MOBSF

ANDROID STATIC ANALYSIS REPORT

Security Services (31.0)

File Name:	App47207443.apk
Package Name:	com.ksers.ctrlp
Scan Date:	Aug. 10, 2024, 6:57 p.m.

App Security Score: 51/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	11	2	1	1

FILE INFORMATION

File Name: App47207443.apk
Size: 3.2MB
MD5: 79bba29345dd8b6420cf3cd4553fbdf9
SHA1: 8188b40fd7877556c4f7961ecb26afedaee12935
SHA256: 07ce8ad939522b072f0144620fb12925816390b1d65caece2173eed56dff589d

APP INFORMATION

App Name: Security Services
Package Name: com.ksers.ctrlp
Main Activity: com.ksers.ctrlp.MainActivity
Target SDK: 30
Min SDK: 26
Max SDK:
Android Version Name: 31.0
Android Version Code: 31

APP COMPONENTS

Activities: 10
Services: 22
Receivers: 17
Providers: 2
Exported Activities: 0
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Facebook Inc., ST=California, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-03-17 15:54:21+00:00
Valid To: 2049-03-11 15:54:21+00:00
Issuer: CN=Facebook Inc., ST=California, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: 007baea4bc1e2b9680d20db2133be2b5
sha1: fd40af1ca4a541ce136a7f8167a6d2ef041f0399

sha256: 6c236ed9be94c67aa4e088d3f71225ceb9f9f0c24a051309ddfd1cb543b65c62
sha512: 4afbbe8841cf41556efc4d02ca9cb638eb53690a922f9831eafc10427df511cc9a480ec1cc64b596f8886a1356806cb5f64402fcc75a47500c07b19d84ec63f3
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 465a507f8c2592605cabb9276ff26a22b6a2216fe77f684997189d42077bfc14
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.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_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.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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.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.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.PACKAGE_USAGE_STATS	signature	update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.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.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.PACKAGERAISED_THREAD_PRIORITY_USAGE_STATS	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.CAPTURE_AUDIO_OUTPUT	SignatureOrSystem	allows capturing of audio output.	Allows an application to capture audio output.
com.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check FINDINGS: Anti Debug Code — DETAILS: Debug.isDebuggerConnected() check FINDINGS: Compiler — DETAILS: r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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.
3	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.
4	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.

CODE ANALYSIS

HIGH: **1** | WARNING: **5** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c/a/e/e.java c/b/c/h.java c/b/f/e.java c/b/f/h/e.java c/b/g/c0.java c/b/g/d0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	c/b/g/j.java c/b/g/p.java c/b/g/s.java c/b/g/x.java c/b/g/z.java c/f/b/d.java c/f/b/i/e.java c/f/c/b.java c/f/c/c.java c/f/c/d.java c/h/b/c.java c/h/b/d.java c/h/b/e.java c/h/b/n.java c/h/c/b/e.java c/h/d/d.java c/h/d/e.java c/h/j/a.java c/h/j/b.java c/h/j/g.java c/h/j/p.java c/h/j/y.java c/h/k/e.java c/j/b/e.java c/k/b/y.java c/o/a.java c/p/a.java c/q/e.java c/q/f.java c/q/i.java c/s/a/c.java c/s/a/f/c.java c/x/a/b.java c/y/a0/a.java c/y/f.java c/y/n.java com/ksers/ctrlp/services/InitialProcess.java com/ksers/ctrlp/utility/CommonMethods.java d/a/a/a/a.java d/a/b/d.java d/a/b/h.java d/a/b/k.java d/a/b/m/b.java d/a/b/m/c.java d/b/a/a/i/d.java d/b/a/a/j/q/k.java d/b/a/b/b/h.java d/b/a/b/p/b.java d/b/a/b/s/a.java d/b/a/b/u/g.java d/b/c/c.java d/b/c/k/m.java d/b/c/l/c.java d/b/c/l/f/b.java d/b/c/l/f/g/a0.java d/b/c/l/f/g/b0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				d/b/c/l/f/g/e.java d/b/c/l/f/g/e0.java d/b/c/l/f/g/j0.java d/b/c/l/f/g/k.java d/b/c/l/f/g/m.java d/b/c/l/f/g/q.java d/b/c/l/f/g/v.java d/b/c/l/f/h/e.java d/b/c/l/f/m/a.java d/b/c/l/f/m/c.java d/b/c/l/f/m/d.java d/b/c/r/n.java d/b/c/r/t.java d/b/c/r/u.java d/b/c/r/v.java d/b/c/t/b.java d/b/c/t/f.java d/b/c/t/q/b.java d/b/c/t/r/c.java d/b/c/v/a.java d/b/c/v/a0.java d/b/c/v/a1.java d/b/c/v/c.java d/b/c/v/c0.java d/b/c/v/d0.java d/b/c/v/e0.java d/b/c/v/k0.java d/b/c/v/m0.java d/b/c/v/n.java d/b/c/v/n0.java d/b/c/v/o0.java d/b/c/v/p0.java d/b/c/v/s0.java d/b/c/v/t0.java d/b/c/v/v.java d/b/c/v/x0.java d/b/c/v/y.java d/d/a/h/d.java pub/devrel/easypermissions/AppSettingsDialogHolderActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	c/q/e.java c/s/a/f/c.java d/b/a/a/j/t/i/t.java d/b/a/a/j/t/i/v.java d/b/a/a/j/t/i/w.java d/b/a/a/j/t/i/x.java d/b/a/a/j/t/i/y.java d/b/a/a/j/t/i/z.java d/d/a/e/a.java d/d/a/e/b.java d/d/a/e/c.java d/d/a/e/d.java d/d/a/e/e.java d/d/a/e/f.java d/d/a/e/g.java d/d/a/e/h.java d/d/a/e/i.java d/d/a/e/j.java d/d/a/e/k.java d/d/a/e/l.java d/d/a/e/m.java d/d/a/e/n.java d/d/a/e/o.java
3	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/ksers/ctrlp/MainActivity.java com/ksers/ctrlp/activity/AutostartScreen.java com/ksers/ctrlp/activity/Login.java com/ksers/ctrlp/activity/Permissions.java com/ksers/ctrlp/activity/Purpose.java com/ksers/ctrlp/activity/Sync.java com/ksers/ctrlp/workers/BatteryStatusWorker.java
4	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ksers/ctrlp/services/AccessService.java com/ksers/ctrlp/services/DeviceSync.java com/ksers/ctrlp/services/DeviceSyncJob.java d/d/a/h/c.java
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	c/q/i.java com/ksers/ctrlp/receivers/PhoneCallsBroadCastReciver.java com/ksers/ctrlp/services/FirebaseMessages.java com/ksers/ctrlp/utility/CommonMethods.java d/b/c/t/q/c.java
6	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	c/a/e/e.java com/ksers/ctrlp/activity/Login.java f/j/a.java f/j/b.java f/j/d/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/ksers/ctrlp/activity/Login.java com/ksers/ctrlp/services/FirebaseMessages.java com/ksers/ctrlp/workers/BatteryStatusWorker.java d/b/c/l/f/g/e.java
8	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	d/b/c/l/f/g/e.java d/b/c/t/q/b.java d/b/c/v/y.java
9	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/ksers/ctrlp/activity/Login.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi-v7a/libnative-lib.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/libnative-lib.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: ['__memmove_chk', '__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libnative-lib.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: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	False warning Symbols are available.
4	x86/libnative-lib.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/libnative-lib.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/libnative-lib.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: ['__memmove_chk', '__strlen_chk', '__vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libnative-lib.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: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	False warning Symbols are available.
8	x86/libnative-lib.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	17/24	android.permission.READ_CONTACTS, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.READ_CALL_LOG, android.permission.READ_SMS, android.permission.RECEIVE_SMS, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.CAMERA, android.permission.WAKE_LOCK

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	7/45	android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.PACKAGE_USAGE_STATS, android.permission.FOREGROUND_SERVICE, android.permission.READ_CALENDAR, android.permission.PROCESS_OUTGOING_CALLS, 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
reports.crashlytics.com	ok	No Geolocation information available.
update.crashlytics.com	ok	**IP:** 142.250.180.227 **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

DOMAIN	STATUS	GEOLOCATION
api1.mobilehunter.io	ok	**IP:** 188.114.97.10 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
firebase.google.com	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

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

HARDCODED SECRETS

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyD3qVXY9ENELvhYwFuxdpHrGdQAElae23U"
"google_api_key" : "AIzaSyD3qVXY9ENELvhYwFuxdpHrGdQAElae23U"
c103703e120ae8cc73c9248622f3cd1e
88nWk2ab9fnVX52SP3KgNxbfXTg2tFJywsq
49f946663a8deb7054212b8adda248c6
470fa2b4ae81cd56ecbcda9735803434cec591fa

SCAN LOGS

Timestamp	Event	Error
2024-08-10 18:57:43	Generating Hashes	OK
2024-08-10 18:57:43	Extracting APK	OK
2024-08-10 18:57:43	Unzipping	OK
2024-08-10 18:57:43	Getting Hardcoded Certificates/Keystores	OK
2024-08-10 18:57:45	Parsing AndroidManifest.xml	OK
2024-08-10 18:57:45	Parsing APK with androguard	OK
2024-08-10 18:57:45	Extracting Manifest Data	OK
2024-08-10 18:57:45	Performing Static Analysis on: Security Services (com.ksers.ctrlp)	OK
2024-08-10 18:57:45	Fetching Details from Play Store: com.ksers.ctrlp	OK
2024-08-10 18:57:46	Manifest Analysis Started	OK
2024-08-10 18:57:46	Checking for Malware Permissions	OK
2024-08-10 18:57:46	Fetching icon path	OK
2024-08-10 18:57:46	Library Binary Analysis Started	OK

2024-08-10 18:57:46	Analyzing lib/armeabi-v7a/libnative-lib.so	OK
2024-08-10 18:57:46	Analyzing lib/x86_64/libnative-lib.so	OK
2024-08-10 18:57:46	Analyzing lib/arm64-v8a/libnative-lib.so	OK
2024-08-10 18:57:46	Analyzing lib/x86/libnative-lib.so	OK
2024-08-10 18:57:47	Analyzing apktool_out/lib/armeabi-v7a/libnative-lib.so	OK
2024-08-10 18:57:47	Analyzing apktool_out/lib/x86_64/libnative-lib.so	OK
2024-08-10 18:57:47	Analyzing apktool_out/lib/arm64-v8a/libnative-lib.so	OK
2024-08-10 18:57:47	Analyzing apktool_out/lib/x86/libnative-lib.so	OK
2024-08-10 18:57:47	Reading Code Signing Certificate	OK
2024-08-10 18:57:48	Running APKiD 2.1.5	OK
2024-08-10 18:57:50	Detecting Trackers	OK
2024-08-10 18:57:51	Decompiling APK to Java with jadx	OK
2024-08-10 18:57:58	Converting DEX to Smali	OK
2024-08-10 18:57:58	Code Analysis Started on - java_source	OK
2024-08-10 18:58:01	Android SAST Completed	OK

2024-08-10 18:58:02	Android API Analysis Started	OK
2024-08-10 18:58:05	Android Permission Mapping Started	OK
2024-08-10 18:58:09	Android Permission Mapping Completed	OK
2024-08-10 18:58:10	Finished Code Analysis, Email and URL Extraction	OK
2024-08-10 18:58:10	Extracting String data from APK	OK
2024-08-10 18:58:10	Extracting String data from SO	OK
2024-08-10 18:58:10	Extracting String data from Code	OK
2024-08-10 18:58:10	Extracting String values and entropies from Code	OK
2024-08-10 18:58:11	Performing Malware check on extracted domains	OK
2024-08-10 18:58:15	Saving to Database	OK
