MOBSF

ANDROID STATIC ANALYSIS REPORT

My Scan APP (2.0)

File Name:	new_sample.apk
Package Name:	com.ldjSxw.heBbQd
Scan Date:	Nov. 16, 2024, 8:58 a.m.
App Security Score:	38/100 (HIGH RISK)
Grade:	C
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	10	1	1	1

FILE INFORMATION

File Name: new_sample.apk
Size: 24.01MB
MD5: a811d17dea54378c55701566cd88b915
SHA1: c68283911030cb890decf888a12a64ac73255dc3
SHA256: 4b5362ee3357caee4f6579c266a19dbb185c826ff9daf89179944d3e426ac123

APP INFORMATION

App Name: My Scan APP
Package Name: com.ldjSxw.heBbQd
Main Activity: com.ldjSxw.heBbQd.IntroActivity
Target SDK: 28
Min SDK: 23
Max SDK:
Android Version Name: 2.0

Android Version Code: 20

APP COMPONENTS

Activities: 4
Services: 5
Receivers: 3
Providers: 2
Exported Activities: 2
Exported Services: 2
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=., ST=., O=., OU=., CN=.
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-11-16 08:56:47+00:00
Valid To: 2052-04-03 08:56:47+00:00
Issuer: C=., ST=., O=., OU=., CN=.
Serial Number: 0x32ff5ed8fa2a4e1d
Hash Algorithm: sha384
md5: 4583433c021b30eeb4066a8b543d2c93
sha1: cacb99490b3692bc76be3643cffea93dc643aa0f
sha256: a344466e4e74c808043b310482103d97dabb22304f6442b371192182305df26f
sha512: 6663be31ad355aaad71734de70ef8cd4ef7e0a80c2496c9d620fcbded3b48273ad65335457f53cfb459588cef449f2899475a10589e0aa522ff388329d7e90be
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 3200df9479ef67df776e80139443cdce724bd8c51e716a4821d6f70fae8e7ade
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.BOOT_COMPLETED	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_USER_PRESENT	unknown	Unknown permission	Unknown permission from android reference
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.ldjSxw.heBbQd.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: dexlib 2.x
kill-classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.MODEL check, Build.TAGS check FINDINGS: Compiler — DETAILS: r8

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>assets/repackaged_pgsHZz.apk!classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>assets/repackaged_pgsHZz.apk!kill-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
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
emulator file check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
assets/repackaged_pgsHZz.apk!kill-classes2.dex	<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 VM check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.ldjSxw.heBbQd.ScanActivity	Schemes: openscan://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
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.

MANIFEST ANALYSIS

HIGH: 5 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.

NO	ISSUE	SEVERITY	DESCRIPTION
3	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.
4	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.
5	Activity (com.ldjSxw.heBbQd.ResultActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level.
6	Activity (com.ldjSxw.heBbQd.ResultActivity) is not Protected. [android:exported=true]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Activity (com.ldjSxw.heBbQd.ScanActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (28) of the app to 29 or higher to fix this issue at platform level.
8	Activity (com.ldjSxw.heBbQd.ScanActivity) is not Protected. [android:exported=true]	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.
9	Service (com.ldjSxw.heBbQd.iservice.TaskService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_ACCESSIBILITY_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
10	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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.
11	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 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.
12	Service (com.google.firebase.iid.FirebaseInstanceIdService) 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: **1** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	com/ldjSxw/heBbQd/MainActivity.java com/ldjSxw/heBbQd/ResultActivity.java com/ldjSxw/heBbQd/a/b.java com/ldjSxw/heBbQd/iservice/JobSevice.java
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	a/b/e/b/b.java com/ldjSxw/heBbQd/a/b.java
3	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/ldjSxw/heBbQd/a/b.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libset.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libset.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/ldjSxw/heBbQd/MainActivity.java com/ldjSxw/heBbQd/ResultActivity.java com/ldjSxw/heBbQd/a/b.java com/ldjSxw/heBbQd/iservice/JobSevice.java com/lzsEsq/dykSgp/jhvqZx/pupsPVlBod.java
00161	Perform accessibility service action on accessibility node info	accessibility service	com/ldjSxw/heBbQd/iservice/TaskService.java
00159	Use accessibility service to perform action getting node info by text	accessibility service	com/ldjSxw/heBbQd/iservice/TaskService.java
00125	Check if the given file path exist	file	com/ldjSxw/heBbQd/MainActivity.java com/lzsEsq/dykSgp/jhvqZx/pupsPVlBod.java
00054	Install other APKs from file	reflection	com/ldjSxw/heBbQd/a/b.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/ldjSxw/heBbQd/a/b.java
00013	Read file and put it into a stream	file	com/ldjSxw/heBbQd/a/b.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/ldjSxw/heBbQd/a/b.java
00036	Get resource file from res/raw directory	reflection	com/ldjSxw/heBbQd/a/b.java
00121	Create a directory	file command	com/lzsEsq/dykSgp/jhvqZx/pupsPVlBod.java

RULE ID	BEHAVIOUR	LABEL	FILES
00104	Check if the given path is directory	file	com/lzsEsq/dykSgp/jhvqZx/pupsPVlBod.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.GET_TASKS, android.permission.VIBRATE, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.READ_PHONE_STATE
Other Common Permissions	5/44	android.permission.FOREGROUND_SERVICE, android.permission.BROADCAST_STICKY, android.permission.CHANGE_WIFI_STATE, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.c2dm.permission.RECEIVE

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

OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.openssl.org	ok	**IP:** 34.49.79.89 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

SCAN LOGS

Timestamp	Event	Error

2024-11-16 08:58:01	Generating Hashes	OK
2024-11-16 08:58:01	Extracting APK	OK
2024-11-16 08:58:01	Unzipping	OK
2024-11-16 08:58:01	Getting Hardcoded Certificates/Keystores	OK
2024-11-16 08:58:01	Parsing APK with androguard	OK
2024-11-16 08:58:03	Parsing AndroidManifest.xml	OK
2024-11-16 08:58:03	Extracting Manifest Data	OK
2024-11-16 08:58:03	Performing Static Analysis on: My Scan APP (com.ldjSxw.heBbQd)	OK
2024-11-16 08:58:03	Fetching Details from Play Store: com.ldjSxw.heBbQd	OK
2024-11-16 08:58:03	Manifest Analysis Started	OK
2024-11-16 08:58:03	Checking for Malware Permissions	OK

2024-11-16 08:58:03	Fetching icon path	OK
2024-11-16 08:58:03	Library Binary Analysis Started	OK
2024-11-16 08:58:03	Analyzing apktool_out/lib/armeabi-v7a/libset.so	OK
2024-11-16 08:58:03	Analyzing lib/armeabi-v7a/libset.so	OK
2024-11-16 08:58:03	Reading Code Signing Certificate	OK
2024-11-16 08:58:04	Running APKiD 2.1.5	OK
2024-11-16 08:58:08	Updating Trackers Database....	OK
2024-11-16 08:58:08	Detecting Trackers	OK
2024-11-16 08:58:09	Decompiling APK to Java with JADX	OK
2024-11-16 08:58:13	Converting DEX to Smali	OK
2024-11-16 08:58:13	Code Analysis Started on - java_source	OK

2024-11-16 08:58:16	Android SAST Completed	OK
2024-11-16 08:58:16	Android API Analysis Started	OK
2024-11-16 08:58:17	Android API Analysis Completed	OK
2024-11-16 08:58:18	Android Permission Mapping Started	OK
2024-11-16 08:58:20	Android Permission Mapping Completed	OK
2024-11-16 08:58:20	Email and URL Extraction Completed	OK
2024-11-16 08:58:20	Android Behaviour Analysis Started	OK
2024-11-16 08:58:22	Android Behaviour Analysis Completed	OK
2024-11-16 08:58:22	Extracting String data from APK	OK
2024-11-16 08:58:22	Extracting String data from SO	OK
2024-11-16 08:58:22	Extracting String data from Code	OK

2024-11-16 08:58:22	Extracting String values and entropies from Code	OK
2024-11-16 08:58:22	Performing Malware check on extracted domains	OK
2024-11-16 08:58:23	Saving to Database	OK
2024-11-16 09:06:16	Performing Malware check on extracted domains	OK
2024-11-16 09:06:20	Detecting Trackers from Domains	OK

Report Generated by - MobSF v4.1.9

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.