ANDROID STATIC ANALYSIS REPORT

Next Step (1.0)

File Name:	app-prod-release.apk
Package Name:	org.dpppt.android.app
Average CVSS Score:	5.8
App Security Score:	60/100 (MEDIUM RISK)

FILE INFORMATION

File Name: app-prod-release.apk
Size: 5.55MB
MD5: 46fa8626fdca387d6f1ae0549dd16e32
SHA1: a74f459f5756682ec6ac29147dc168781cba4def
SHA256: a51a2f58b683f943da30f33308deeeee819e3d256957929d0b63839a5a5f882f

APP INFORMATION

App Name: Next Step
Package Name: org.dpppt.android.app
Main Activity: org.dpppt.android.app.main.MainActivity
Target SDK: 29
Min SDK: 23
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 2
Services: 5
Receivers: 8
Providers: 1
Exported Activities: 0
Exported Services: 1
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: O=STAR AndroidSDK Sample
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-04-10 12:49:30+00:00
Valid To: 2120-03-17 12:49:30+00:00
Issuer: O=STAR AndroidSDK Sample
Serial Number: 0x5770d336
Hash Algorithm: sha256
md5: 1314090a97e310e8e64795d8698fe8c7
sha1: a1a137b12762ce771ea6a2c5bbfef709dbc1ecfa
sha256: 5e8840868c4cb0cfbb703f7df9acb21352acd20be06c1347041c846941138a42
sha512:
6c750692814332aabf9970c1cc676e273aefac8777a6d5c585dd7e4924f8736d6503d1a3101125906b8dde8e80db46a1105a226af961a0691eb020833b893043

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 52bdf92ab6f0a327a64357bf44fc32602f0465a8740fc6ebdb7673590d702a5f
```

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	dangerous	create Bluetooth connections	Allows an application to view configuration of the local Bluetooth phone and to make and accept connections with paired devices.
android.permission.BLUETOOTH_ADMIN	dangerous	bluetooth administration	Allows an application to configure the local Bluetooth phone and to discover and pair with remote devices.
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.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
App has a Network Security Configuration [android:networkSecurityConfig]	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.
Application Data can be Backed up [android:allowBackup=true]	medium	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.
Broadcast Receiver (org.dpppt.android.sdk.internal.TracingServiceBroadcastReceiver) is not Protected. An intent-filter exists.	high	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.
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]	high	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.

CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES

ISSUE	SEVERITY	STANDARDS	FILES
The App logs information. Sensitive information should never be logged.	info	**CVSS V2:** 7.5 (high) **CWE:** CWE-532 - Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3	org/dpppt/android/sdk/internal/TracingService.java org/dpppt/android/sdk/internal/TracingServiceBroadcastReceiver.java org/dpppt/android/sdk/internal/gatt/BleClient.java org/dpppt/android/sdk/internal/gatt/GattConnectionTask.java org/dpppt/android/sdk/internal/gatt/BleServer.java
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-312 - Cleartext Storage of Sensitive Information **OWASP Top 10:** M9: Reverse Engineering **OWASP MASVS:** MSTG-STORAGE-14	org/dpppt/android/sdk/internal/database/KnownCases.java org/dpppt/android/sdk/internal/crypto/CryptoModule.java io/reactivex/rxjava3/internal/schedulers/SchedulerPoolFactory.java
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.	high	**CVSS V2:** 5.9 (medium) **CWE:** CWE-89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') **OWASP Top 10:** M7: Client Code Quality	org/dpppt/android/sdk/internal/database/Transaction.java
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	**CVSS V2:** 2.3 (low) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP MASVS:** MSTG-CRYPTO-4	io/reactivex/rxjava3/core/Notification.java io/reactivex/rxjava3/internal/util/NotificationLite.java io/reactivex/rxjava3/internal/util/OpenHashSet.java io/reactivex/rxjava3/internal/util/VolatileSizeArrayList.java io/reactivex/rxjava3/schedulers/Timed.java retrofit2/Utils.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
github.com	good	**IP:** 52.64.108.95 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
discovery.dpppt.org	good	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Indiana **City:** Francisco **Latitude:** 38.333332 **Longitude:** -87.44722 **View:** Google Map

🌐 URLS

URL	FILE
https://discovery.dpppt.org/	org/dpppt/android/sdk/internal/backend/DiscoveryRepository.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/rxjava3/exceptions/UndeliverableException.java
http://localhost/	retrofit2/Response.java

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM

APP SECURITY SCORE	RISK
71 - 100	LOW

Report Generated by - MobSF v3.0.8 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.

© 2020 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.