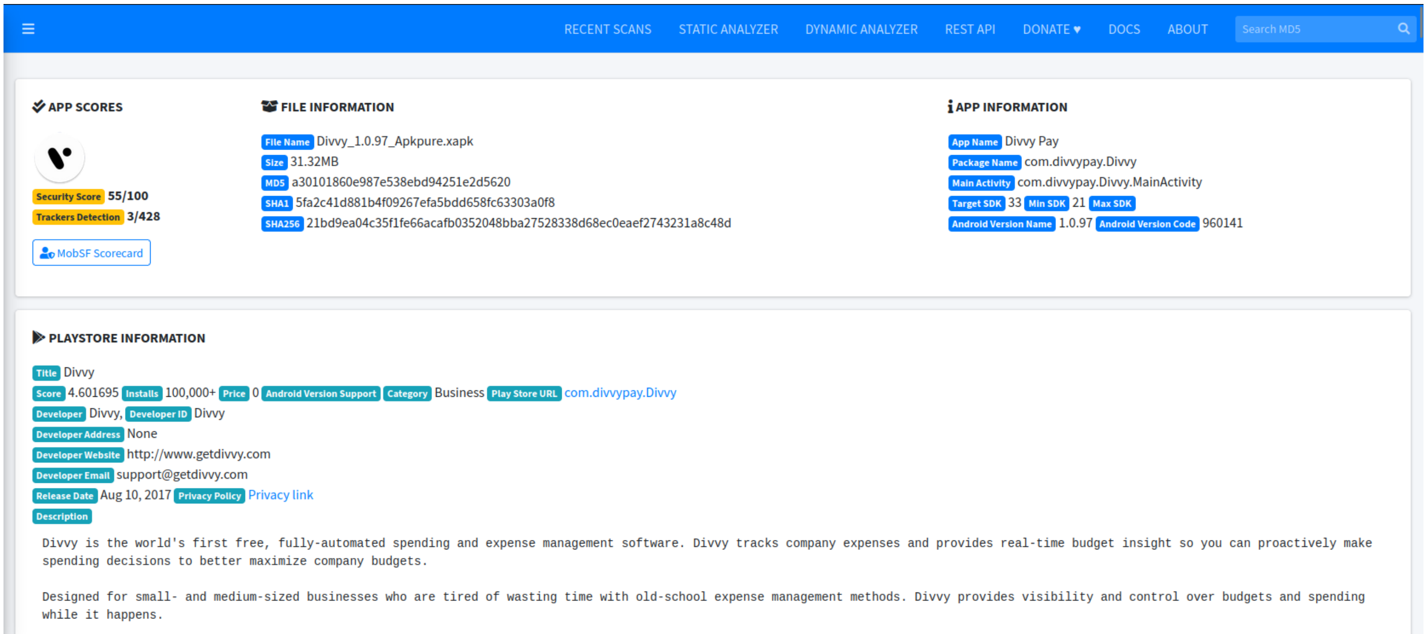
DIVVY.APK

TABLE OF CONTENTS PAGE NO.

DIVVY APK



APP SCORES

Security Score 55/100
Trackers Detection 3/428

MobSF Scorecard

FILE INFORMATION

File Name Divvy_1.0.97_Apkpure.xapk
Size 31.32MB
MD5 a30101860e987e538ebd94251e2d5620
SHA1 5fa2c41d881b4f09267efa5bdd658fc63303a0f8
SHA256 21bd9ea04c35f1fe66acafb0352048bba27528338d68ec0eaef2743231a8c48d

APP INFORMATION

App Name Divvy Pay
Package Name com.divvypay.Divvy
Main Activity com.divvypay.Divvy.MainActivity
Target SDK 33 Min SDK 21 Max SDK
Android Version Name 1.0.97 Android Version Code 960141

PLAYSTORE INFORMATION

Title Divvy
Score 4.601695 Installs 100,000+ Price 0 Android Version Support Category Business Play Store URL com.divvypay.Divvy
Developer Divvy, Developer ID Divvy
Developer Address None
Developer Website http://www.getdivvy.com
Developer Email support@getdivvy.com
Release Date Aug 10, 2017 Privacy Policy Privacy link
Description

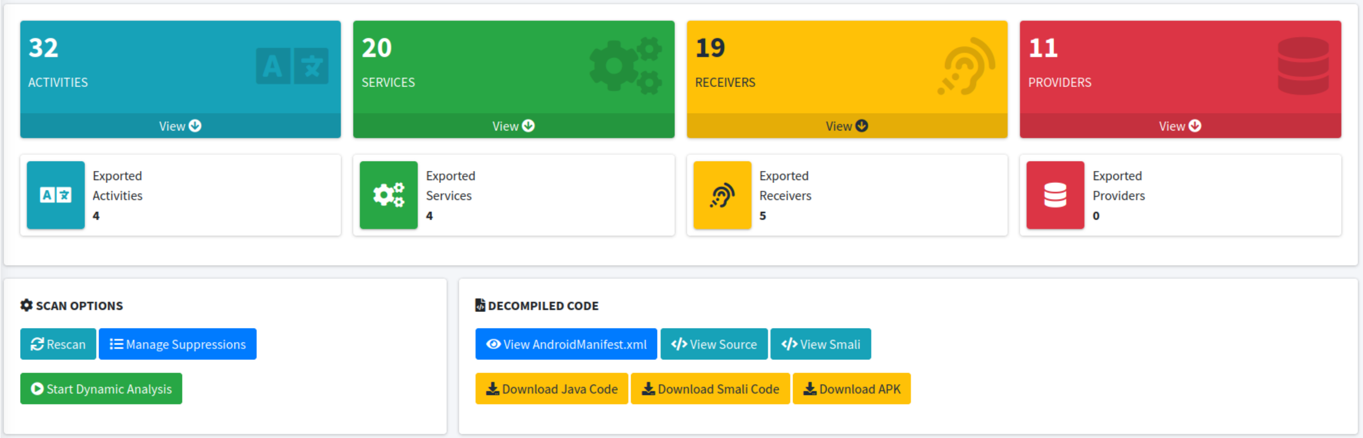
```
Divvy is the world's first free, fully-automated spending and expense management software. Divvy tracks company expenses and provides real-time budget insight so you can proactively make
spending decisions to better maximize company budgets.

Designed for small- and medium-sized businesses who are tired of wasting time with old-school expense management methods. Divvy provides visibility and control over budgets and spending
while it happens.
```

Divvy is the world’s first free, fully automated spending and expense management software. Divvy tracks company expenses and provides real-time budget insight so you can proactively make spending decisions to better maximize company budgets.

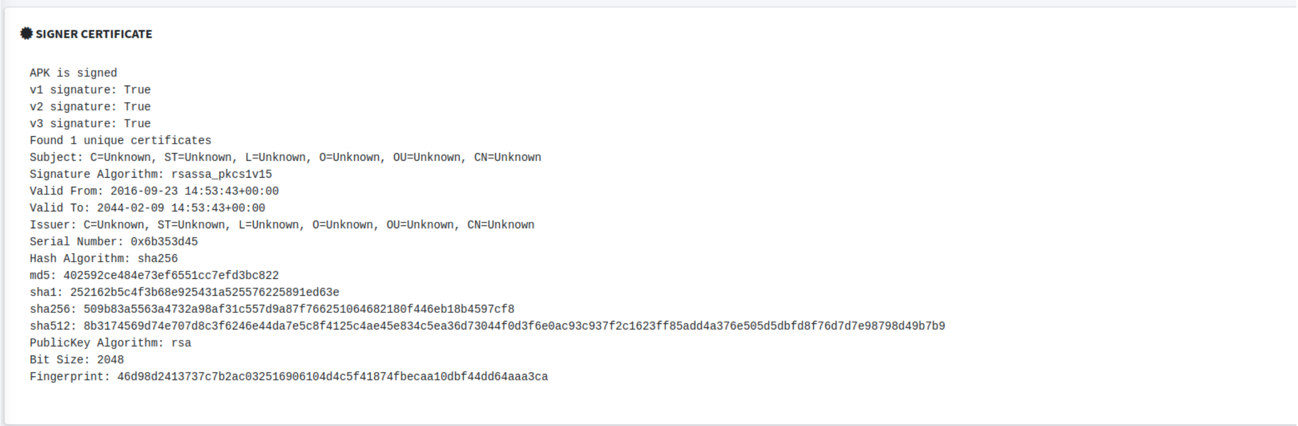
Designed for small- and medium-sized businesses who are tired of wasting time with old-school expense management methods. Divvy provideds visibility and control over budgets and spending while it happens.

SCAN OPTIONS



Here, we can see that we have scan that we can see that in the above figure there are 32 activities, 20 services, 19 receivers, 11 providers.

SIGNER CERTIFICATE

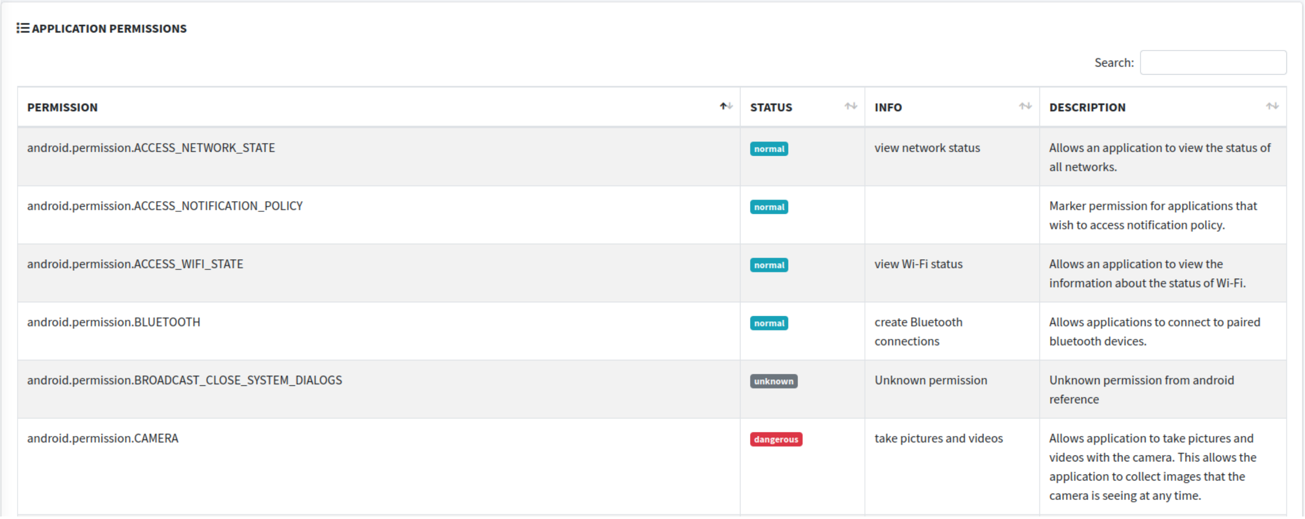


SIGNER CERTIFICATE

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-09-23 14:53:43+00:00
Valid To: 2044-02-09 14:53:43+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Serial Number: 0x6b353d45
Hash Algorithm: sha256
md5: 402592ce484e73ef6551cc7efd3bc822
sha1: 252162b5c4f3b68e925431a525576225891ed63e
sha256: 509b83a5563a4732a98af31c557d9a87f766251064682180f446eb18b4597cf8
sha512: 8b3174569d74e707d8c3f6246e44da7e5c8f4125c4ae45e834c5ea36d73044f0d3f6e0ac93c937f2c1623ff85add4a376e505d5dbfd8f76d7d7e98798d49b7b9
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 46d98d2413737c7b2ac032516906104d4c5f41874fbecaa10dbf44dd64aaa3ca
```

Here, we can see that there is verified signature that this is verified app and can be updated in play store.

PERMISSION



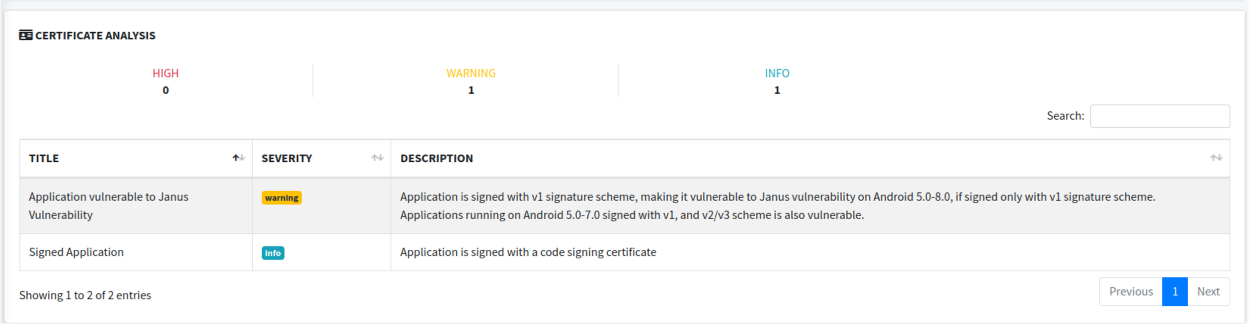
APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_NOTIFICATION_POLICY	normal		Marker permission for applications that wish to access notification policy.
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
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.

Here, we can see that there is permission, status, info and Description So, at first we have see that there are normal status that means this is no dangerous and we can the dangerous in the camera permission is dangerous i.e. in info we can see that they can take picture and Allow this application to take pictures and videos with the camera. And this allows the application to collect images that the camera is seeing at the time.

CERTIFICATE ANALYSIS



CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
0	1	1

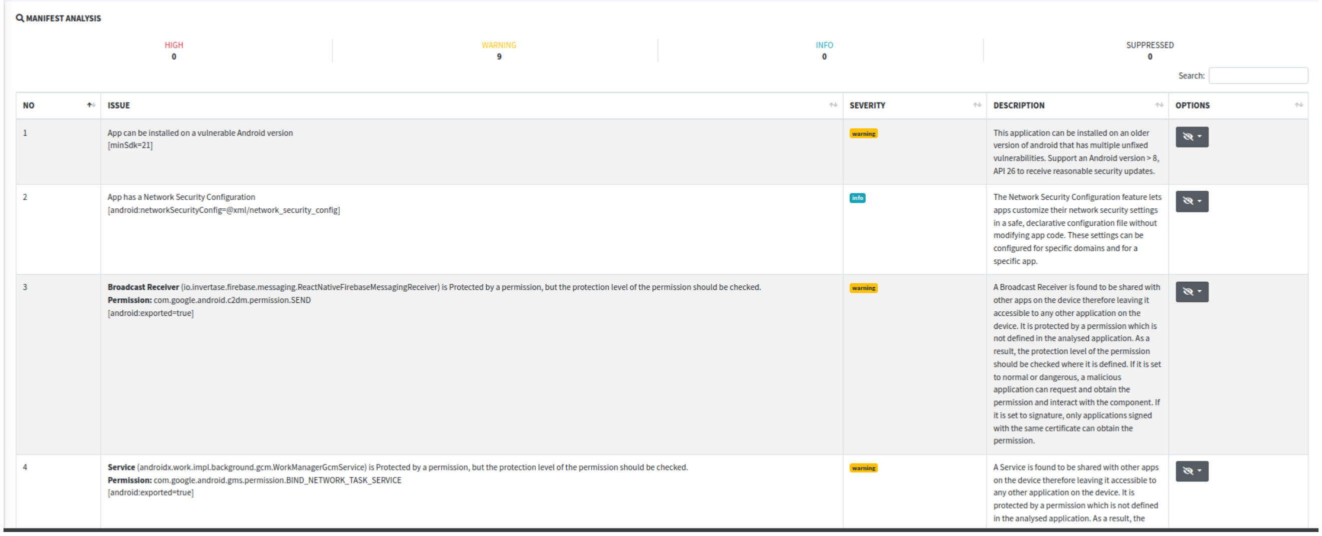
Search:

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.
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 2 of 2 entries

Here, we can see that there is 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. Application running on Android 5.0-7.0, signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS



MANIFEST ANALYSIS

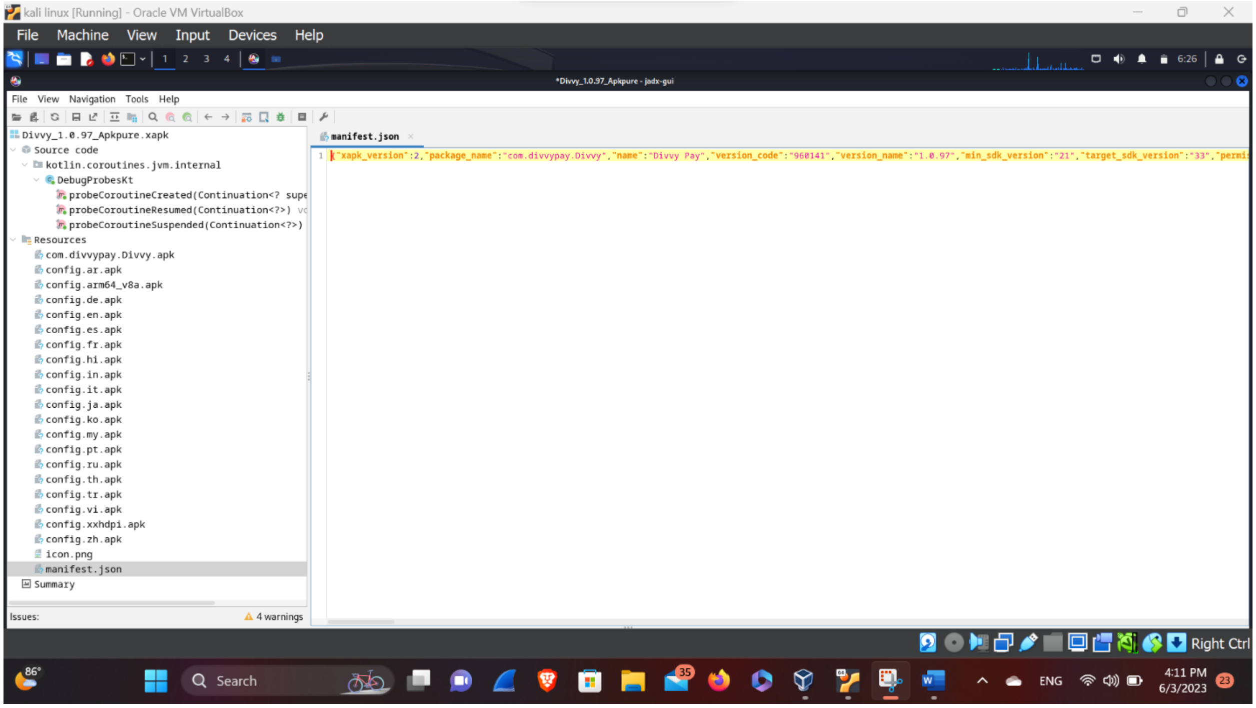
HIGH 0 | WARNING 9 | INFO 0 | SUPPRESSED 0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable Android version [minSdk=21]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 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.	
3	**Broadcast Receiver** (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 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.	
4	**Service** (androidx.work.impl.background.gcm.WorkManagerGcmService) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** com.google.android.gms.permission.BIND_NETWORK_TASK_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	

Here, we can see that there is 9 warning and that can vulnerable so, we can try to exploit them and we can stay safe by disabling this features.

JDAX


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*Divvy_1.0.97_Apkpure - jadx-gui
File View Navigation Tools Help
manifest.json
Issues:
4 warnings
Right Ctrl
Search
ENG
4:11 PM
6/3/2023

```
Divvy_1.0.97_Apkpure.xapk
  Source code
    kotlin.coroutines.jvm.internal
      DebugProbesKt
        probeCoroutineCreated(Continuation<? supe
        probeCoroutineResumed(Continuation<?>) vc
        probeCoroutineSuspended(Continuation<?>)
  Resources
    com.divvypay.Divvy.apk
    config.ar.apk
    config.arm64_v8a.apk
    config.de.apk
    config.en.apk
    config.es.apk
    config.fr.apk
    config.hi.apk
    config.in.apk
    config.it.apk
    config.ja.apk
    config.ko.apk
    config.my.apk
    config.pt.apk
    config.ru.apk
    config.th.apk
    config.tr.apk
    config.vi.apk
    config.xxhdpi.apk
    config.zh.apk
    icon.png
    manifest.json
  Summary
```

```
{"xapk_version":2,"package_name":"com.divvypay.Divvy","name":"Divvy Pay","version_code":"960141","version_name":"1.0.97","min_sdk_version":"21","target_sdk_version":"33","permi
```

Here, we can analysis that what there is the issue by checking the code and we can see this by manifest.json there we can see the permission what the permission are given to this app we can see that there in the above picture we can see that there is permission of the camera that may takes the personal photo of ours let's not to give the permission.

CONCLUSION

So, here let’s try not to allow the permission that an app may take an advantage of the malicious issue. So, this app may contain the permission of the camera that can be used to steal our photos and videos. So, we have to be aware of that.