MOBSF

ANDROID STATIC ANALYSIS REPORT

Dohone (1.7.0)

File Name:	DOHONE-10.apk
Package Name:	com.i4u.dohone
Average CVSS Score:	6.5
App Security Score:	85/100 (LOW RISK)

FILE INFORMATION

File Name: DOHONE-10.apk
Size: 14.45MB
MD5: 163a2c34ba84f9ddad02c8774cccfe5c
SHA1: 33311caacf0cd75b7c18785e1f91b7cee740409b
SHA256: f6c102a794e82bd43dbc696b87a7669fb83c5959841730l3d52bed87b8c7dd1d

APP INFORMATION

App Name: Dohone
Package Name: com.i4u.dohone
Main Activity: .SplashscreenActivity
Target SDK: 26
Min SDK: 26
Max SDK:
Android Version Name: 1.7.0
Android Version Code: 10

APP COMPONENTS

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

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=CM, ST=Cameroun, L=Yaoundé, O=Innov For You, OU=Dohone, CN=Wilfreid Ngah Nanga
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-01-02 12:50:07+00:00
Valid To: 2115-12-09 12:50:07+00:00
Issuer: C=CM, ST=Cameroun, L=Yaoundé, O=Innov For You, OU=Dohone, CN=Wilfreid Ngah Nanga
Serial Number: 0x7e6f8344
Hash Algorithm: sha256
md5: 66b2d8197066182cabc27e62dcb24bfa
sha1: ba486e2185eefa4513df24dbd8f2f1d07a96485a
sha256: b6472cddeeb3c1e32b2afb0a62a9befe8d030fb2923852a5581c008cbcfb2dc1
sha512:
f44b4236e747b121533eb30d6f0ce5fa6bb4105265230ee9bd5f3a860ec5f970a5455d9e628a952bc1b3c963e0b543c7daf1036b08ae578100e17c537edf2e34

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
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_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

<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.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr>
</table>
</td></tr>
</table>

	Manipulator Found	dexmerge

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
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.
Activity (.MainActivity) is not Protected. An intent-filter exists.	high	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.

CODE ANALYSIS

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	com/i4u/dohone/MainActivity.java
App can read/write to External Storage. Any App can read data written to External Storage.	high	**CVSS V2:** 5.5 (medium) **CWE:** CWE-276 - Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	nl/xservices/plugins/SocialSharing.java
This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	**CVSS V2:** 0 (info) **OWASP MASVS:** MSTG-STORAGE-10	nl/xservices/plugins/SocialSharing.java

URLS

URL	FILE
file:///android_asset/www/pages/index.html file:///android_asset/www/pages/about.html	com/i4u/dohone/MainActivity.java
data:image/	nl/xservices/plugins/SocialSharing.java

EMAILS

EMAIL	FILE
someone@domain.com	nl/xservices/plugins/SocialSharing.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
71 - 100	LOW

Report Generated by - MobSF v3.0.9 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.