ANDROID STATIC ANALYSIS REPORT

Backup (16.18)

File Name:	app-release16.18.99.apk
Package Name:	com.phone_tra_app_spa.alarm
Scan Date:	Aug. 10, 2024, 7:07 p.m.

App Security Score:	50/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
1	42	1	1	1

FILE INFORMATION

File Name: app-release16.18.99.apk
Size: 15.45MB
MD5: 63a512363c3508c0709f5e006a7035fb
SHA1: cf9973eb7ab8d161cbd6e7f47dd75a6b725f0795
SHA256: a4dc20a55e344388e575bf5f84e8626e8fa1771d623dfef4f72f5c34d97ee065

APP INFORMATION

App Name: Backup
Package Name: com.phone_tra_app_spa.alarm
Main Activity:
Target SDK: 31
Min SDK: 19
Max SDK:
Android Version Name: 16.18
Android Version Code: 123

APP COMPONENTS

Activities: 14
Services: 29
Receivers: 32
Providers: 2
Exported Activities: 3
Exported Services: 6
Exported Receivers: 14
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=liudmiluta
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-02-24 12:33:38+00:00
Valid To: 2065-02-11 12:33:38+00:00
Issuer: CN=liudmiluta
Serial Number: 0x5d47fb67
Hash Algorithm: sha256
md5: 25787378ed94e2808e66a8f3ee917b29
sha1: 26af8554ee338d6969fac51bf4dac3186098056e
sha256: dec20b810f50658775d42745847bb4b146f282ed6d0f1375216124b3fdbb27c4

sha512: 35c99e674b9f80739313964207e067d897b1debb735ee0267d7354abedab3d4b66453aa5d8194f204b9888d3cbb721c872d361bd96ebca355f609b5f04908ecb

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: f503aaf688de67f7d3d3a1b75b1be9416f9783c6d31673d0642c0eca557106cc

Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.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.
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.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.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.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.PROCESS_OUTGOING_CALLS	dangerous	intercept outgoing calls	Allows application to process outgoing calls and change the number to be dialled. Malicious applications may monitor, redirect or prevent outgoing calls.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_ADVERTISE	dangerous	required to advertise to nearby Bluetooth devices.	Required to be able to advertise to nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.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.KILL_BACKGROUND_PROCESSES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.
android.hardware.camera.autofocus	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_MMS	dangerous	receive MMS	Allows application to receive and process MMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.VOICE_COMMUNICATION	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMCORDER	unknown	Unknown permission	Unknown permission from android reference
android.permission.MANAGE_EXTERNAL_STORAGE	dangerous	Allows an application a broad access to external storage in scoped storage	Allows an application a broad access to external storage in scoped storage. Intended to be used by few apps that need to manage files on behalf of the users.
android.permission.ACCESS_RESTRICTED_SETTINGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
android.permission.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

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.MANUFACTURER check
Build.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

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: **1** | WARNING: **36** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.4-4.4.4, [minSdk=19]	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	Launch Mode of activity (com.phone_tra_app_spa.alarm.MainActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
4	Activity (com.phone_tra_app_spa.alarm.MainActivity) 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.
5	Activity-Alias (com.phone_tra_app_spa.alarm.AliasActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Launch Mode of activity (com.phone_tra_app_spa.alarm.CheckWarnings) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
7	Launch Mode of activity (com.phone_tra_app_spa.alarm.activities.EnableAccesibilityAccess) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
8	Launch Mode of activity (com.phone_tra_app_spa.alarm.activities.AllowExternalStorage) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
9	Launch Mode of activity (com.phone_tra_app_spa.alarm.activities.DisableNotification) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
10	Launch Mode of activity (com.phone_tra_app_spa.alarm.activities.DisableNotificationOld) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
11	Launch Mode of activity (com.phone_tra_app_spa.alarm.other.Actv_other) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
12	Activity-Alias (com.phone_tra_app_spa.alarm.AliasActivity1) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Launch Mode of activity (com.phone_tra_app_spa.alarm.activities.EnableNotificationAccess) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
14	Launch Mode of activity (com.phone_tra_app_spa.alarm.activities.PhoneAlreadyRegistered) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
15	Launch Mode of activity (com.phone_tra_app_spa.alarm.activities.ThankYouForRegistering) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
16	Broadcast Receiver (com.phone_tra_app_spa.alarm.MySetupBoot) is not Protected. [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.
17	Broadcast Receiver (com.phone_tra_app_spa.alarm.PhoneCallReceiver) is not Protected. [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.
18	Broadcast Receiver (com.phone_tra_app_spa.alarm.SMSReceiver) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
19	Broadcast Receiver (com.phone_tra_app_spa.alarm.ChangedRingerMode) is not Protected. [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.
20	Broadcast Receiver (com.phone_tra_app_spa.alarm.MMSReceiver) is not Protected. [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.
21	Broadcast Receiver (com.phone_tra_app_spa.alarm.ScreenChancedReceiver) is not Protected. [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.
22	Broadcast Receiver (com.phone_tra_app_spa.alarm.MyNetworkChangeReceiver) is not Protected. [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.
23	Broadcast Receiver (com.phone_tra_app_spa.alarm.PackageChangeReceiver) is not Protected. [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.
24	Broadcast Receiver (com.phone_tra_app_spa.alarm.CalendarChangedReceiver) is not Protected. [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.
25	Broadcast Receiver (com.phone_tra_app_spa.alarm.DeviceAdminSampleReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_DEVICE_ADMIN [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.
26	Service (com.phone_tra_app_spa.alarm.services.MyNotificationListener) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_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
27	Service (com.phone_tra_app_spa.alarm.services.MyAccessibilityService) 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.
28	Service (com.phone_tra_app_spa.alarm.receivers.MyFirebaseInstanceIDService) 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.
29	Broadcast Receiver (com.phone_tra_app_spa.alarm.receivers.MyPlugInControlReceiver) is not Protected. [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.
30	Service (com.phone_tra_app_spa.alarm.services.MyWorkerServerCom) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_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.
31	Service (com.phone_tra_app_spa.alarm.services.MyFirebaseMessagingService) 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.
32	Broadcast Receiver (com.phone_tra_app_spa.alarm.receivers.MySystemCalls) is not Protected. [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.
33	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.
34	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]	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
35	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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.
36	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.
37	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

HIGH: **0** | WARNING: **4** | INFO: **1** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	a/h/a/a/cacvdasvds.java b/b/a/a/a/c/a/bdhjjyky.java b/b/a/a/a/c/a/fegdgrehfht.java b/b/a/a/a/c/a/grhhjjyjk.java b/b/a/a/a/c/a/gyyo.java b/b/a/a/a/c/a/qwebb.java b/b/a/a/a/c/a/zsss.java com/phone_tra_app_spa/alarm/a/regbrtyrth.java com/phone_tra_app_spa/alarm/ggfgffbb.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/phone_tra_app_spa/alarm/MainActivity.java com/phone_tra_app_spa/alarm/PhoneCallReceiver.java com/phone_tra_app_spa/alarm/a/fegdgrehfht.java com/phone_tra_app_spa/alarm/a/gwegfdgr.java com/phone_tra_app_spa/alarm/a/tyyuyy.java com/phone_tra_app_spa/alarm/fdfsfsfg.java com/phone_tra_app_spa/alarm/fsbbfbh.java com/phone_tra_app_spa/alarm/receivers/StopRecord.java com/phone_tra_app_spa/alarm/services/CallRecordingService.java com/phone_tra_app_spa/alarm/services/RemoteRecordingService.java com/phone_tra_app_spa/alarm/services/TakePicApi21.java com/phone_tra_app_spa/alarm/uyoo.java org/appspot/apprtc/PeerConnectionClient.java org/appspot/apprtc/RecordedAudioToFileController.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/phone_tra_app_spa/alarm/ServerCommunicate.java com/phone_tra_app_spa/alarm/a/fdfsfsfg.java com/phone_tra_app_spa/alarm/fsbbfbh.java de/tavendo/autobahn/WebSocketWriter.java
4	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	org/appspot/apprtc/PeerConnectionClient.java
5	MD5 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/phone_tra_app_spa/alarm/a/weww.java

SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
2	x86_64/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsnprintf_chk', '__vsprintf_chk', '__fgets_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__strchr_chk', '__memset_chk']	False warning Symbols are available.
3	arm64-v8a/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsnprintf_chk', '__vsprintf_chk', '__fgets_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__strchr_chk', '__memset_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
5	armeabi-v7a/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.
6	x86_64/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsnprintf_chk', '__vsprintf_chk', '__fgets_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__strchr_chk', '__memset_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	True info The binary has the following fortified functions: ['__memcpy_chk', '__vsnprintf_chk', '__vsprintf_chk', '__fgets_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__read_chk', '__strchr_chk', '__memset_chk']	False warning Symbols are available.
8	x86/libjingle_peerconnection_so.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	18/24	android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_PHONE_STATE, android.permission.RECEIVE_SMS, android.permission.READ_SMS, android.permission.ACCESS_COARSE_LOCATION, android.permission.RECORD_AUDIO, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_CALL_LOG, android.permission.READ_CONTACTS, android.permission.ACCESS_FINE_LOCATION, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.CAMERA, android.permission.GET_TASKS, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.SYSTEM_ALERT_WINDOW
Other Common Permissions	13/45	android.permission.CHANGE_WIFI_STATE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.READ_CALENDAR, android.permission.PROCESS_OUTGOING_CALLS, android.permission.FOREGROUND_SERVICE, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FLASHLIGHT, android.permission.BROADCAST_STICKY, android.permission.PACKAGE_USAGE_STATS, 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.sappmonitoring.com	ok	No Geolocation information available.
tools.ietf.org	ok	**IP:** 104.16.45.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
appr.tc	ok	**IP:** 216.239.32.21 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.251.39.4 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.ietf.org	ok	**IP:** 104.16.44.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.webrtc.org	ok	**IP:** 142.250.180.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
appro@openssl.org	lib/arm64-v8a/libjingle_peerconnection_so.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libjingle_peerconnection_so.so

HARDCODED SECRETS

POSSIBLE SECRETS
"password" : "Palavra-passe"
"pref_aecdump_key" : "aecdump_preference"
"please_enter_an_email_and_a_password" : "□□□□□□□□□□□□"
"password" : "Slaptažodis"
"pref_miscsettings_key" : "misc_settings_key"
"password" : "Şifre"
"password" : "პაროლი"
"pref_room_server_url_key" : "room_server_url_preference"
"show_password" : "□□□□"
"pref_fps_key" : "fps_preference"
"password" : "Passord"
"password" : "Passwort"
"enter_password" : "■■■■■■■■■■■■"
"password" : "Шифра"
"password" : "Wagwoord"
"pref_enable_datachannel_key" : "enable_datachannel_preference"
"google_api_key" : "AIzaSyBM092nD06xPtqMAnVhQTpX8U9qbbPfwMM"
"pref_opensles_key" : "opensles_preference"
"password" : "Hasło"

POSSIBLE SECRETS
"pref_disable_built_in_ns_key" : "disable_built_in_ns_preference"
"password" : "■■■■■■■■■"
"password" : "Adgangskode"
"pref_audiosettings_key" : "audio_settings_key"
"password" : "Password"
"please_enter_an_email_and_a_password" : "□□□□□□□□□□□□□"
"pref_data_protocol_key" : "Subprotocol"
"pref_videosettings_key" : "video_settings_key"
"password" : "■■■■■■"
"password" : "□□"
"enter_password" : "□□□□□□□□□□□□□□□□□"
"pref_room_list_key" : "room_list_preference"
"password" : "Salasana"
"pref_negotiated_key" : "negotiated_preference"
"pref_videocall_key" : "videocall_preference"
"pref_resolution_key" : "resolution_preference"
"password" : "Parola"
"password" : "Parool"
"pref_maxvideobitratevalue_key" : "maxvideobitratevalue_preference"
"show_password" : "■■■■■■■■■■"

POSSIBLE SECRETS
"pref_datasettings_key" : "data_settings_key"
"pref_enable_save_input_audio_to_file_key" : "enable_key"
"password" : "Pasword"
"pref_noaudioprocessing_key" : "audioprocessing_preference"
"password" : "пароль"
"password" : "■■■■■▯■▯"
"password" : "Lösenord"
"please_enter_an_email_and_a_password" : "■■■■■■■■■■■■■■■■■■■"
"password" : "Šifra"
"password" : "Parole"
"password" : "գաղտնաբառ"
"password" : "Nenosiri"
"pref_room_key" : "room_preference"
"enter_password" : "■■■■■▯■▯■▯■▯■■▯■"
"google_crash_reporting_api_key" : "AIzaSyBM092nD06xPtqMAnVhQTpX8U9qbbPfwMM"
"pref_audiocodec_key" : "audiocodec_preference"
"password" : "▯▯▯▯"
"pref_tracing_key" : "tracing_preference"
"pref_disable_webrtc_agc_and_hpf_key" : "disable_webrtc_agc_and_hpf_preference"
"password" : "Contrasenya"

POSSIBLE SECRETS
"password" : "Parol"
"pref_disable_built_in_agc_key" : "disable_built_in_agc_preference"
"pref_maxvideobitrate_key" : "maxvideobitrate_preference"
"pref_camera2_key" : "camera2_preference"
"pref_videocodec_key" : "videocodec_preference"
"pref_startaudiobitrate_key" : "startaudiobitrate_preference"
"please_enter_an_email_and_a_password" : "□□□□□□□□□□□□□□□□□□□□□□."
"pref_flexfec_key" : "flexfec_preference"
"password" : "Парола"
"password" : "Heslo"
"password" : "Jelszó"
"pref_max_retransmits_key" : "max_retransmits_preference"
"pref_capturequalityslider_key" : "capturequalityslider_preference"
"pref_use_legacy_audio_device_key" : "use_legacy_audio_device_key"
"password" : "□□□□□"
"password" : "Geslo"
"pref_disable_built_in_aec_key" : "disable_built_in_aec_preference"
"password" : "סיסמה"
"pref_max_retransmit_time_ms_key" : "max_retransmit_time_ms_preference"
"password" : "Contraseña"

POSSIBLE SECRETS
"password" : "■■■■■■■"
"password" : "□□"
"enter_password" : "□□□□□□"
"password" : "лозинка"
"show_password" : "□□□□"
"pref_data_id_key" : "data_id_preference"
"pref_hwcodec_key" : "hwcodec_preference"
"pref_ordered_key" : "ordered_preference"
"pref_screencapture_key" : "screencapture_preference"
"pref_startaudiobitratevalue_key" : "startaudiobitratevalue_preference"
"pref_enable_rtceventlog_key" : "enable_rtceventlog_key"
"pref_speakerphone_key" : "speakerphone_preference"
"show_password" : "□□□□□□□□d"
"pref_displayhud_key" : "displayhud_preference"
"password" : "Wachtwoord"
"enter_password" : "□□□□□□"
c103703e120ae8cc73c9248622f3cd1e
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
01360240043788015936020505

POSSIBLE SECRETS
49f946663a8deb7054212b8adda248c6

SCAN LOGS

Timestamp	Event	Error
2024-08-10 19:07:41	Generating Hashes	OK
2024-08-10 19:07:41	Extracting APK	OK
2024-08-10 19:07:41	Unzipping	OK
2024-08-10 19:07:42	Getting Hardcoded Certificates/Keystores	OK
2024-08-10 19:07:43	Parsing AndroidManifest.xml	OK
2024-08-10 19:07:43	Parsing APK with androguard	OK
2024-08-10 19:07:43	Extracting Manifest Data	OK
2024-08-10 19:07:43	Performing Static Analysis on: Backup (com.phone_tra_app_spa.alarm)	OK
2024-08-10 19:07:43	Fetching Details from Play Store: com.phone_tra_app_spa.alarm	OK
2024-08-10 19:07:44	Manifest Analysis Started	OK

2024-08-10 19:07:44	Checking for Malware Permissions	OK
2024-08-10 19:07:44	Fetching icon path	OK
2024-08-10 19:07:44	Library Binary Analysis Started	OK
2024-08-10 19:07:44	Analyzing lib/armeabi-v7a/libjingle_peerconnection_so.so	OK
2024-08-10 19:07:44	Analyzing lib/x86_64/libjingle_peerconnection_so.so	OK
2024-08-10 19:07:44	Analyzing lib/arm64-v8a/libjingle_peerconnection_so.so	OK
2024-08-10 19:07:45	Analyzing lib/x86/libjingle_peerconnection_so.so	OK
2024-08-10 19:07:45	Analyzing apktool_out/lib/armeabi-v7a/libjingle_peerconnection_so.so	OK
2024-08-10 19:07:45	Analyzing apktool_out/lib/x86_64/libjingle_peerconnection_so.so	OK
2024-08-10 19:07:45	Analyzing apktool_out/lib/arm64-v8a/libjingle_peerconnection_so.so	OK
2024-08-10 19:07:45	Analyzing apktool_out/lib/x86/libjingle_peerconnection_so.so	OK
2024-08-10 19:07:46	Reading Code Signing Certificate	OK
2024-08-10 19:07:46	Running APKiD 2.1.5	OK
2024-08-10 19:07:48	Detecting Trackers	OK

2024-08-10 19:07:48	Decompiling APK to Java with jadx	OK
2024-08-10 19:07:53	Converting DEX to Smali	OK
2024-08-10 19:07:53	Code Analysis Started on - java_source	OK
2024-08-10 19:08:00	Android SAST Completed	OK
2024-08-10 19:08:00	Android API Analysis Started	OK
2024-08-10 19:08:08	Android Permission Mapping Started	OK
2024-08-10 19:08:32	Android Permission Mapping Completed	OK
2024-08-10 19:08:33	Finished Code Analysis, Email and URL Extraction	OK
2024-08-10 19:08:33	Extracting String data from APK	OK
2024-08-10 19:08:33	Extracting String data from SO	OK
2024-08-10 19:08:34	Extracting String data from Code	OK
2024-08-10 19:08:34	Extracting String values and entropies from Code	OK
2024-08-10 19:08:35	Performing Malware check on extracted domains	OK
2024-08-10 19:08:38	Saving to Database	OK

Report Generated by - MobSF v4.0.6

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.