MOBSF

ANDROID STATIC ANALYSIS REPORT

MainActivity (1.0)

File Name:	test.apk
Package Name:	com.metasploit.stage
Scan Date:	Nov. 23, 2024, 7:26 p.m.

App Security Score: 49/100 (MEDIUM RISK)

Grade: B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	5	0	2	1

FILE INFORMATION

File Name: test.apk
Size: 0.01MB
MD5: c7428805748b8f2a516ba4f0a5f603b4
SHA1: d561c7db68b2212c0ff602f242cec58b639b0a82
SHA256: c583d8548474903bd97a929781a0505887d55000a0b87c4edb5b19c4b636c6f5

APP INFORMATION

App Name: MainActivity
Package Name: com.metasploit.stage
Main Activity: .MainActivity
Target SDK: 17
Min SDK: 10
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

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

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=US/O=Android/CN=Android Debug
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-03-13 01:00:22+00:00
Valid To: 2037-06-11 10:41:17+00:00
Issuer: C=US/O=Android/CN=Android Debug
Serial Number: 0x1
Hash Algorithm: sha1
md5: f324a6fc56edb86dfec17b1f180a5203
sha1: bcb5ad1ee34ed4f36dc81baa8eae5fc5549345f0
sha256: 314c09de91b7ce3d37f0b9ccfc3fa4824256ba2fb730a6ba1fbd7cb7ab65028b

sha512: 42bc444ec10d26b1af8c7629672ad018ee0e113f1ab450c0ee07dc52a2b27a2b36314e376854b460089110d6ef90dc6a1423964d9070ab64e3cc92f06370c312
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
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.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.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.

PERMISSION	STATUS	INFO	DESCRIPTION
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.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
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.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to 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.SET_WALLPAPER	normal	set wallpaper	Allows the application to set the system wallpaper.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
android.permission.WRITE_CALL_LOG	dangerous	allows writing to (but not reading) the user's call log.	Allows an application to write (but not read) the user's call log data.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: dx

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
.MainActivity	Schemes: metasploit://, Hosts: my_host,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **2** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 2.3.3-2.3.7, [minSdk=10]	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.
2	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.
3	Broadcast Receiver (.MainBroadcastReceiver) 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 (.MainService) is not Protected. [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.

CODE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 0 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/metasploit/stage/f.java
2	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/metasploit/stage/f.java
3	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	com/metasploit/stage/Payload.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00079	Hide the current app's icon	evasion	com/metasploit/stage/Payload.java
00022	Open a file from given absolute path of the file	file	com/metasploit/stage/Payload.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	18/24	android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_PHONE_STATE, android.permission.SEND_SMS, android.permission.RECEIVE_SMS, android.permission.RECORD_AUDIO, android.permission.READ_CONTACTS, android.permission.WRITE_SETTINGS, android.permission.CAMERA, android.permission.READ_SMS, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.SET_WALLPAPER, android.permission.READ_CALL_LOG, android.permission.WAKE_LOCK
Other Common Permissions	4/45	android.permission.CHANGE_WIFI_STATE, android.permission.CALL_PHONE, android.permission.WRITE_CONTACTS, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

SCAN LOGS

Timestamp	Event	Error
2024-11-23 19:26:18	Generating Hashes	OK

2024-11-23 19:26:18	Extracting APK	OK
2024-11-23 19:26:18	Unzipping	OK
2024-11-23 19:26:18	Getting Hardcoded Certificates/Keystores	OK
2024-11-23 19:26:19	Parsing AndroidManifest.xml	OK
2024-11-23 19:26:19	Parsing APK with androguard	OK
2024-11-23 19:26:19	Extracting Manifest Data	OK
2024-11-23 19:26:19	Performing Static Analysis on: MainActivity (com.metasploit.stage)	OK
2024-11-23 19:26:19	Fetching Details from Play Store: com.metasploit.stage	OK
2024-11-23 19:26:20	Manifest Analysis Started	OK
2024-11-23 19:26:20	Checking for Malware Permissions	OK
2024-11-23 19:26:20	Fetching icon path	OK
2024-11-23 19:26:20	Library Binary Analysis Started	OK
2024-11-23 19:26:20	Reading Code Signing Certificate	OK

2024-11-23 19:26:20	Failed to get signature versions	CalledProcessError(1, ['/jdk-22.0.2/bin/java', '-Xmx1024M', '-Djava.library.path=', '-jar', '/home/mobsf/Mobile-Security-Framework-MobSF/mobsf/StaticAnalyzer/tools/apksigner.jar', 'verify', '--verbose', '/home/mobsf/.MobSF/uploads/c7428805748b8f2a516ba4f0a5f603b4/c7428805748b8f2a516ba4f0a5f603b4.apk'])
2024-11-23 19:26:20	Running APKiD 2.1.5	OK
2024-11-23 19:26:22	Detecting Trackers	OK
2024-11-23 19:26:22	Decompiling APK to Java with jadx	OK
2024-11-23 19:26:24	Converting DEX to Smali	OK
2024-11-23 19:26:24	Code Analysis Started on - java_source	OK
2024-11-23 19:26:24	Android SAST Completed	OK
2024-11-23 19:26:24	Android API Analysis Started	OK
2024-11-23 19:26:25	Android Permission Mapping Started	OK
2024-11-23 19:26:25	Android Permission Mapping Completed	OK
2024-11-23 19:26:25	Email and URL Extraction Completed	OK
2024-11-23 19:26:25	Android Behaviour Analysis Started	OK
2024-11-23 19:26:25	Android Behaviour Analysis Completed	OK

2024-11-23 19:26:25	Extracting String data from APK	OK
2024-11-23 19:26:25	Extracting String data from Code	OK
2024-11-23 19:26:25	Extracting String values and entropies from Code	OK
2024-11-23 19:26:25	Performing Malware check on extracted domains	OK
2024-11-23 19:26:25	Saving to Database	OK

Report Generated by - MobSF v4.1.8

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.