities.formlist.FormListActivity
org.openmrs.mobile.activities.formadmission.FormAdmissionActivity
org.openmrs.mobile.activities.formentrypatientlist.FormEntryPatientListActivity
org.openmrs.mobile.activities.addeditpatient.AddEditPatientActivity
org.openmrs.mobile.activities.formdisplay.FormDisplayActivity
org.openmrs.mobile.activities.lastviewedpatients.LastViewedPatientsActivity
org.openmrs.mobile.activities.matchingpatients.MatchingPatientsActivity
org.openmrs.mobile.activities.patientdashboard.details.PatientPhotoActivity
org.openmrs.mobile.activities.logs.LogsActivity
org.openmrs.mobile.activities.patientdashboard.charts.ChartsViewActivity
org.openmrs.mobile.activities.providermanagerdashboard.ProviderManagerDashboardActivity
org.openmrs.mobile.activities.addeditprovider.AddEditProviderActivity
org.openmrs.mobile.activities.providerdashboard.ProviderDashboardActivity
org.openmrs.mobile.activities.community.contact.ContactUsActivity
org.openmrs.mobile.activities.addeditallergy.AddEditAllergyActivity
com.yalantis.ucrop.UCropActivity
com.chuckerteam.chucker.internal.ui.MainActivity
com.chuckerteam.chucker.internal.ui.transaction.TransactionActivity
com.chuckerteam.chucker.internal.ui.throwable.ThrowableActivity
com.google.android.libraries.places.widget.AutocompleteActivity
com.google.android.gms.common.api.GoogleApiActivity
leakcanary.internal.activity.LeakActivity
leakcanary.internal.RequestStoragePermissionActivity

SERVICES

▼ Showing all **13** services
org.openmrs.mobile.services.ConceptDownloadService
org.openmrs.mobile.services.PatientService
org.openmrs.mobile.services.EncounterService
org.openmrs.mobile.services.FormListService
org.openmrs.mobile.services.AuthenticateCheckService
com.chuckerteam.chucker.internal.support.ClearDatabaseService
leakcanary.internal.HeapAnalyzerService
androidx.work.impl.background.systemalarm.SystemAlarmService
androidx.work.impl.background.systemjob.SystemJobService

androidx.work.impl.foreground.SystemForegroundService
androidx.room.MultiInstanceInvalidationService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService

RECEIVERS

▼ Showing all **10** receivers
org.openmrs.mobile.api.SyncStateReceiver
androidx.work.impl.utils.ForceStopRunnable$BroadcastReceiver
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryChargingProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryNotLowProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$StorageNotLowProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$NetworkStateProxy
androidx.work.impl.background.systemalarm.RescheduleReceiver
androidx.work.impl.background.systemalarm.ConstraintProxyUpdateReceiver
com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver
leakcanary.internal.NotificationReceiver

PROVIDERS

▼ Showing all **6** providers
com.chuckerteam.chucker.internal.support.ChuckerFileProvider
com.amitshekhar.debug.DebugDBInitProvider
androidx.lifecycle.ProcessLifecycleOwnerInitializer
leakcanary.internal.LeakCanaryFileProvider
leakcanary.internal.AppWatcherInstaller$MainProcess
leakcanary.internal.PlumberInstaller

LIBRARIES

▼ Showing all **1** libraries

org.apache.http.legacy

SBOM

▼ Showing all **76** Versioned Packages

androidx.activity:activity-ktx@1.2.0
androidx.activity:activity@1.2.2
androidx.annotation:annotation-experimental@1.0.0
androidx.appcompat:appcompat-resources@1.3.0-alpha01
androidx.appcompat:appcompat@1.3.0-alpha01
androidx.arch.core:core-runtime@2.1.0
androidx.asynclayoutinflater:asynclayoutinflater@1.0.0
androidx.cardview:cardview@1.0.0
androidx.coordinatorlayout:coordinatorlayout@1.1.0
androidx.core:core-ktx@1.2.0
androidx.core:core@1.4.0-alpha01
androidx.cursoradapter:cursoradapter@1.0.0
androidx.customview:customview@1.1.0
androidx.databinding:viewbinding@4.1.1
androidx.documentfile:documentfile@1.0.0
androidx.drawerlayout:drawerlayout@1.1.0
androidx.dynamicanimation:dynamicanimation@1.0.0
androidx.exifinterface:exifinterface@1.1.0-beta01
androidx.fragment:fragment-ktx@1.3.0
androidx.fragment:fragment@1.3.2
androidx.gridlayout:gridlayout@1.0.0
androidx.hilt:hilt-work@1.0.0
androidx.interpolator:interpolator@1.0.0
androidx.legacy:legacy-support-core-ui@1.0.0
androidx.legacy:legacy-support-core-utils@1.0.0
androidx.legacy:legacy-support-v13@1.0.0
androidx.legacy:legacy-support-v4@1.0.0
androidx.lifecycle:lifecycle-extensions@2.1.0
androidx.lifecycle:lifecycle-livedata-core-ktx@2.3.0
androidx.lifecycle:lifecycle-livedata-core@2.3.1
androidx.lifecycle:lifecycle-livedata-ktx@2.2.0
androidx.lifecycle:lifecycle-livedata@2.2.0

androidx.lifecycle:lifecycle-process@2.1.0
androidx.lifecycle:lifecycle-runtime-ktx@2.3.0
androidx.lifecycle:lifecycle-runtime@2.3.1
androidx.lifecycle:lifecycle-service@2.1.0
androidx.lifecycle:lifecycle-viewmodel-ktx@2.3.0
androidx.lifecycle:lifecycle-viewmodel-savedstate@2.3.1
androidx.lifecycle:lifecycle-viewmodel@2.3.1
androidx.loader:loader@1.0.0
androidx.localbroadcastmanager:localbroadcastmanager@1.0.0
androidx.media:media@1.0.0
androidx.navigation:navigation-common-ktx@2.3.0
androidx.navigation:navigation-common@2.3.0
androidx.navigation:navigation-fragment-ktx@2.3.0
androidx.navigation:navigation-fragment@2.3.0
androidx.navigation:navigation-runtime-ktx@2.3.0
androidx.navigation:navigation-runtime@2.3.0
androidx.navigation:navigation-ui-ktx@2.3.0
androidx.navigation:navigation-ui@2.3.0
androidx.palette:palette-ktx@1.0.0
androidx.palette:palette@1.0.0
androidx.print:print@1.0.0
androidx.recyclerview:recyclerview@1.2.0-alpha03
androidx.room:room-ktx@2.2.5
androidx.room:room-runtime@2.3.0-alpha01
androidx.room:room-rxjava2@2.0.0
androidx.savedstate:savedstate-ktx@1.1.0
androidx.savedstate:savedstate@1.1.0
androidx.slidingpanelayout:slidingpanelayout@1.0.0
androidx.sqlite:sqlite-framework@2.1.0
androidx.sqlite:sqlite@2.1.0
androidx.swiperefreshlayout:swiperefreshlayout@1.0.0
androidx.tracing:tracing@1.0.0
androidx.transition:transition@1.3.0
androidx.vectordrawable:vectordrawable-animated@1.1.0
androidx.vectordrawable:vectordrawable@1.1.0
androidx.versionedparcelable:versionedparcelable@1.1.0
androidx.viewpager2:viewpager2@1.0.0
androidx.viewpager:viewpager@1.0.0

androidx.work:work-runtime@2.3.4
com.google.android.material:material@1.3.0
com.google.dagger:dagger-lint-aar@2.38.1
com.google.dagger:dagger@2.38.1
com.google.dagger:hilt-android@2.38.1
com.google.dagger:hilt-core@2.38.1

▼ Showing all **38** Packages

com.amitshekhar
com.chuckerteam.chucker
com.futuremind.recyclerviewfastscroll
com.github.amlcurran.showcaseview
com.github.appintro
com.github.mikephil.charting
com.hbb20
com.jakewharton.rxbinding
com.openmrs.android_sdk
com.vladium.emma.rt
com.yalantis.ucrop
dagger
hilt_aggregated_deps
io.michaelrocks.libphonenumber.android
io.reactivex
javax.annotation
javax.inject
leakcanary
okio
org.adw.library.widgets.discreteseekbar
org.checkerframework.checker.nullness.compatqual
org.intellij.lang.annotations
org.jacoco.agent.rt
org.jdeferred
org.jetbrains.annotations
org.joda.time
org.kxml2.io
org.kxml2.kdom
org.kxml2.wap
org.mindrot.jbcrypt
org.openmrs.mobile

org.reactivestreams
org.slf4j
org.xmlpull.v1
permissions.dispatcher
retrofit2
rx
shark

FILES

▶ Show all **3151** files